Bitdefender®
MOBILE SECURITY

GEBRUIKSAAN WIJZING

Bitdefender Mobile Security

Handleiding

Publicatiedatum 11/22/2022

Juridische kennisgeving

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Voor wie is deze handleiding bedoeld?

Deze gids is bedoeld voor alle Android-gebruikers die Bitdefender Mobile Security hebben gekozen als beveiligingsoplossing voor hun mobiele apparaten. De informatie in dit boek is niet alleen geschikt voor mensen met een technische achtergrond, maar is toegankelijk voor iedereen die met Android-apparaten kan werken.

U zult ontdekken hoe u Bitdefender Mobile Security kunt configureren en gebruiken om uzelf te beschermen tegen dreigingen en andere schadelijke toepassingen. U leert hoe u het beste uit Bitdefender kunt halen.

We wensen u veel leesplezier met deze handleiding.

Hoe kunt u deze handleiding gebruiken?

De handleiding is ingedeeld aan de hand van enkele hoofdonderwerpen:

Aan de slag (pagina 5)

Aan de slag met Bitdefender Mobile Security en zijn gebruikersinterface.

Kenmerken en functionaliteiten (pagina 11)

Ontdek hoe u Bitdefender Mobile Security kunt gebruiken om uzelf te beschermen tegen dreigingen en schadelijke toepassingen door meer te weten te komen over de kenmerken en functionaliteiten.

Hulp vragen (pagina 49)

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 MOBILE SECURITY

Online activiteiten zoals facturen betalen, vakanties boeken of goederen en diensten kopen zijn eenvoudig en zonder gedoe. Maar naarmate zoveel activiteiten op het internet geëvolueerd zijn, zijn er grote risico's aan verbonden, en als beveiligingsgegevens genegeerd worden, kunnen persoonsgegevens gehackt worden. En wat is er belangrijker dan de bescherming van uw gegevens in online accounts en op uw persoonlijke smartphone?

Met **Bitdefender Mobile Security** kunt u:

- De beste bescherming krijgen voor uw Android smartphone en tablet met minimale impact op de levensduur van de batterij
- Voorkomen dat u het slachtoffer wordt van op links gebaseerde mobiele oplichting
- Toegang krijgen tot uw beveiligde VPN voor een snelle, anonieme en veilige ervaring tijdens het surfen op het web
- Lokaliseer, vergrendel en wis informatie van uw Android-apparaat van op afstand in het geval van verlies of diefstal
- Controleren of uw e-mailaccount betrokken is geweest bij gegevensinbreuken of datalekken

2. AAN DE SLAG

2.1. Apparaatvereisten

Bitdefender Mobile Security werkt op alle apparaten met Android 5.0 of latere versies van het besturingssysteem. Een actieve internetverbinding is vereist voor in-the-cloud scannen op dreigingen.

2.2. Installeer Bitdefender Mobile Security

- **Vanuit Bitdefender Central**
  - Android
    1. Ga naar: https://central.bitdefender.com.
    2. Log in op uw Bitdefender-account.
    3. Selecteer het paneel **Mijn apparaten**.
    4. Tik op **BESCHERMING INSTALLEREN** en tik vervolgens op **Dit apparaat beschermen**.
    5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
    6. U wordt doorgestuurd naar **Google Play**. In het scherm van Google Play tikt u op de installatie-optie.
  - Op Windows, macOS en iOS
    1. Ga naar: https://central.bitdefender.com.
    2. Meld u aan bij uw Bitdefender-account.
    3. Selecteer de **Mijn apparaten** paneel.
    4. Druk op **BESCHERMING INSTALLEREN** en druk vervolgens op **Andere apparaten beschermen**.
    5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
    6. Druk op **DOWNLOADKOPPELING VERZENDEN**.

7. Voer in het overeenstemmende veld een e-mailadres in en druk op **E-MAIL VERSTUREN**. De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
8. Controleer op het apparaat waarop u Bitdefender wilt installeren, het e-mailadres dat u ingevoerd hebt en druk op de overeenstemmende downloadknop.

- **Vanuit Google Play**
  Zoek Bitdefender Mobile Security om de app te vinden en te installeren.
  Als alternatief kunt u de QR-code scannen:

  Voordat u de valideringsstappen kunt volgen, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security.
  Tik op **VERDERGAAN** om verder te gaan naar het volgende venster.

2.3. Log in op uw Bitdefender-account

Om Bitdefender Mobile Security te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google-, Apple- of Microsoft-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd in the loggen op een account.

Als u Bitdefender Mobile Security hebt geïnstalleerd vanuit uw Bitdefender-account, probeert de app zich automatisch aan te melden bij dat account.

Om uw apparaat te koppelen aan een Bitdefender-account:

1. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account. Hebt u geen Bitdefender-account en wenst u er een aan te maken, klik op de daartoe bestemde link.

2. Tik op **AANMELDEN**.

Om in te loggen via een Facebook-, Google- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij Of log in met. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security.

> **Opmerking**
> Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

2.4. Bescherming configureren

Eens u ingelogd bent op de toepassing verschijnt het venster Bescherming configureren. Om uw apparaat te beveiligen, raden we aan dat u de volgende stappen doorloopt:

- **Status abonnement**. Om te worden beschermd door Bitdefender Mobile Security, moet u uw product activeren met behulp van een abonnement, dat aangeeft hoelang u het product mag gebruiken. Wanneer het abonnement verlopen is, zal de toepassing niet meer werken en is uw apparaat niet langer beschermd.
  Tik op IK **HEB EEN CODE**, en vervolgens op **ACTIVEREN**, indien u een activeringscode hebt.
  Indien u ingelogd bent met een nieuwe Bitdefender-account en geen activeringscode hebt, kunt u het product 14 dagen lang gratis gebruiken.
- **Webbescherming**. Tik op **ACTIVEREN** indien uw apparaat Toegankelijkheid vereist om Webbescherming te activeren. U wordt dan doorgestuurd naar het menu Toegankelijkheid. Tik op Bitdefender Mobile Security, en schakel de overeenkomstige schakelaar in.
- **Malware scanner**. Voer een eenmalige scan uit om te verzekeren dat uw apparaat geen bedreigingen bevat. Tik op **NU SCANNEN** om het scanproces op te starten.
  Het dashboard verschijnt zodra het scanproces begint. Hier ziet u de beveiligingsstatus van uw apparaat.

2.5. Dashboard

Tik op het Bitdefender Mobile Security-pictogram in de app drawer van uw apparaat om de app-interface te openen.

Het Dashboard biedt u informatie over de beveiligingsstatus van uw apparaat en helpt u aan de hand van Autopilot de beveiliging van uw apparaat te verbeteren, door u aanbevelingen te doen over de functies.

De statuskaart bovenaan het venster informeert u aan de hand van expliciete berichten en suggestieve kleuren over de beveiligingsstatus van het apparaat. Indien Bitdefender Mobile Security geen waarschuwingen bevat, is de statuskaart groen. Wanneer er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statuskaart naar rood.

Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing van Bitdefender Mobile Security inbegrepen zijn, ontdekken, en ervan genieten.

Als er een procedure actief is of als u actie moet ondernemen, wordt er in het Dashboard een kaart weergegeven met meer informatie en mogelijke acties.

Vanuit de onderste navigatiebalk hebt u toegang tot de Bitdefender Mobile Security-functies en kunt u eenvoudig navigeren:

Malware Scanner

Hiermee kunt u een scan starten en de optie Opslag scannen inschakelen. Zie Malwarescanner (pagina 11) voor meer informatie.

Webbescherming

Garandeert een veilige surfervaring door u te waarschuwen over mogelijke schadelijke websites. Zie Webbescherming (pagina 13) voor meer informatie.

VPN

Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie VPN (pagina 14) voor meer informatie.

