

Bitdefender[®] MOBILE SECURITY



BENUTZERHANDBUCH





Bitdefender Mobile Security Benutzerhandbuch

Veröffentlicht 19.07.2020

Copyright© 2020 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation ist urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „wie besehen“ zur Verfügung gestellt und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere Webseiten, die nicht von Bitdefender erstellt wurden, und auch nicht von ihr kontrolliert werden können. Somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. Bitdefender stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass Bitdefender in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.



Inhaltsverzeichnis

1. Sicherheitsfunktionen	1
2. Erste Schritte	2
3. Virens Scanner	7
4. Internet-Schutz	10
5. VPN	12
6. Diebstahlschutz-Funktionen	16
7. Kontoschutz	21
8. App-Sperre	23
9. Berichte	28
10. WearON	29
11. Info über	30
12. Bitdefender Central	31
13. Häufig gestellte Fragen	38
14. Hilfe erhalten	44



1. SICHERHEITSFUNKTIONEN

Bitdefender Mobile Security schützt Ihr Android-Gerät mit den folgenden Funktionen:

- Virens Scanner
- Internet-Schutz
- VPN
- Diebstahlschutz:
 - Fern-Gerätortung
 - Fern-Gerätesperrung
 - Fern-Gerätelöschung
 - Fern-Tonsignale
- Kontoschutz
- App-Sperre
- Berichte
- WearON

Sie können die Produktfunktionen 14 Tage lang kostenlos verwenden. Nach Ablauf dieses Zeitraums müssen Sie die Vollversion erwerben, um Ihr Mobilgerät zu schützen.



2. ERSTE SCHRITTE

Systemanforderungen

Bitdefender Mobile Security läuft auf allen Geräten ab Android 4.1. Für den Bedrohungs-Scan über die Cloud wird eine aktive Internet-Verbindung benötigt.

Installation von Bitdefender Mobile Security

● Über Bitdefender Central

● Android

1. Gehen Sie zu: <https://central.bitdefender.com>.
2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
3. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
4. Tippen Sie auf **SCHUTZ INSTALLIEREN**, und danach auf **Dieses Gerät schützen**.
5. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
6. Sie werden zur **Google Play**-App weitergeleitet. Tippen Sie in Google Play auf Installieren.

● Auf Windows, macOS, iOS

1. Gehen Sie zu: <https://central.bitdefender.com>.
2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
3. Tippen Sie oben links auf das  und wählen Sie danach **Meine Geräte** aus.
4. Tippen Sie auf **SCHUTZ INSTALLIEREN**, und danach auf **Andere Geräte schützen**.
5. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, drücken Sie auf die entsprechende Schaltfläche.
6. Tippen Sie auf **DOWNLOAD-LINK SENDEN**.



7. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie auf **E-MAIL VERSENDEN**. Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
8. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und tippen Sie in der E-Mail auf die Download-Schaltfläche.

● Über Google Play

Suchen Sie nach Bitdefender Mobile Security, um die App zu finden und zu installieren.

Sie können auch den QR-Code einscannen:



QR-Code

Bevor Sie die Bestätigungsschritte abschließen können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google-, Apple- oder Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.



Wenn Sie Bitdefender Mobile Security über Ihr Bitdefender-Konto installiert haben, wird die App automatisch versuchen, sich bei diesem Konto anzumelden.

So können Sie Ihr Gerät mit einem Bitdefender-Konto verknüpfen:

1. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Konto in die entsprechenden Felder ein. Falls Sie noch kein Bitdefender-Konto haben und jetzt eines anlegen möchten, klicken Sie auf den entsprechenden Link.
2. Tippen Sie auf **ANMELDEN**.

Tippen Sie zur Anmeldung mit einem Facebook-, Google- oder Microsoft-Konto im Bereich **Oder melden Sie sich an über** auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet. Befolgen Sie die Anweisungen zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security.



Beachten Sie

Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

Schutz konfigurieren

Nach der erfolgreichen Anmeldung in der App wird das Fenster **Schutz konfigurieren** angezeigt. Um Ihr Gerät zu schützen, sollten Sie die folgende Anleitung befolgen:

- **Abonnementstatus.** Um mit Bitdefender Mobile Security umfassend geschützt zu sein, müssen Sie Ihr Produkt zunächst mit einem Abonnement aktivieren. Dieses legt fest, wie lange Sie das Produkt nutzen können. Nach Ablauf des Abonnements wird die Anwendung nicht mehr funktionieren und Ihr Gerät nicht mehr schützen.

Wenn Sie einen Aktivierungscode haben, tippen Sie auf **ICH HABE EINEN CODE** und danach auf **AKTIVIEREN**.

Falls Sie sich mit einem neuen Bitdefender-Benutzerkonto angemeldet haben und über keinen Aktivierungscode verfügen, können Sie das Produkt 14 Tage kostenlos testen.