Scam Alert

Houdt u veilig door u te waarschuwen voor schadelijke links die binnenkomen via SMS, berichtentoepassingen en elk type melding. Raadpleeg Scam Alert (pagina 17) voor meer informatie.

Anti-Theft

Hiermee kunt u de Anti-Theft-functies in- of uitschakelen en instellingen configureren. Zie Antidiefstalfuncties (pagina 20) voor meer informatie.

Accountprivacy

Controleert of er een gegevenslek was in uw online accounts. Zie Accountprivacy (pagina 24) voor meer informatie.

App Lock

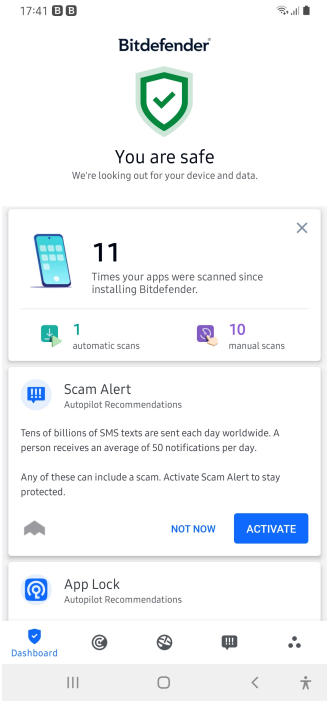
Hiermee kunt u de geïnstalleerde apps beveiligen door een pincode in te stellen. Zie App Lock (pagina 26) voor meer informatie.

Rapporten

Hier wordt een logboek bijgehouden van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten op uw apparaat. Raadpleeg Rapporten (pagina 30) voor meer informatie.

WearON

Deze functie communiceert met uw smartwatch om uw telefoon terug te vinden als deze is zoekgeraakt. Zie WearON (pagina 31) voor meer informatie.


17:41
Bitdefender
You are safe
We're looking out for your device and data.
11
Times your apps were scanned since installing Bitdefender.
1
automatic scans
10
manual scans
Scam Alert
Autopilot Recommendations
Tens of billions of SMS texts are sent each day worldwide. A person receives an average of 50 notifications per day.
Any of these can include a scam. Activate Scam Alert to stay protected.
NOT NOW
ACTIVATE
App Lock
Autopilot Recommendations
Dashboard

3. KENMERKEN EN FUNCTIONALITEITEN

3.1. Malwarescanner

Bitdefender beschermt uw apparaat en uw gegevens tegen schadelijke apps, door scans uit te voeren tijdens de installatie van nieuwe apps. U kunt ook handmatig een scan starten.

De interface van de Malwarescanner biedt een lijst van alle soorten dreigingen waar Bitdefender naar op zoek is, alsook hun definities. Tik op een dreiging om de definitie ervan weer te geven.

> **Opmerking**
> Zorg dat uw mobiele apparaat verbonden is met internet. Als uw apparaat geen internetverbinding heeft, kan de scan niet worden gestart.

- **Scannen bij installatie**
  Zodra u een nieuwe app installeert, wordt deze automatisch door Bitdefender Mobile Security gescand met behulp van cloud-technologie. Deze scanprocedure wordt herhaald wanneer u een update van de geïnstalleerde apps uitvoert.
  Als een geïnstalleerde app schadelijk blijkt te zijn, verschijnt er een waarschuwing met het advies de app te verwijderen. Tik dan op **Verwijderen** om naar het verwijderingsscherm voor de app te gaan.
- **Scannen op verzoek**
  Wanneer u wilt controleren of u alle apps op uw apparaat veilig kunt gebruiken, kunt u een scan op aanvraag uitvoeren.
  Om de scan op verzoek te starten:
  1. Tik op **Malware Scanner** in de onderste navigatiebalk.
  2. Tik op **SCAN STARTEN**.

> **Opmerking**
> In Android 6 zijn extra machtigingen vereist voor de Malware Scanner-functie. Nadat u de knop **SCAN STARTEN** hebt ingedrukt, selecteert u **Toestaan** voor de volgende items:
>
> - **Antivirus** toestaan om telefoongesprekken te starten en te beheren?
> - **Antivirus** toegang geven tot foto's, media en bestanden op uw apparaat?

De voortgang van de scan wordt weergegeven. U kunt de scan op elk gewenst moment afbreken.

Bitdefender Mobile Security scant normaal gesproken het interne geheugen van uw apparaat met inbegrip van een eventueel aanwezige SD-kaart (de "opslag"). Hierdoor worden ook schadelijke apps op de geheugenkaart opgespoord voordat ze schade kunnen aanrichten.

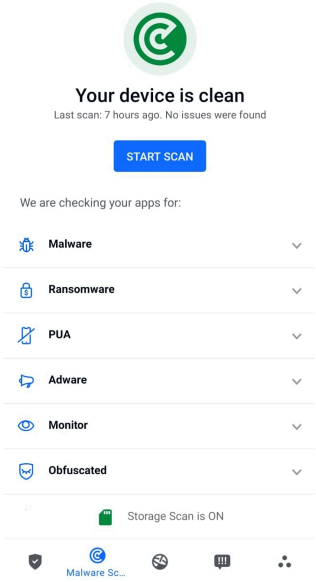
Om de instelling Opslag scannen uit te schakelen:

1. Tik op **Meer** in de onderste navigatiebalk.
2. Tik op **Instellingen**.
3. Schakel de schakelaar **Opslag scannen** in het gebied Malwarescanner uit.

Als er schadelijke apps worden aangetroffen, krijgt u hier bericht over. U kunt deze apps dan verwijderen via de knop **Verwijderen**.

De Malwarescanner-kaart geeft de status van uw apparaat weer. Zolang het apparaat veilig is, is de kaart groen. Wanneer er een scan moet worden uitgevoerd of als u actie moet ondernemen, wordt de kaart rood.

Als uw Android-versie 7.1 of recenter is, kunt u een snelkoppeling gebruiken naar Malware Scanner zodat u scans sneller kunt uitvoeren, zonder de Bitdefender Mobile Security interface te openen. Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het icoon selecteren.



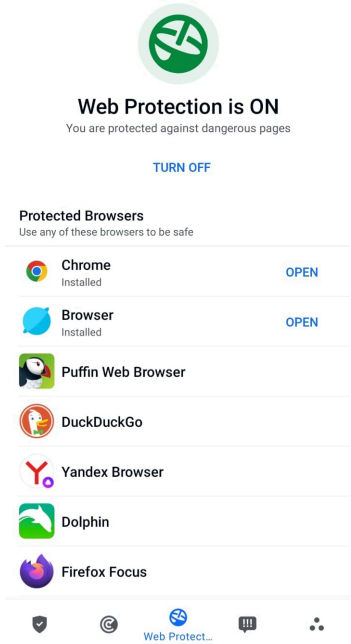
3.2. Webbescherming

Web Protection gebruikt de cloudservices van Bitdefender om de webpagina's te controleren die u bezoekt met de standaard Android-browser, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser en Dolphin.

Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Webbeveiliging.

Geef de functie toestemming om zich te registreren als een Toegankelijkheid-service en tik op **Aanzetten** wanneer hierom wordt gevraagd. Tik op **Antivirus** en zet de schakelaar aan. Bevestig vervolgens dat u toestemming geeft voor de toegang.



Telkens u een website voor internetbankieren gebruikt, vraagt Bitdefender Web Protection u om Bitdefender VPN te gebruiken. De notificatie verschijnt in de statusbalk. We raden aan dat u Bitdefender VPN gebruikt wanneer u ingelogd bent op uw bankrekening, zodat u beveiligd blijft tegen mogelijke beveiligingsinbreuken.

Om de notificatie Webbescherming uit te schakelen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel de overeenstemmende schakelaar in het gebied Webbescherming uit.