- **Internet-Schutz.** Falls Ihr Gerät zur Aktivierung des Internet-Schutzes die Eingabehilfe-Option benötigt, tippen Sie auf **AKTIVIEREN**. Sie werden zum



Menü für die Eingabehilfe weitergeleitet. Tippen Sie auf Bitdefender Mobile Security, und aktivieren Sie den entsprechenden Schalter.

- **Virens Scanner.** Führen Sie einen einmaligen Scan durch, um sicherzustellen, dass auf Ihrem Gerät keine Bedrohungen vorliegen. Tippen Sie zum Start des Scan-Vorgangs auf **JETZT SCANNEN**.

Mit Beginn des Scan-Vorgangs wird das Dashboard angezeigt. Hier können Sie den Sicherheitsstatus Ihres Geräts einsehen.

Dashboard

Tippen Sie im App-Depot Ihres Geräts auf das Symbol für Bitdefender Mobile Security, um die Anwendungsoberfläche anzuzeigen.

Im Dashboard finden Sie Informationen zum Sicherheitsstatus Ihres Geräts. Hier unterstützt Sie auch der Autopilot bei der Verbesserung Ihrer Gerätesicherheit, indem er Ihnen Empfehlungen zu den einzelnen Funktionen anzeigt.

Die Statuskarte oben im Fenster informiert Sie mit eindeutigen Meldungen und auffälligen Farben über den Sicherheitsstatus Ihres Geräts. Liegen in Bitdefender Mobile Security keine Warnmeldungen vor, ist die Statuskarte grün. Wurde ein Sicherheitsproblem gefunden, wechselt die Farbe der Statuskarte nach rot.

Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der **Bitdefender-Autopilot** als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen, der Bitdefender-Autopilot liefert Ihnen kontextabhängige Empfehlungen, die sich an Ihrer Gerätenutzung und an Ihren Anforderungen orientieren. So lernen Sie alle Vorteile der Funktionen in Ihrer Bitdefender Mobile Security-App kennen und können umfassend davon profitieren.

Wenn ein Prozess ausgeführt wird oder eine Funktion Ihre Aufmerksamkeit erfordert, wird eine Kachel mit weiteren Informationen und möglichen Aktionen im Dashboard angezeigt.

Sie können auf die Funktionen von Bitdefender Mobile Security zugreifen und einfach über die untere Navigationsleiste navigieren:

Virens Scanner

Hiermit können Sie Bedarf-Scans starten oder Speicher-Scans aktivieren. Weitere Informationen finden Sie unter „**Virens Scanner**“ (S. 7).



Internet-Schutz

Lässt Sie sicher im Web surfen, indem er Sie vor potenziell schädlichen Seiten warnt. Weitere Informationen finden Sie unter „**Internet-Schutz**“ (S. 10).

VPN

Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter „**VPN**“ (S. 12).

Diebstahlschutz

Hiermit können Sie die Diebstahlschutzfunktionen aktivieren und deaktivieren und die Einstellungen für den Diebstahlschutz konfigurieren. Weitere Informationen finden Sie unter „**Diebstahlschutz-Funktionen**“ (S. 16).

Kontoschutz

Prüft, ob die Datensicherheit Ihrer Online-Konten kompromittiert wurde. Weitere Informationen finden Sie unter „**Kontoschutz**“ (S. 21).

App-Sperre

Hiermit können Sie Ihre installierten Anwendungen durch Festlegung einer PIN für den Zugriff schützen. Weitere Informationen finden Sie unter „**App-Sperre**“ (S. 23).

Berichte

Führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten im Zusammenhang mit den Aktivitäten Ihres Geräts. Weitere Informationen finden Sie unter „**Berichte**“ (S. 28).

WearON

Kommuniziert mit Ihrer Smartwatch, damit Sie Ihr Telefon schneller wiederfinden können. Weitere Informationen finden Sie unter „**WearON**“ (S. 29).



3. VIRENSCANNER

Bitdefender schützt Ihr Gerät und Ihre Daten mit Scans während der Installation und bei Bedarf vor schädlichen Anwendungen.

In der Benutzeroberfläche des Virenschanners finden Sie eine Liste aller Bedrohungstypen, nach denen Bitdefender sucht, einschließlich ihrer Definition. Tippen Sie auf die jeweilige Bedrohung, um die Definition anzuzeigen.



Beachten Sie

Stellen Sie sicher, dass Ihr Mobilgerät mit dem Internet verbunden ist. Sollte keine Internet-Verbindung bestehen, wird der Scan-Vorgang nicht gestartet.

● Installations-Scans

Bitdefender Mobile Security scannt automatisch all neu installierten Anwendungen mithilfe der Cloud-Technologie. Der gleiche Scan-Vorgang wird bei jedem Update einer installierten App wiederholt.

Wenn die Anwendung als schädlich eingestuft wird, wird eine Aufforderung angezeigt, die Anwendung zu deinstallieren. Tippen Sie auf **Deinstallieren**, um zum Deinstallationsbildschirm der Anwendung zu gelangen.