3.3. VPN

Met Bitdefender VPN houdt u uw data privé telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. Zo vermijdt u onfortuinlijke situaties, bijvoorbeeld diefstal van persoonlijke gegevens of pogingen om het IP-adres van uw apparaat toegankelijk te maken voor hackers.

De VPN werkt zoals een tunnel tussen uw apparaat en het netwerk waarmee u verbindt: de VPN beveiligt die verbinding, door aan de hand van versleuteling volgens bankrichtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het praktisch onmogelijk wordt om uw apparaat te identificeren tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.

> **Opmerking**
> Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de Bitdefender VPN-app voor het eerst probeert te gebruiken. Door het gebruik van de app verder te zetten, bevestigt u dat u op de hoogte bent van de toepasselijke reguleringen van het land en van de risico's die u mogelijk loopt.

Er zijn twee manieren om Bitdefender VPN in of uit te schakelen:

- Tik in de VPN-kaart op het Dashboard op **VERBINDEN**.
  De status van Bitdefender VPN wordt weergegeven.
- Tik op **VPN** in de onderste navigatiebalk en tik vervolgens op **VERBINDEN**.
  Tik op **VERBINDEN** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.
  Tik op **VERBREKEN** wanneer u de verbinding wilt verbreken.

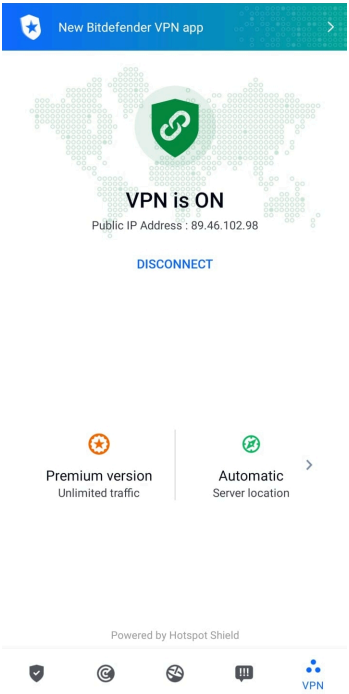
> **Opmerking**
> De eerste keer dat u VPN opstart, zal u worden gevraagd Bitdefender toe te laten een VPN verbinding op te zetten die het netwerkverkeer zal monitoren. Tik op **OK** om verder te gaan.

Als de versie van uw Android 7.1 of hoger is, hebt u toegang tot een snelkoppeling naar Bitdefender VPN, zonder de interface van Bitdefender Mobile Security te openen.

Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het icoon selecteren.

Om uw batterij te sparen, raden we aan de VPN-functie uit te schakelen wanneer u dit niet gebruikt.

Indien u een premium-abonnement hebt en u de server naar wens wilt veranderen, tik op Serverlocatie in de VPN-functie en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg



3.3.1. VPN Instellingen

Voor een geavanceerde configuratie van uw VPN:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.

In het VPN-gebied kunt u de volgende opties configureren:

- Snelle toegang VPN - er verschijnt een notificatie in de statusbalk van uw apparaat waarmee u VPN snel kunt inschakelen.

- Waarschuwing Open wifinetwerk - telkens u verbinding maakt met een open wifinetwerk, wordt u via de statusbalk van uw apparaat gevraagd om de VPN te gebruiken.

3.3.2. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermde inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk ogenblik upgraden naar de versie Bitdefender Premium VPN door te tikken op **Premium activeren** in het VPN-venster.

Het Bitdefender Premium VPN-abonnement staat los van het Bitdefender Mobile Security-abonnement, wat betekent dat u het kunt gebruiken zolang het beschikbaar is, ongeacht de status van uw beveiligingsabonnement. Als het Bitdefender Premium VPN-abonnement afloopt, maar het abonnement voor Bitdefender Mobile Security nog steeds actief is, wordt u teruggezet naar het gratis plan.

Bitdefender VPN is een cross-platform product en is beschikbaar in de Bitdefender-producten die compatibel zijn met Windows, macOS, Android en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.

> **Opmerking**
> Bitdefender VPN werkt ook als zelfstandige applicatie op alle ondersteunde besturingssystemen, namelijk Windows, macOS, Android en iOS.

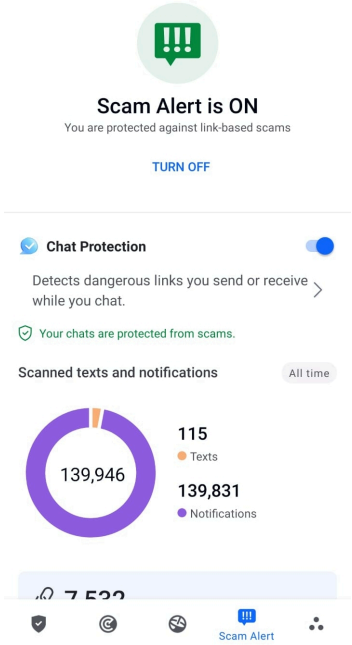
3.4. Scam Alert

De Scam Alert-functie neemt preventieve maatregelen en pakt potentieel gevaarlijke situaties aan voordat ze een probleem kunnen worden, inclusief malwaredreigingen. Scam Alert controleert alle inkomende SMS-berichten en Android-meldingen in real time.

Wanneer een gevaarlijke link in een bericht op uw telefoon binnenkomt, verschijnt er een waarschuwing op uw scherm. Bitdefender biedt twee

opties. De eerste optie is om de informatie te verwerpen. De tweede optie is **DETAILS WEERGEVEN**. Dit geeft u meer informatie over het incident, evenals essentiële adviezen, zoals:

- Open de gedetecteerde koppeling niet en stuur deze niet door.
- Als het om teksten gaat, wis het bericht dan indien mogelijk.
- Blokkeer de afzender als dit geen betrouwbare contactpersoon is.
- Wis de app die gevaarlijke koppelingen verstuurt in notificaties.



Opmerking

Vanwege de beperkingen van het Android-besturingssysteem kan Bitdefender geen tekstberichten verwijderen of directe maatregelen nemen met betrekking tot de SMS-berichten of andere bronnen van schadelijke notificaties. Als u de Scam Alert-waarschuwing negeert en de gevaarlijke koppeling probeert te openen, zal de Web Protection-functie van Bitdefender deze automatisch opvangen en voorkomen dat uw apparaat wordt geïnfecteerd.

3.4.1. Scam Alert activeren

Om Scam Alert in te schakelen, moet u de Bitdefender Mobile Security-app toegang verlenen tot de SMS-berichten en het notificatiesysteem:

1. Open de Bitdefender Mobile Security-app die op uw Android-telefoon of -tablet is geïnstalleerd.
2. Tik in het hoofdscherm van de Bitdefender-app op de optie **Scam Alert** in de onderste navigatiebalk en druk vervolgens op **INSCHAKELEN**.
3. Tik op de knop **TOESTAAN**.
4. Zet Bitdefender Security in de lijst Notificatietoegang op de positie **AAN**.
5. Bevestig de actie door op **TOESTAAN** te drukken.
6. Keer terug naar het Scam Alert-scherm en druk op **TOESTAAN** om Bitdefender de mogelijkheid te geven inkomende SMS-berichten te scannen.

3.4.2. Chatbeveiliging in real time

Chatberichten zijn onze meest comfortabele manier om contact te houden, maar ze zijn ook een gemakkelijke manier voor gevaarlijke koppelingen om u te bereiken.

Als de functie Chatbeveliging actief is, wordt de Scam Alert-module uitgebreid van het beschermen van uw teksten en notificaties tot het beveiligen van uw chats tegen aanvallen op basis van koppelingen, door gevaarlijke koppelingen te detecteren die u tijdens het chatten verzendt of ontvangt.

Om Chatbeveiliging in te schakelen:

1. Open de Bitdefender Mobile Security-app die op uw Android-telefoon of -tablet is geïnstalleerd.
2. Tik in het hoofdscherm van de Bitdefender-app op de optie **Scam Alert** in de onderste navigatiebalk.
3. Bovenaan het tabblad Scam Alert vindt u de functie Chatbeveiliging. Zet de betreffende schakelaar in de stand **AAN**.

Opmerking
Momenteel is Chatbeveiliging compatibel met de volgende toepassingen:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

3.5. Antidiefstalfuncties

Bitdefender helpt u bij het terugvinden van uw apparaat en kan verhinderen dat uw gegevens in verkeerde handen vallen.

Hiervoor hoeft u alleen maar Anti-Theft te activeren op het apparaat. Als het nodig blijkt te zijn, kunt u vervolgens vanuit elke webbrowser toegang krijgen tot **Bitdefender Central**.

Opmerking
In de Antidiefstal-interface vindt u ook een link naar onze Bitdefender Central-app in de Google Play Store. Gebruik deze link om de app te downloaden indien u dat nog niet gedaan hebt.

Bitdefender Mobile Security biedt de volgende Antidiefstalfuncties:

Lokaliseren op afstand

Bekijk de huidige locatie van uw apparaat in Google Maps. De locatie wordt elke 5 seconden vernieuwd, dus u kunt deze volgen indien hij in beweging is.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als de GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie worden bepaald tot binnen tientallen meters als Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.

- Anders wordt de locatie bepaald met gebruikmaking van alleen gegevens van het mobiele netwerk, dat geen betere nauwkeurigheid dan enkele honderden meters kan bieden.

Vergrendelen op afstand

Vergrendel het scherm van uw apparaat en stel een numerieke pincode in, die moet worden ingevoerd om het scherm te ontgrendelen.

Wissen op afstand

U kunt alle persoonlijke gegevens op uw apparaat op afstand wissen als het apparaat niet langer in uw bezit is.

Waarschuwing naar apparaat sturen (Scream-functie)

U kunt op afstand een bericht op het scherm van het apparaat laten weergeven, of een luid geluidssignaal laten afspelen via de luidspreker van het apparaat.

Als het apparaat is zoekgeraakt, kunt u een bericht op het scherm van het apparaat weergeven, zodat de eerlijke vinder weet hoe hij of zij u kan bereiken.

En als u het apparaat niet kunt vinden, terwijl het misschien vlakbij is (bijvoorbeeld ergens in huis of op kantoor), kunt u een luid geluidssignaal laten klinken via de Scream-functie. Dit werkt ook als het apparaat in de stille modus staat.

3.5.1. Antidiefstal activeren

Om de Antidiefstalfuncties te activeren, voltooit u de configuratieprocedure vanaf de Antidiefstalkaart in het Dashboard.

In plaats hiervan kunt u Antidiefstal ook op deze manier activeren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Antidiefstal**.
3. Tik op **INSCHAKELEN**.
4. U kunt deze functie nu als volgt activeren:

Opmerking
In Android 6 zijn extra machtigingen vereist voor de functie Anti-Theft.

Volg deze stappen om dit in te schakelen:

a. Tik op **Antidiefstal activeren**, tik vervolgens op **INSCHAKELEN**.

b. Geef **Antivirus** toestemming om de locatie van uw apparaat te kennen.

a. **Beheerdersbevoegdheden toekennen**
Deze bevoegdheden zijn absoluut noodzakelijk om de Anti-Theft-module te kunnen gebruiken. U moet daarom beheerdersbevoegdheden toekennen voordat u verder kunt gaan.

b. **Pincode van de toepassing instellen**
Stel een pincode in om ongeoorloofde toegang tot uw apparaat te vermijden. Telkens er een poging wordt gedaan om uw apparaat te gebruiken, moet een pincode worden ingegeven. Voor apparaten die authenticatie via vingerafdruk ondersteunen, kan een bevestiging via vingerafdruk worden ingesteld in plaats van de pincode.
Dezelfde pincode wordt ook door App Lock gebruikt om uw geïnstalleerde apps te beschermen.

c. **Snap Photo activeren**
Telkens iemand het apparaat probeert te ontgrendelen terwijl Snapshot ingeschakeld is, en hier niet in slaagt, neemt Bitdefender een foto van die persoon.
Meer in detail: telkens wanneer de door u ingestelde pincode, het wachtwoord of de vingerafdruk drie keer na elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt samen met het tijdstempel en de reden opgeslagen. U kunt deze informatie opvragen door Bitdefender Mobile Security te openen en naar het scherm Antidiefstal te gaan.
Of u kunt de foto bekijken in uw Bitdefender-account.

i. Ga naar: https://central.bitdefender.com.

ii. Inloggen op uw account.

iii. Selecteer de **Mijn apparaten** paneel.

iv. Selecteer uw Android-apparaat en vervolgens het tabblad **Antidiefstal**.

v. Tik op ⋮ naast **Uw snapshots controleren** om de laatst gemaakte foto's te bekijken.
Alleen de twee recentste foto's worden opgeslagen.

Eens de functie Antidiefstal geactiveerd is, kunt u de Webbeheer-opdrachten vanuit het scherm Antidiefstal individueel in- of uitschakelen door op de bijbehorende opties te tikken.

3.5.2. De Antidiefstalfuncties gebruiken vanuit Bitdefender Central

> **Opmerking**
> Voor alle Anti-Theft-functies is het noodzakelijk dat de optie **Achtergrondgegevens** bij de gegevensgebruik-instellingen van uw apparaat is ingeschakeld.

Zo opent u de Anti-Theft-functies vanuit uw Bitdefender-account:

1. Ga naar **Bitdefender Central**.
2. Selecteer de **Mijn apparaten** paneel.
3. Selecteer in het venster **MIJN APPARATEN** de gewenste apparaatkaart door op de bijbehorende **Details weergeven** knop te tikken.
4. Selecteer het tabblad **Anti-Theft**.
5. Tik op de knop die overeenstemt met de functie die u wilt gebruiken:
   Lokaliseren - geef de locatie van uw apparaat weer in Google Maps.
   IP tonen - geeft het laatste IP-adres voor het geselecteerde apparaat weer.
   Waarschuwing - typ een bericht om op het scherm van uw apparaat te laten weergeven en/of laat het apparaat een geluidssignaal afspelen.
   Vergrendelen - uw toestel vergrendelen en een pincode instellen om het te ontgrendelen.
   Wissen - alle gegevens van uw apparaat verwijderen.

Belangrijk
Nadat u een apparaat hebt gewist, stoppen de functies van Antidiefstal.

3.5.3. Antidiefstalinstellingen.

Als u de opdrachten vanop afstand wilt in- of uitschakelen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Anti diefstal**.
3. Schakel de gewenste opties in of uit.

3.6. Accountprivacy

Bitdefender Account Privacy gaat na of er gegevensinbreuken hebben plaatsgevonden in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende toepassingen of websites. De gegevens die in een account opgeslagen zijn, kunnen wachtwoorden, kredietkaartinformatie of bankrekeninginformatie betreffen en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op uw privacy.

De privacystatus van een account wordt weergegeven na de validering.

Automatische nieuwe controles zijn geprogrammeerd om in de achtergrond uitgevoerd te worden, maar u kunt ook dagelijks manuele scans lanceren.

Telkens wanneer er nieuwe inbreuken worden ontdekt op gevalideerde e-mailaccounts, worden notificaties weergegeven.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Accountprivacy**.
3. Tik op **AAN DE SLAG**.
4. Het e-mailadres dat werd gebruikt om uw Bitdefender-account te maken, verschijnt, en wordt automatisch toegevoegd aan de lijst van gemonitorde accounts.

5. Om een andere account toe te voegen, tikt u in het venster Accountprivacy op **ACCOUNT TOEVOEGEN** en voert u het e-mailadres in.
   Tik op **TOEVOEGEN** om door te gaan.
   Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.
   Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer uw Ongewenste mail.
   De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts inbreuken worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.