● On-Demand Prüfung

Wenn Sie einmal unsicher sein sollten, ob eine Anwendung auf Ihrem Gerät sicher ist, können Sie einen Bedarf-Scan starten.

So können Sie einen Bedarf-Scan starten:

1. Tippen Sie in der unteren Navigationsleiste auf  **Virenschanner**.
2. Tippen Sie auf **SCAN STARTEN**.



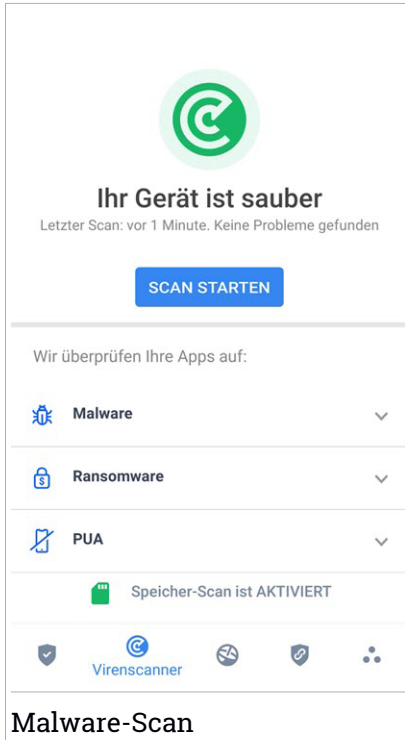
Beachten Sie

Für den Virenschanner werden unter Android 6 zusätzliche Berechtigungen benötigt. Tippen Sie auf **SCAN STARTEN** und wählen Sie danach **Zulassen** für folgende Anfragen aus:

- Zulassen, dass der **Virenschutz** Anrufe tätigt und verwaltet?
- Zulassen, dass der **Virenschutz** auf Fotos, Medien und Dateien auf Ihrem Gerät zugreift?



Der Scan-Fortschritt wird angezeigt. Sie können den Vorgang jederzeit abbrechen.



Malware-Scan

Bitdefender Mobile Security scannt standardmäßig den internen Speicher Ihres Gerätes sowie vorhandene SD-Karten. So können gefährliche Anwendungen, die sich auf der Karte befinden könnten, erkannt werden, bevor Sie Schaden anrichten können.

So können Sie die Einstellung Speicher prüfen deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Deaktivieren Sie im Bereich Virens Scanner den Schalter **Speicher prüfen**.



Wird eine schädliche Anwendung gefunden, werden entsprechende Informationen zu dieser Anwendung angezeigt. Tippen Sie auf **DEINSTALLIEREN**, um sie zu entfernen.

Die Virens Scanner-Kachel zeigt den Status Ihres Geräts an. Ein grüne Kachel zeigt, dass Ihr Gerät geschützt ist. Ein rote Kachel bedeutet, dass ein Scan durchgeführt werden muss oder Ihre Aufmerksamkeit gefordert ist.

Wenn Sie über ein Gerät mit Android Version 7.1 oder höher verfügen, können Sie über einen Kurzbefehl auf den Virens Scanner zugreifen und eine Virensuche schnell starten, ohne Bitdefender Mobile Security zu öffnen. Halten Sie einfach das Symbol Bitdefender auf Ihrem Startbildschirm oder in Ihrem App-Drawer, und wählen Sie dann das Symbol für .



4. INTERNET-SCHUTZ

Der Surfschutz nutzt die Bitdefender-Cloud-Dienste, um die von Ihnen im Standard-Android-Browser, in Google Chrome, Firefox, Opera, Opera Mini, Edge, Samsung Internet und Dolphin. Im Bereich Surfschutz finden Sie eine Liste mit allen unterstützten Browsern.



Beachten Sie

Für den Surfschutz werden unter Android 6 zusätzliche Berechtigungen benötigt.

Erteilen Sie die Erlaubnis zur Registrierung als Accessibility-Dienst und tippen Sie nach Aufforderung auf **AKTIVIEREN**. Tippen Sie auf **Antivirus** und aktivieren Sie den Schalter. Bestätigen Sie anschließend, dass Sie dem Zugriff auf die Berechtigungen Ihre Geräts zustimmen.

Der Bitdefender-Internet-Schutz ist so konfiguriert, dass Sie bei jedem Aufruf einer Bank-Website zur Verwendung von Bitdefender VPN aufgefordert werden. Die Benachrichtigung wird in der Statusleiste angezeigt. Wir empfehlen Ihnen, Bitdefender VPN zu verwenden, während Sie in Ihr Bankkonto eingeloggt sind, damit Ihre Daten vor möglichen Sicherheitsverletzungen geschützt sind.

So können Sie die Benachrichtigung durch den Internet-Schutz deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Internet-Schutz.





Internet-Schutz ist AN

Sie sind vor gefährlichen Seiten geschützt

[DEAKTIVIEREN](#)

Geschützte Browser

Nutzen Sie einen dieser Browser, um sich zu schützen



Chrome
Installiert

[OFFEN](#)



Dolphin



Firefox



[Internet-Schutz](#)

Internet-Schutz



5. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie unglückliche Situationen wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.



Beachten Sie

In einigen Ländern wird das Internet zensiert, weshalb der Einsatz von VPN dort gesetzlich nicht erlaubt ist. Um rechtliche Folgen vorzubeugen, kann es sein, dass eine Warnmeldung angezeigt wird, wenn Sie zum ersten Mal versuchen, die VPN-Funktion von Bitdefender zu verwenden. Wenn Sie die Funktion dann verwenden, bestätigen Sie damit, dass Sie die relevanten Bestimmungen Ihres Landes kennen und sich der entsprechenden Risiken bewusst sind.

Sie haben zwei Optionen zur Aktivierung oder Deaktivierung von Bitdefender VPN:

- Tippen Sie in der VPN-Kachel des Dashboards auf **VERBINDEN**.

Der Status von Bitdefender VPN wird angezeigt.

- Tippen Sie in der unteren Navigationsleiste auf  **VPN** und dann auf **VERBINDEN**.

Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.

Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.



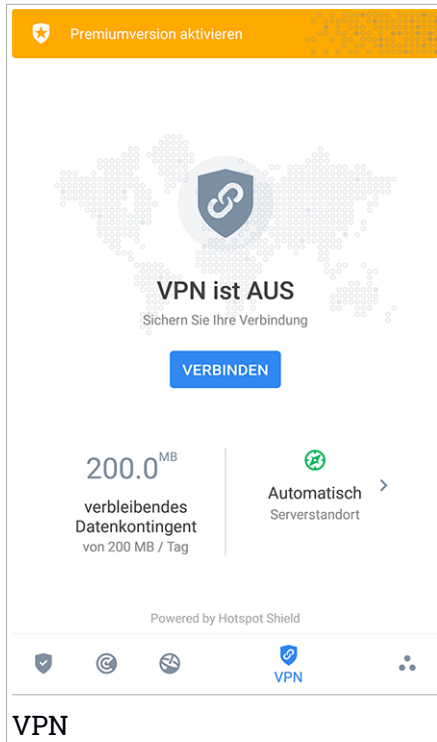
Beachten Sie

Wenn Sie VPN das erste Mal einschalten, werden Sie gebeten, Bitdefender zu erlauben, eine VPN-Verbindung herzustellen, die den Netzwerkdatenverkehr überwacht. Tippen Sie auf **OK** um fortzufahren.

Wenn Sie über ein Gerät mit Android Version 7.1 oder höher verfügen, können Sie über einen Kurzbefehl auf Bitdefender VPN zugreifen, ohne Bitdefender Mobile Security zu öffnen. Halten Sie einfach das Symbol für Bitdefender auf Ihrem Startbildschirm oder in Ihrem App-Drawer, und wählen Sie dann das Symbol für .

Um Ihren Akku zu schonen, empfehlen wir Ihnen, die VPN-Funktion zu deaktivieren, wenn Sie sie nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Funktion auf **Serverstandort** und wählen Sie den gewünschten Standort aus. Weitere Details zu den VPN-Abonnements finden Sie unter „**Abonnements**“ (S. 15).



VPN-Einstellungen

Für eine erweiterte Konfiguration Ihres VPN:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.

Im VPN-Bereich können Sie die folgenden Optionen konfigurieren:

- **VPN-Schnellzugriff** – eine Benachrichtigung wird in der Statusleiste Ihres Geräts angezeigt, über die Sie das VPN schnell aktivieren können.
- **Warnung bei offenen WLAN-Netzwerken** - Jedes Mal, wenn Sie sich mit einem offenen WLAN-Netzwerk verbinden, werden Sie in der Statusleiste Ihres Geräts zur Verwendung des VPN aufgefordert.



Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie im Dashboard auf **Premium aktivieren** bzw. in der VPN-Benutzeroberfläche **Premiumversion aktivieren** tippen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem Bitdefender Mobile Security-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen, unabhängig von Status Ihres Sicherheitsabonnements. Wenn Ihr Bitdefender Premium-VPN-Abonnement abläuft, Ihr Bitdefender Mobile Security-Abonnement aber weiterhin aktiv ist, kehren Sie zum kostenlosen Angebot zurück.

Bitdefender VPN ist plattformunabhängig und in den Windows-, macOS-, Android- und iOS-Produkten von Bitdefender verfügbar. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.



6. DIEBSTAHLSCHUTZ-FUNKTIONEN

Bitdefender kann Ihnen dabei helfen, Ihr Gerät zu finden, und verhindert, dass Ihre privaten Daten in die falschen Hände gelangen.