Eens u een account die deel uitmaakte van een privacyschending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde inbreuken aan te duiden als Opgelost. Om dit te doen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Accountprivacy**.
3. Tik op de account die u net beveiligd hebt.
4. Tik op de inbreuk waarvoor u de account beveiligd hebt.
5. Tik op **OPGELOST** om te bevestigen dat de account beveiligd is.

Wanneer alle gedetecteerde inbreuken aangeduid zijn als **Opgelost**, wordt de account niet langer gemarkeerd als geschonden, tot er een nieuwe inbreuk wordt ontdekt.

Om geen notificaties meer te ontvangen telkens een automatische scan wordt uitgevoerd:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel de bijbehorende schakelaar in het gebied Accountprivacy uit.

3.7. App Lock

Bepaalde apps, bijvoorbeeld voor e-mail, foto's of berichten, bevatten persoonlijke informatie die u waarschijnlijk graag privé wilt houden. U kunt deze informatie beschermen door de toegang tot deze apps te beperken.

Via App Lock kunt u apps beveiligen met een speciale pincode, zodat onbevoegden deze apps niet meer kunnen gebruiken. U moet hiervoor een pincode van minimaal 4 en maximaal 8 cijfers instellen. Elke keer dat u een van de beveiligde apps wilt gebruiken, moet u deze pincode invoeren.

Biometrische verificatie (zoals vingerafdrukbevestiging of gezichtsherkenning) kan worden gebruikt in plaats van de geconfigureerde pincode.

3.7.1. App Lock activeren

Om de toegang tot bepaalde apps te beperken, configureert u App Lock vanaf de kaart die in het Dashboard wordt weergegeven nadat Antidiefstal is geactiveerd.

In plaats hiervan kunt u App Lock ook op deze manier activeren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **App Lock**.
3. Kraan **AANZETTEN**.
4. Toegang tot gebruikersgegevens toestaan voor Bitdefender Security.
5. Sta **Weergeven over andere toepassingen** toe.
6. Ga terug naar de app, configureer de toegangscode en tik op **Pincode instellen**.

   Opmerking
   Deze stap is alleen beschikbaar als u nog geen pincode voor Antidiefstal hebt ingesteld.

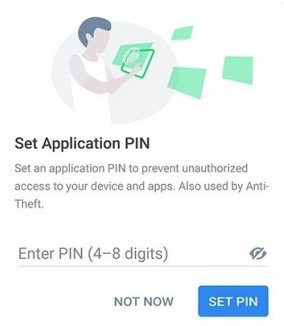
7. Gebruik de optie Snapshot om indringers te betrappen die proberen toegang te krijgen tot uw persoonlijke gegevens.

> **Opmerking**
> In Android 6 zijn extra machtigingen vereist voor de functie Snapshot. Om deze functie in te schakelen, moet u **Antivirus** toestemming geven om foto's te maken en video's op te nemen.

8. Selecteer welke toepassingen u wilt beschermen.

Als vijf keer achter elkaar een verkeerde pincode of vingerafdruk wordt gebruikt, wordt een time-out van 30 seconden gestart. Hierdoor wordt het vrijwel onmogelijk om in de beveiligde apps in te breken.

> **Opmerking**
> Dezelfde pincode wordt ook door Antidiefstal gebruikt.



3.7.2. Vergrendelmodus

De eerste keer dat u een toepassing aan App Lock toevoegt, verschijnt het venster App Lock Mode. Hier kunt u kiezen wanneer de functie App Lock de toepassingen op uw apparaat moet beschermen.

U kunt kiezen uit deze opties:

- **Telkens ontgrendelen** - telkens wanneer de vergrendelde toepassingen worden gebruikt, moet de pincode of vingerafdruk die u hebt ingesteld, worden gebruikt.
- **Ontgrendeld houden tot scherm uit** - de toepassingen zijn toegankelijk totdat het scherm wordt uitgeschakeld.
- **Vergrendelen na 30 seconden** - u kunt uw niet-vergrendelde toepassingen verlaten en binnen 30 seconden terug openen.

Als u de geselecteerde instelling wilt wijzigen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik in het gebied App Lock op **Telkens ontgrendelen**.
4. Kies de gewenste optie.

3.7.3. App Lock-instellingen

Voor een geavanceerde configuratie van App Lock:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.

In het gebied App Lock kunt u de volgende opties configureren:

- **Suggestie gevoelige toepassing** - ontvang een lock-notificatie telkens u een gevoelige toepassing installeert.
- **Telkens ontgrendelen** - kies een van de beschikbare vergrendelings- en ontgrendelingsopties.
- **Smart Unlock** - houdt toepassingen ontgrendeld wanneer u verbonden bent met vertrouwde wifinetwerken.
- V**Willekeurig toetsenbord** - voorkom PIN-aflezing door de posities van de getallen te randomiseren.

3.7.4. Snapshot

Met Bitdefender Snap Photo kunt u uw vrienden of familie op heterdaad betrappen. Zo kunt u hen een lesje leren, zodat ze niet langer nieuwsgierig uw persoonlijke bestanden doorlopen of de apps bekijken die u gebruikt.

Deze functie werkt heel eenvoudig: telkens wanneer de pincode of vingerafdruk drie keer achter elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt samen met het tijdstempel en de reden opgeslagen. U kunt deze informatie opvragen via de App Lock-functie van Bitdefender Mobile Security.

> **Opmerking**
> Deze functie is alleen beschikbaar op apparaten die aan de voorkant beschikken over een camera.

Om de functie Snapshot voor App Lock te configureren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel de bijbehorende schakelaar in het gebied Snapshot in.

De foto's die tijdens het invoeren van een incorrecte pincode worden gemaakt, worden in het venster App Lock weergegeven en kunnen in het volledige scherm worden bekeken.

U kunt de foto's ook bekijken in uw Bitdefender-account:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw account.
3. Selecteer het paneel **Mijn apparaten**.
4. Selecteer uw Android-apparaat en vervolgens het **Anti diefstal** tabblad.
5. Kraan naast **Controleer uw momentopnamen** om de laatste gemaakte foto's te bekijken.

Alleen de twee meest recente foto's worden opgeslagen.

Om de genomen foto's niet langer naar uw Bitdefender-account te uploaden:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel **Foto's uploaden** in het gebied Snapshot uit.

3.7.5. Smart Unlock

Met Smart Unlock kunt u heel eenvoudig voorkomen dat u elke keer een pincode of vingerafdrukscan nodig hebt voor de beveiligde apps.

U kunt bepaalde Wi-Fi-netwerken als 'vertrouwd' aanmerken, zodat de App Lock-blokkeringsinstellingen worden uitgeschakeld zolang u via een van deze netwerken verbonden bent met internet.

Zo configureert u de functie Smart Unlock:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Applicatie vergrendeling**.
3. Tik op de knop.

4. Tik op de schakelaar naast **Smart Unlock** indien de voorziening nog niet ingeschakeld is.
   Valideer aan de hand van uw vingerafdruk of uw pincode.
   Wanneer u de voorziening voor het eerst activeert, moet u de locatiemachtiging inschakelen. Tik op de knop **TOESTAAN** en klik vervolgens opnieuw op **TOESTAAN**.
5. Tik op **TOEVOEGEN** om de wifiverbinding die u momenteel gebruikt, als vertrouwd in te stellen.

Als u later van mening verandert, kunt u de functie weer uitschakelen. De vertrouwde Wi-Fi-netwerken worden dan niet langer vertrouwd.

3.8. Rapporten

De Rapporten-functie houdt een uitgebreid logboek bij van gebeurtenissen met betrekking tot de scanactiviteiten op uw apparaat.