Sie müssen nur den Diebstahlschutz über das Gerät aktivieren und können dann bei Bedarf jederzeit und mit jedem Browser auf **Bitdefender Central** zugreifen.



Beachten Sie

In der Oberfläche des Diebstahlschutzes finden Sie auch einen Link zu unserer Bitdefender Central-App im Google Play Store. Über diesen Link können Sie die App herunterladen, falls Sie dies noch nicht getan haben.

Bitdefender Mobile Security bietet die folgenden Diebstahlschutzfunktionen:

Fernortung

Hiermit können Sie den Standort Ihres Geräts in Google Maps anzeigen. Der Standort wird alle 5 Sekunden aktualisiert, eine Bewegung kann also nachverfolgt werden.

Die Genauigkeit der Ortung hängt davon ab, wie gut Bitdefender seinen Standort bestimmen kann:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.
- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.
- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.

Fernsperrung

Frieren Sie den Bildschirm Ihres Geräts ein, und legen Sie eine PIN fest, mit der er wieder aktiviert werden kann.

Fernlöschung

Löschen Sie alle persönlichen Daten von Ihrem Gerät.



Signal an das Gerät senden (Aufschrei)

Sie können aus der Ferne eine Nachricht an das Gerät senden, die auf dem Bildschirm angezeigt wird, oder ein lautes Tonsignal über die Lautsprecher abspielen lassen.

Wenn Sie Ihr Gerät verlieren, können Sie den potenziellen Finder wissen lassen, wie er es Ihnen zukommen lassen kann, indem Sie auf dem Bildschirm des Geräts eine Nachricht anzeigen lassen.

Wenn Sie Ihr Gerät verlegt haben, liegt es mit einiger Wahrscheinlichkeit ganz in der Nähe (in der Wohnung oder im Büro). Sie finden es ganz leicht, indem Sie es einen lauten Ton abspielen lassen. Der Ton wird abgespielt, auch wenn das Gerät auf lautlos gestellt ist.

Aktivierung des Diebstahlschutzes

Zur Aktivierung der Diebstahlschutzfunktionen müssen Sie nur den Konfigurationsvorgang über die Diebstahlschutz-Kachel im Dashboard abschließen.

Alternativ können Sie den Diebstahlschutz folgendermaßen aktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Diebstahlschutz**.
3. Tippen Sie auf **AKTIVIEREN**.
4. Der folgende Prozess wird eingeleitet, um Sie bei der Aktivierung dieser Funktion zu unterstützen:



Beachten Sie

Für den Diebstahlschutz werden unter Android 6 zusätzliche Berechtigungen benötigt. Um sie zu aktivieren, gehen Sie folgendermaßen vor:

- a. Tippen Sie zunächst auf **Diebstahlschutz aktivieren** und danach auf **AKTIVIEREN**.
 - b. Erteilen Sie dem **Virenschutz** die Berechtigung, auf Ihren Gerätestandort zuzugreifen.
- a. **Administratorrechte erteilen**
- Diese Rechte sind für den Betrieb des Diebstahlschutz unbedingt erforderlich und müssen eingeräumt werden, um diesen Vorgang fortzusetzen.



b. Anwendungs-PIN festlegen

Um einen unbefugten Zugriff auf Ihr Gerät zu verhindern, muss ein PIN-Code festgelegt werden, der bei jedem Zugriffsversuch auf Ihr Gerät zunächst eingegeben werden muss. Bei Geräten, die die Fingerabdruckererkennung unterstützen, kann anstelle des festgelegten PIN-Codes auch die Bestätigung per Fingerabdruck verwendet werden.

Die gleiche PIN wird von der App-Sperre verwendet, um Ihre installierten Anwendungen zu schützen.

c. Foto aufnehmen aktivieren

Ist Foto aufnehmen aktiviert, wird Bitdefender bei jedem erfolglosen Zugriffsversuch ein Foto der betreffenden Person aufnehmen.

Im Detail heißt das: Wird dreimal hintereinander die falsche PIN, das falsche Passwort oder der falsche Fingerabdruck eingegeben, wird mit der Frontkamera ein Foto aufgenommen. Das Foto wird dann mit Zeitstempel und einem Hinweis auf den Aufnahmegrund gespeichert und kann in Bitdefender Mobile Security im Fenster für den Diebstahlschutz eingesehen werden. Alternativ können Sie das aufgenommene Foto auch über Ihr Bitdefender-Benutzerkonto einsehen:

- i. Gehen Sie zu: <https://central.bitdefender.com>.
- ii. Melden Sie sich bei Ihrem Konto an.
- iii. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
- iv. Wählen Sie Ihr Android-Gerät aus und wechseln Sie dann zum Reiter **Diebstahlschutz**.
- v. Tippen Sie neben **Fotos einsehen** auf , um die neuesten Aufnahmen einzusehen.

Es werden nur die zwei aktuellsten Fotos gespeichert.