Elke keer dat er iets gebeurt dat van belang is voor de beveiliging van het apparaat, wordt een nieuw bericht toegevoegd aan de rapporten.

Zo opent u de Rapporten:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Rapporten**.

Het venster Rapporten bevat de volgende tabbladen:

- **Weekrapporten** - hier kunt u de beveiligingsstatus en de uitgevoerde taken van de huidige en de vorige week bekijken. Elke zondag wordt het rapport van de afgelopen week gegenereerd. U krijgt bericht wanneer het weekrapport beschikbaar is.
  Elke week wordt hier een nieuwe tip weergegeven, dus kom hier regelmatig terug om uw app zo goed mogelijk te leren gebruiken.
  Om geen notificaties meer te ontvangen telkens een rapport werd gegenereerd:

  1. Kraan **Meer** op de onderste navigatiebalk.
  2. Kraan **Instellingen**.
  3. Schakel de schakelaar **Notificatie nieuw rapport** uit in het gebied Rapporten.

- **Activiteitenlogboek** - hier kunt u gedetailleerde informatie bekijken over de activiteiten van uw Bitdefender Mobile Security-app vanaf het moment van installatie op uw Android-apparaat.
  Om het beschikbare activiteitenlogboek te verwijderen:

  1. Kraan **Meer** op de onderste navigatiebalk.
  2. Kraan **Instellingen**.
  3. Tik op **Activiteitenlogboek wissen** en tik vervolgens op **WISSEN**.

3.9. WearON

Met Bitdefender WearON kunt u uw smartphone heel gemakkelijk terugvinden als u deze bent kwijtgeraakt, bijvoorbeeld op kantoor of thuis. Deze functie werkt ook als de stille modus van de telefoon actief is.

Zorg dat deze functie altijd ingeschakeld is, zodat u uw smartphone zo nodig gemakkelijk kunt terugvinden.

> **Opmerking**
> Deze functie werkt met Android 4.3 en Android Wear.

3.9.1. WearON activeren

Om WearON te gebruiken, koppelt u uw smartwatch aan Bitdefender Mobile Security en activeert u de WearON-functie met deze spraakopdracht:

Start:<Waar is mijn telefoon>

Bitdefender WearON heeft twee opdrachten:

1. **Phone Alert**
   De functie Phone Alert waarschuwt u als u te ver van uw smartphone verwijderd bent.
   Indien u uw smartwatch bij zich hebt, detecteert deze automatisch de toepassing op uw telefoon en trilt wanneer u te ver verwijderd bent van uw telefoon, en in het bijzonder wanneer de Bluetooth-verbinding wordt verbroken.
   U kunt deze functie als volgt inschakelen: open Bitdefender Mobile Security, tik in het menu op **Algemene instellingen** en activeer de schakelaar in het gedeelte WearON.

2. **Scream**
   Als uw telefoon toch is zoekgeraakt, kunt u vanaf uw smartwatch een Scream-opdracht naar de telefoon sturen om een luid geluidssignaal op de telefoon te laten klinken.

3.10. Info

Voor meer informatie over de Bitdefender Mobile Security-versie die u geïnstalleerd hebt, raadpleeg de Abonnementsovereenkomst en het Privacybeleid en bekijk de Open source-licenties.

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik op de gewenste optie in het gebied Over.

4. OVER BITDEFENDER CENTRAL

Bitdefender Central is het platform dat u toegang geeft tot de online functies en diensten van het product. Vanuit dit platform kunt u vanop afstand belangrijke taken uitvoeren op de apparaten waarop Bitdefender is geïnstalleerd. U kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan of rechtstreeks vanuit de Bitdefender Central-app op Android- en iOS-apparaten.

Om de Bitdefender Central-toepassing op uw apparaten te installeren:

- **Op Android** - zoek Bitdefender Central op Google Play en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.
- **Op iOS** - zoek Bitdefender Central in de App Store en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.

Zodra u aangemeld bent, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
  - De Bitdefender Windows-productlijn
  - Bitdefender Antivirus for Mac
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment ook bent.
- Bescherm de netwerktoestellen en hun gegevens tegen diefstal of verlies met Antidiefstal.

4.1. Toegang tot Bitdefender Central

Er zijn twee manieren om toegang te krijgen tot Bitdefender Central

- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar: https://central.bitdefender.com.
  3. Log in op uw account met uw e-mailadres en wachtwoord.
- Vanaf uw Android- of iOS-apparaat:
  Open de Bitdefender Central-app die u hebt geïnstalleerd.

  Opmerking
  Hierin zitten de opties die u ook in de webinterface vindt.

4.2. Twee-factorenauthenticatie

De twee-factorenauthenticatiemethode voegt een extra veiligheidslaag toe aan uw Bitdefender account, door een authenticatiecode te vragen bovenop uw aanmeldgegevens. Op deze manier voorkomt u dat uw account wordt overgenomen en houdt u types cyberaanvallen, zoals keyloggers, bruteforce- of woordenlijstaanvallen, af.

4.2.1. Twee-factorenauthenticatie activeren

Door de twee-factorenauthenticatie te activeren, maakt u uw Bitdefender account veel veiliger. Uw identiteit zal gecontroleerd worden telkens u zich aanmeldt via verschillende apparaten, hetzij om één van de Bitdefender producten te installeren, hetzij om de status van uw abonnement te controleren of vanop afstand taken uit te voeren op uw apparaten.

Om de twee-factorenauthenticatie te activeren:

1. Toegang Bitdefender Centraal.
2. Tik op het pictogram rechtsboven op het scherm.
3. Tik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Kraan **BEGIN**.
   Kies een van de volgende methodes:

- **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.
  Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.

  a. Tik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.

  b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.
  Om u aan te melden op een laptop of computer, kunt u de getoonde code manueel toevoegen.
  Tik op **VERDERGAAN**.

  c. Voer de code in die de app geeft of deze die weergegeven wordt in de vorige stap, en tik dan op **ACTIVEREN**.

- **E-mail** - telkens u zich aanmeldt in uw Bitdefender account, zal er een verificatiecode naar het Postvak-IN van uw e-mail worden gestuurd. Controleer de e-mail en gebruik dan de code die u ontving.

  a. Tik op **E-MAIL GEBRUIKEN** om te starten.

  b. Controleer uw e-mail en tik de verstrekte code in.
  Let erop dat u vijf minuten hebt om uw e-mailaccount te controleren en tik de gegenereerde code in. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

  c. Tik dan op **ACTIVEREN**.

  d. U krijgt tien activeringscodes. U kunt de lijst kopiëren, downloaden of afdrukken en deze gebruiken in het geval u uw e-mailadres verliest of u zich niet meer kunt aanmelden. Elke code kan slechts één keer gebruikt worden.

  e. Tik op **GEREED**.

In het geval u wilt stoppen met het gebruik van de twee-factorenauthenticatie:

1. Tik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.

2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.
   In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.
3. Bevestig uw keuze.

4.3. Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

1. Toegang Bitdefender Centraal.
2. Druk op pictogram in de rechterbovenhoek van het scherm.
3. Kraan **Bitdefender-account** in het diamenu.
4. Selecteer de **Wachtwoord en beveiliging** tabblad.
5. Tik op **Vertrouwde apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Tik op het gewenste apparaat.

U kunt zo veel apparaten toevoegen als u wilt, op voorwaarde dat Bitdefender erop geïnstalleerd is en uw abonnement geldig is.

4.4. Mijn apparaten

Vanaf **Mijn apparaten** in uw Bitdefender-account kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en die verbinding hebben met het internet. De apparaatkaarten geven de naam en de beveiligingsstatus van het apparaat weer en geven weer of er beveiligingsrisico's zijn die de bescherming van uw apparaten beïnvloeden.