Nach Aktivierung der Diebstahlschutzfunktion können Sie die Web-Steuerungsbefehle durch Antippen der entsprechenden Optionen einzeln aktivieren oder deaktivieren.



Zugriff auf Diebstahlschutz-Funktionen über Bitdefender Central



Beachten Sie

Für die Diebstahlschutz-Funktionen muss die Option **Hintergrunddaten** in den Datennutzungseinstellungen Ihres Gerätes aktiviert sein.

So können Sie über Ihr Bitdefender-Konto auf die Diebstahlschutzfunktionen zugreifen:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
3. Klicken Sie im Fenster **MEINE GERÄTE** auf die gewünschte Gerätekachel.
4. Wechseln Sie zum Reiter **Diebstahlschutz**.
5. Tippen Sie im unteren Feld auf  und danach auf die Schaltfläche für die Funktion, die Sie verwenden möchten:

Orten - zeigt den Standort Ihres Geräts auf Google Maps.



Benachrichtigung - Sie können eine Nachricht eingeben, die auf dem Bildschirm Ihres Geräts angezeigt werden soll, und/oder das Gerät einen Ton abspielen lassen.



Verriegeln - den Computer verriegeln und eine PIN zur Entriegelung festlegen.



Löschen - Entfernen aller Daten auf Ihrem Gerät.



Wichtig

Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

IP ANZEIGEN - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.

Diebstahlschutz-Einstellungen

So können Sie die Fernbefehle aktivieren oder deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.



2. Tippen Sie auf  **Diebstahlschutz**.
3. Aktivieren oder deaktivieren Sie die gewünschten Optionen.



7. KONTOSCHUTZ

Der Bitdefender-Kontoschutz erkennt, ob es bei Ihren Benutzerkonten, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden, zu Datenschutzverletzungen gekommen ist. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Im Hintergrund werden automatisch weitere Prüfungen durchgeführt und Sie können darüber hinaus täglich manuelle Prüfungen durchführen.

Sie erhalten eine Benachrichtigung, sobald neue Datenschutzverletzungen bekannt werden, die eines Ihrer bestätigten E-Mail-Konten betreffen.

So können Sie Ihre persönlichen Daten schützen:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Kontoschutz**.
3. Tippen Sie auf **ERSTE SCHRITTE**.
4. Die E-Mail-Adresse, die zur Erstellung Ihres Bitdefender-Benutzerkontos verwendet wurde, erscheint und wird automatisch zur Liste der überwachten Konten hinzugefügt.
5. Um ein weiteres Konto hinzuzufügen, tippen Sie im Fenster Kontoschutz auf **BENUTZERKONTO HINZUFÜGEN**, und geben Sie die E-Mail-Adresse ein.

Tippen Sie zum Fortfahren auf **HINZUFÜGEN**.

Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.

Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.

Der Privatsphärestatus des bestätigten Kontos wird angezeigt.



Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.
- Verwenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.

Nachdem Sie ein Konto gesichert haben, das von einer Datenschutzverletzung betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als **Gelöst** markieren. Gehen Sie dazu wie folgt vor:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Kontoschutz**.
3. Tippen Sie auf das Konto, das Sie gerade gesichert haben.
4. Tippen Sie auf die Datenpanne, wegen der Sie das Benutzerkonto abgesichert haben.
5. Tippen Sie auf **GELÖST**, um zu bestätigen, dass das Konto gesichert wurde.

Wenn alle gefundenen Datenschutzverletzungen als **Gelöst** markiert wurden, wird das Konto nicht mehr als von einer Datenpanne betroffen angezeigt, zumindest bis es zu einer weiteren Datenpanne kommt.

Gehen Sie folgendermaßen vor, um nicht mehr jedes Mal benachrichtigt zu werden, wenn automatische Scans durchgeführt werden:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Kontoschutz.



8. APP-SPERRE

Installierte Anwendungen so z.B. für E-Mail, Fotos oder Nachrichten können persönliche Daten enthalten, die Sie vor fremden Zugriff durch selektive Zugangssperren schützen können.

Mit der App-Sperre können Sie unbefugten Zugriff auf Ihre Anwendungen verhindern, indem Sie einen PIN-Code für den Zugriff festlegen. Der PIN-Code muss 4-8 Ziffern enthalten und bei jedem Zugriff auf die zugriffsbeschränkten Anwendungen eingegeben werden.

Anstelle der PIN ist bei Geräten mit Fingerabdrucksensor auch eine Bestätigung per Fingerabdruck möglich.

App-Sperre wird aktiviert

Um den Zugriff auf ausgewählte Anwendungen einzuschränken, können Sie die App-Sperre über die Kachel im Dashboard konfigurieren, die nach Aktivierung des Diebstahlschutzes angezeigt wird.

Alternativ können Sie die App-Sperre folgendermaßen aktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **App-Sperre**.
3. Tippen Sie auf **AKTIVIEREN**.
4. Erlauben Sie Bitdefender Security den Zugriff auf die Nutzungsdaten.
5. **Über anderen Apps einblenden** erlauben.
6. Öffnen Sie die App erneut, konfigurieren Sie den Zugriffscode und tippen Sie auf **PIN FESTLEGEN**.



Beachten Sie

Dieser Schritt steht nur zur Auswahl, wenn Sie die PIN noch nicht beim Diebstahlschutz eingerichtet haben.

7. Aktivieren Sie die Option Foto aufnehmen, um Eindringlinge zu erwischen, die versuchen, auf Ihre privaten Daten zuzugreifen.



Beachten Sie

Für die Funktion Foto aufnehmen werden unter Android 6 zusätzliche Berechtigungen benötigt.

Erlauben Sie dem **Virenschutz** das Aufnehmen von Fotos und Videos, um sie zu aktivieren.

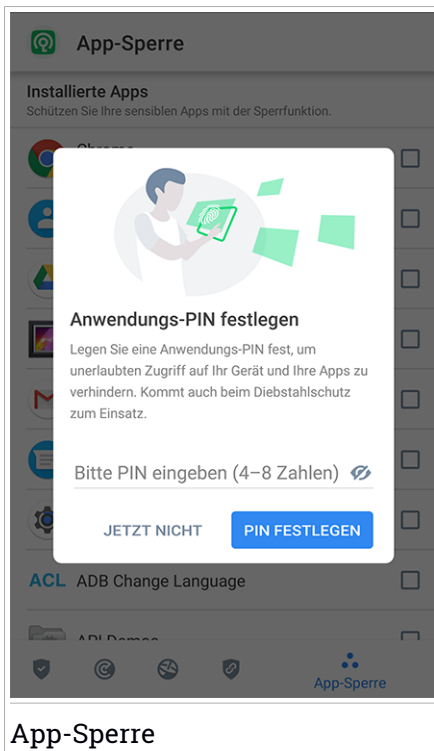
8. Wählen Sie die Apps aus, die Sie schützen möchten.

Wird fünfmal in Folge die falsche PIN eingegeben oder der falsche Fingerabdruck verwendet, tritt eine 30-sekündige Sperre ein. Auf diese Weise werden Versuche auf geschützte Apps zuzugreifen unterbunden.



Beachten Sie

Die gleiche PIN wird vom Diebstahlschutz verwendet, um den Standort Ihres Geräts zu ermittelt.





Sperrmodus

Wenn Sie eine App zum ersten Mal zur App-Sperre hinzufügen, erscheint der Bildschirm App-Sperre-Modus, in dem Sie auswählen können, wann die App-Sperre-Funktion die auf Ihrem Gerät installierten Apps schützen soll.

Ihnen stehen die folgenden Optionen zur Auswahl:

- **Entsperren immer erforderlich** - Der PIN-Code oder Fingerabdruck müssen bei jedem Aufruf einer gesperrten App eingegeben werden.
- **Bis zur Bildschirmabschaltung entsperrt lassen** - Sie können bis zur nächsten Bildschirmabschaltung auf die Apps zugreifen.
- **Nach 30 Sekunden sperren** - Sie können innerhalb von 30 Sekunden bereits geschlossene Apps wieder aufrufen.

So können Sie die ausgewählte Einstellung wieder ändern:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Tippen Sie im Bereich App-Sperre auf **Entsperren immer erforderlich**.
4. Wählen Sie gewünschte Option aus.

App-Sperre-Einstellungen

Für eine erweiterte Konfiguration der App-Sperre:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.

Im Bereich der App-Sperre können Sie die folgenden Optionen konfigurieren:

- **Vorschlag zu sensiblen Apps** - Sie erhalten bei jeder Installation einer sensiblen App eine Sperrbenachrichtigung.
- **Entsperren immer erforderlich** - Wählen Sie eine der verfügbaren Optionen für das Sperren und Entsperren aus.
- **Intelligentes Entsperren** - Ihre Apps bleiben bei Verbindungen mit vertrauenswürdigen WLAN-Netzwerken entsperrt.
- **Zufallstastatur** - Verhindern Sie durch zufällige Anordnung der Ziffern das Ablesen Ihrer PIN.



Foto aufnehmen

Mit der Foto-aufnehmen-Funktion von Bitdefender erwischen Sie Ihre Freunde oder Verwandten auf frischer Tat. So können Sie ihnen klar machen, dass Ihre persönlichen Dateien und installierten Anwendungen nicht für Ihre Augen bestimmt sind.

Es funktioniert ganz einfach: Wird dreimal hintereinander die falsche PIN oder der falsche Fingerabdruck eingegeben, wird mit der Frontkamera ein Foto aufgenommen. Das Foto wird dann mit Zeitstempel und einem Hinweis auf den Aufnahmegrund gespeichert und kann in Bitdefender Mobile Security über die App-Sperre-Funktion angezeigt werden.