4.4.1. Toevoeging van een nieuw apparaat

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Mobile Security erop installeren, als volgt:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en tik vervolgens op **INSTALLEER BESCHERMING**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
     Druk op **DOWNLOADKOPPELING VERZENDEN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadkoppeling is slechts 24 uur geldig. Indien de koppeling vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en tik vervolgens op de overeenkomstige downloadknop.
4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

4.4.2. Uw apparaten aanpassen

Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam aanpassen:

1. Toegang Bitdefender Centraal.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.

4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam apparaat** in en klik op **OPSLAAN**.

U kunt een eigenaar aanmaken en toekennen aan elk van uw apparaten, om het beheer te vergemakkelijken:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen** en vul de bijbehorende velden in. Pas het profiel aan: voeg een foto toe, selecteer een geboortedatum en voeg een e-mailadres en geboortedatum toe.
6. Klik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **TOEWIJZEN**.

4.4.3. Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Update**.

Voor meer acties van op afstand en informatie over uw Bitdefender-product op een specifiek toestel, klik op de gewenste toestelkaart.

Wanneer u op een apparaatkaart klikt, zijn de volgende tabbladen beschikbaar:

- **Dashboard.** In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en de Bitdefender VPN-status controleren en nakijken hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus is altijd groen (dan zijn er geen problemen voor uw apparaat), geel (dan moet

u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Wanneer er problemen zijn met uw apparaat, klik dan op het uitklappijltje in het bovenste statusgebied voor meer details. Hier kunt u

- **Bescherming.** In dit tabblad kunt u op afstand een snelle of systeemscan uitvoeren op uw apparaten. Klik op de knop **Scan** om de scan te starten. U kunt ook zien wanneer de laatste scan op het apparaat is uitgevoerd en er is een rapport beschikbaar met de belangrijkste gegevens van de laatste scan.
- **Optimalisatie.** Hier kunt u op afstand de prestaties van een apparaat verbeteren door snel te scannen, nutteloze bestanden te detecteren en op te schonen. Klik op de **START** knop, en selecteer vervolgens de gebieden die u wilt optimaliseren. Klik nogmaals op de knop **START** om het optimalisatieproces te starten. Klik op **Meer details** voor een gedetailleerd rapport over de opgeloste problemen.
- **Anti-diefstal.** In geval van misplaatsing, diefstal of verlies kunt u met de anti-diefstalfunctie uw apparaat lokaliseren en op afstand acties ondernemen. Klik op **LOKALISEREN** om de positie van het apparaat te achterhalen. De laatst bekende positie wordt weergegeven, samen met de tijd en datum.
- **Kwetsbaarheid.** Om een apparaat te controleren op kwetsbaarheden zoals ontbrekende Windows-updates, verouderde apps of zwakke wachtwoorden klikt u op de knop **SCANNEN** in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet op afstand worden verholpen. Als er een kwetsbaarheid wordt gevonden, moet u een nieuwe scan uitvoeren op het apparaat en vervolgens de aanbevolen acties ondernemen. Klik op **Meer details** voor een gedetailleerd rapport over de gevonden problemen.

4.5. Activiteit

In de Activiteitzone hebt u toegang tot informatie over de apparaten waar Bitdefender op geïnstalleerd is.

Wanneer u naar het **Activiteiten**-venster gaat, zijn de volgende kaarten beschikbaar:

- **Mijn apparaten.** Hier kunt u het aantal aangesloten apparaten en hun beschermingsstatus bekijken. Om problemen met de gedetecteerde

apparaten op afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **SCANNEN EN PROBLEMEN OPLOSSEN**.
Om details te zien over de gedetecteerde problemen, klikt u op **Problemen bekijken**.
Informatie over de gedetecteerde bedreigingen kan voor iOS-apparaten niet worden opgehaald.

- **Dreigingen geblokkeerd.** Hier ziet u een grafiek met de algemene statistieken, met inbegrip van informatie over de bedreigingen die de voorbije 24 uur en 7 dagen werden geblokkeerd. De weergegeven informatie wordt opgehaald naargelang het schadelijke gedrag dat in de bestanden, toepassingen en url's werd gedetecteerd.
- **Topgebruikers met geblokkeerde bedreigingen.** Hier ziet u de gebruikers waarbij de meeste bedreigingen werden gevonden.
- **Topapparaten met geblokkeerde bedreigingen.** Hier ziet u de apparaten waarop de meeste bedreigingen werden gevonden.

4.6. Mijn abonnementen

Via het Bitdefender Central-platform beheert u heel eenvoudig de abonnementen die u voor uw apparaten hebt aangeschaft.

4.6.1. Controleer beschikbare abonnementen

Zo controleert u uw beschikbare abonnementen:

1. Toegang Bitdefender Centraal.
2. Ga naar het paneel **Mijn abonnementen**.

Hier vindt u informatie over de beschikbaarheid van uw abonnementen en het aantal apparaten dat gebruikmaakt van deze abonnementen.

U kunt een nieuw apparaat aan een abonnement toevoegen of een abonnement verlengen door een abonnementskaart te selecteren.

> **Opmerking**
> U kunt een of meer lidmaatschappen op uw account hebben, op voorwaarde dat ze voor verschillende platforms bestemd zijn (Windows, macOS, iOS of Android).

4.6.2. Abonnement activeren

U kunt een abonnement tijdens het installatieproces activeren via uw Bitdefender-account. De geldigheidsduur van het abonnement begint te lopen vanaf het moment van activering.

Als u een activeringscode hebt ontvangen van een van onze leveranciers, of als u een activeringscode cadeau hebt gekregen, kunt u deze toevoegen aan uw Bitdefender-abonnement.

Volg de onderstaande stappen om een abonnement te activeren met behulp van een activeringscode:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **ACTIVEREN** om door te gaan.

Het abonnement is nu geactiveerd.

4.6.3. Abonnement verlengen

Indien u automatische verlenging voor uw Bitdefender-abonnement hebt uitgeschakeld, kunt u het handmatig verlengen via de volgende stappen:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Selecteer de gewenste abonnementskaart.
4. Klik op **VERLENGEN** om door te gaan.

In uw webbrowser wordt een webpagina geopend waar u uw Bitdefender-abonnement kunt verlengen.

4.7. Meldingen

Om u op de hoogte te houden van wat er gebeurt op de apparaten die aan uw account gekoppeld zijn, hebt u de -icoon ter beschikking. Zodra u erop klikt, krijgt u een algemeen beeld met informatie over de activiteit van de Bitdefender-producten die op uw apparaten geïnstalleerd zijn.

5. VEELGESTELDE VRAGEN

Waarom is er voor Bitdefender Mobile Security een internetverbinding nodig?

De applicatie moet met Bitdefender-servers communiceren om te kunnen bepalen of de geïnstalleerde applicaties en de bezochte webpagina's wel veilig zijn, en ook om opdrachten vanaf uw Bitdefender-account te kunnen ontvangen wanneer u de Anti-Theft-functies gebruikt.

Waar heeft Bitdefender Mobile Security elke toestemming voor nodig?

- Internettoegang -> nodig voor communicatie met de cloud.
- Telefoonstatus en -identiteit lezen -> wordt gebruikt om te bepalen of het apparaat verbonden is met internet en om bepaalde apparaatinformatie op te vragen, waarmee een unieke ID kan worden samengesteld voor de communicatie met de Bitdefender-cloud.
- Browserfavorieten lezen en schrijven -> de module Webbeveiliging verwijdert schadelijke websites uit uw browsergeschiedenis.
- Loggegevens lezen -> Bitdefender Mobile Security detecteert sporen van dreigingsactiviteiten in de Android-logboeken.
- Locatie -> nodig voor lokalisatie op afstand.
- Camera -> nodig voor Snapshot.
- Opslag -> nodig om de Malwarescanner ook de SD-kaart te laten scannen.

Hoe dien ik niet langer informatie in bij Bitdefender over verdachte toepassingen?

Bitdefender Mobile Security stuurt standaard rapporten naar de Bitdefender-servers over verdachte toepassingen die u installeert. Deze informatie is van essentieel belang voor de verbetering van de detectie van dreigingen en kan ons helpen om u in de toekomst een betere ervaring te bieden. Voor het geval u wilt stoppen met het ons toesturen van informatie over verdachte apps:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel **In-de-cloud-detectie** in het gebied Malwarescanner uit.

Waar zie ik de details over de activiteit van de toepassing?

Bitdefender Mobile Security houdt een logboek bij van alle belangrijke acties, statuswijzigingen en andere kritische boodschappen die gelinkt zijn aan de activiteiten. Om de activiteiten van de toepassing te bekijken:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **rapporten**.
   In het venster WEKELIJKSE RAPPORTEN kunt u de rapporten bekijken die wekelijks worden opgesteld en in het venster ACTIVITEITENLOGBOEK ziet u de informatie over de activiteiten van uw Bitdefender-toepassing.

Ik ben de pincode vergeten waarmee ik mijn app heb beveiligd. Wat moet ik doen?

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. De pincode wordt weergegeven in het veld **Applicatiepincode**.

Hoe kan ik de pincode die ik heb ingesteld voor App Lock en Antidiefstal wijzigen?

Als u de pincode die u ingesteld hebt voor App Lock of Antidiefstal wilt wijzigen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik in het gebied Antidiefstal op Beveiliging **PINCODE**.
4. Voer de huidige pincode in.
5. Voer de nieuwe pincode in die u wilt configureren.

Hoe kan ik App Lock uitzetten?

U kunt de App Lock-functie als zodanig niet uitzetten, maar u kunt de functie wel heel eenvoudig uitschakelen door de selectievakjes naast alle geselecteerde apps leeg te maken. (Hiervoor hebt u uw pincode of vingerafdruk nodig.).

Hoe kan ik een ander draadloos netwerk instellen als vertrouwd netwerk?

Eerst moet u uw apparaat verbinden met het draadloze netwerk dat u als vertrouwd hebt ingesteld. Volg vervolgens deze stappen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Applicatie vergrendeling**.
3. Tik op in de rechterbovenhoek.
4. Tik naast het netwerk dat u als vertrouwd wilt instellen, op **TOEVOEGEN**.

Hoe kan ik de snapshots die op mijn apparaten genomen zijn, niet meer zien?

Om de op uw apparaten gemaakte fotosnaps niet langer zichtbaar te maken:

1. Toegang Bitdefender Centraal.
2. Tik op rechtsboven op het scherm.
3. Tik op **Instellingen** in het schuifmenu.
4. Deactiveer de optie **Snapshots die met uw apparaten zijn gemaakt, tonen/niet tonen**.

Hoe kan ik veilig online blijven winkelen?

Online winkelen gaat gepaard met hoge risico's als u enkele details over het hoofd ziet. Om niet het slachtoffer te worden van fraude, bevelen wij u het volgende aan:

- Houd uw beveiligingsapp up to date.
- Voer enkel online betalingen met kopersbescherming uit.
- Gebruik een VPN wanneer u een verbinding maakt met het internet via openbare en onbeveiligde draadloze netwerken.
- Wees aandachtig voor de wachtwoorden die u hebt toegekend aan uw online accounts. Ze moeten sterk zijn, met hoofdletters en kleine letters, cijfers en symbolen (@, !, %, #, etc.).
- Zorg ervoor dat de informatie die u verzendt, via veilige verbindingen gaat. De online website-extensies moet HTTPS://, zijn, niet HTTP//.

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om te verzekeren dat u veilig bent wanneer u surft op het web, raden we aan dat u Bitdefender VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Zal Bitdefender VPN een negatief effect hebben op de batterij van mijn apparaat?

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom is het internet soms trager wanneer ik verbonden ben met Bitdefender VPN?

Bitdefender VPN is ontworpen om u een aangename ervaring te bieden tijdens het surfen. Uw internetconnectiviteit of de afstand met de server waarmee u verbonden bent, kan echter zorgen voor vertraging. In dat geval, indien het niet noodzakelijk is om te verbinden met een server die veraf gehost wordt (bijv. van China naar de VS), raden we aan Bitdefender VPN toe te staan om u automatisch te verbinden met de dichtstbijzijnde server, of een server te vinden die dichter bij uw huidige locatie gelegen is.

Kan ik het Bitdefender-account dat aan mijn apparaat is gekoppeld wijzigen?

Ja, u kunt als volgt wijzigen welke Bitdefender-account aan uw apparaat is gekoppeld:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op uw e-mailadres.
3. Tik op **Uitloggen van account**. Is er een pincode geconfigureerd, wordt u gevraagd deze in te voeren.

4. Bevestig uw keuze.
5. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in en tik dan op **AANMELDEN**.

Hoe beïnvloedt Bitdefender Mobile Security de prestaties van mijn apparaat en de autonomie van de batterij?

We hebben dit effect tot een minimum beperkt. De toepassing wordt enkel uitgevoerd wanneer dit van essentieel belang is - nadat u een toepassing installeert, wanneer u de interface van de toepassing gebruikt of wanneer u een beveiligingscontrole wenst. Bitdefender Mobile Security is niet op de achtergrond actief wanneer u telefoongesprekken voert, een sms-bericht invoert of een spel speelt.

Wat is apparaatbeheerder?

Apparaatbeheerder is een Android-functie die Bitdefender Mobile Security de benodigde bevoegdheden geeft om bepaalde taken op afstand te kunnen uitvoeren. Zonder deze bevoegdheden zou vergrendeling op afstand niet werken en zouden niet alle gegevens op afstand kunnen worden gewist. Als u de app wilt verwijderen, moet u eerst deze machtigingen intrekken via **Instellingen > Beveiliging > Apparaatbeheerders kiezen**.

Hoe de fout "Geen Google-token" oplossen die verschijnt bij het aanmelden bij Bitdefender Mobile Security.

Deze fout treedt op als het apparaat niet aan een Google-account is gekoppeld of als het apparaat wel aan een account is gekoppeld, maar er vanwege een tijdelijk probleem geen verbinding met Google gemaakt kan worden. Probeer een van de volgende oplossingen:

- Ga naar Android Instellingen > Applicaties > Applicatiebeheer > Bitdefender Mobile Security en tik op **Gegevens wissen**. Probeer vervolgens opnieuw in te loggen.
- Controleer of uw apparaat is gekoppeld aan een Google-account.
  Dit kunt u als volgt controleren: ga naar Instellingen > Accounts & synchronisatie en kijk of er een Google-account wordt weergegeven onder **Accounts beheren**. Voeg uw account toe als er geen account wordt weergegeven, start het apparaat opnieuw op en probeer opnieuw in te loggen op Bitdefender Mobile Security.
- Start het apparaat opnieuw op en probeer opnieuw in te loggen.

In welke talen is Bitdefender Mobile Security beschikbaar?

Bitdefender Mobile Security is momenteel beschikbaar in de volgende talen:

- Braziliaans
- Tsjechisch
- Nederlands
- Engels
- Frans
- Duits
- Grieks
- Hongaars
- Italiaans
- Japans
- Koreaans
- Pools
- Portugees
- Roemeens
- Russisch
- Spaans
- Zweeds
- Thais
- Turks
- Vietnamees

In de toekomst komen nog meer talen beschikbaar. Om de taal voor de interface van Bitdefender Mobile Security te wijzigen, gaat u naar de instellingen voor **Taal en toetsenbord** van uw apparaat en kiest u de gewenste taal.

6. HULP VRAGEN

6.1. 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.

6.2. 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.

6.2.1. 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/.

6.2.2. 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/

6.2.3. 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/.

6.3. 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/

6.3.1. 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.