Beachten Sie

Diese Funktion steht nur auf Telefonen mit Frontkamera zur Verfügung.

So können Sie die Funktion Foto aufnehmen für die App-Sperre konfigurieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Aktivieren Sie den entsprechenden Schalter im Bereich Foto aufnehmen.

Die Fotos, die nach Eingabe einer falschen PIN aufgenommen werden, werden im App-Sperre-Fenster angezeigt und können dort als Vollbild eingesehen werden.

Alternativ können Sie diese auch über Ihr Bitdefender-Konto anzeigen:

1. Gehen Sie zu: <https://central.bitdefender.com>.
2. Melden Sie sich bei Ihrem Konto an.
3. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
4. Wählen Sie Ihr Android-Gerät aus und wechseln Sie dann zum Reiter **Diebstahlschutz**.
5. Tippen Sie neben **Fotos einsehen** auf , um die neuesten Aufnahmen einzusehen.

Es werden nur die zwei aktuellsten Fotos gespeichert.

So können Sie das Hochladen der aufgenommenen Fotos auf Ihr Bitdefender-Benutzerkonto beenden:



1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Deaktivieren Sie im Bereich Foto aufnehmen die Option **Fotos hochladen**.

Intelligentes Entsperren

Damit die App-Sperre Sie nicht bei jedem Aufrufen einer geschützten App nach Ihrer PIN oder Ihrem Fingerabdruck fragt, können Sie das intelligente Entsperren aktivieren.

Mit der Funktion für das intelligente Entsperren können Sie vertrauenswürdige WLAN-Netzwerke festlegen. Bei Verbindung mit einem dieser Netzwerke werden die Blockierungseinstellungen der App-Sperre für die geschützten Apps deaktiviert.

So können Sie die Funktion Intelligentes Entsperren konfigurieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **App-Sperre**.
3. Tippen Sie auf die Schaltfläche .
4. Tippen Sie auf den Schalter neben **Intelligentes Entsperren**, falls die Funktion noch nicht aktiviert ist.

Bestätigen Sie mit Ihrem Fingerabdruck oder Ihrer PIN.

Wenn Sie die Funktion zum ersten Mal aktivieren, müssen Sie die Standortberechtigung aktivieren. Tippen Sie auf die Schaltfläche **ZULASSEN** und dann erneut auf **ZULASSEN**.

5. Tippen Sie auf **HINZUFÜGEN**, um Ihre aktuelle WLAN-Verbindung als vertrauenswürdig festzulegen.

Falls Sie es sich anders überlegen, können Sie die Funktion jederzeit deaktivieren. Alle bisher als vertrauenswürdig eingestuften WLAN-Netzwerke gelten dann wieder als nicht vertrauenswürdig.



9. BERICHTE

Die Berichtsfunktion protokolliert alle Ereignisse im Zusammenhang mit den Scans auf Ihrem Gerät.

Für jedes sicherheitsrelevante Ereignis auf Ihrem Gerät wird den Berichten eine neue Nachricht hinzugefügt.

So können Sie auf den Bereich Berichte zugreifen:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Berichte**.

Im Fenster Berichte finden Sie die folgenden Reiter:

- **WÖCHENTLICHE BERICHTE** - Hier können Sie den Sicherheitsstatus und die durchgeführten Aktionen für die aktuelle und vorausgegangene Woche einsehen. Der Bericht für die aktuelle Woche wird jeweils Sonntags erstellt und werden benachrichtigt, sobald er verfügbar ist.

In diesem Bereich wird jede Woche ein neuer Hinweis angezeigt. Schauen Sie also regelmäßig vorbei, um optimalen Nutzen aus der App zu ziehen.

So können Sie die Benachrichtigung für jeden neuen Bericht deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
 2. Tippen Sie auf  **Einstellungen**.
 3. Deaktivieren Sie den Schalter **Benachrichtigung bei neuen Berichten** im Bereich Berichte.
- **AKTIVITÄTSPROTOKOLL** - Hier können Sie ausführliche Informationen zu den Aktivitäten Ihrer Bitdefender Mobile Security-App seit Installation auf Ihrem Android-Gerät einsehen.

So können Sie das verfügbare Aktivitätsprotokoll löschen:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Tippen Sie auf **Aktivitätsprotokoll löschen** und danach auf **AUSWAHL AUFHEBEN**.



10. WEARON

Mit Bitdefender-WearON können Sie Ihr Smartphone schnell und einfach wiederfinden, egal ob Sie es bei der Arbeit im Besprechungsraum oder unter einem Kissen auf dem Sofa vergessen haben. Das Gerät lässt sich auch dann aufspüren, wenn es auf lautlos gestellt ist.

Lassen Sie diese Funktion aktiviert, damit Sie Ihr Smartphone jederzeit zur Hand haben.



Beachten Sie

Diese Funktion benötigt Android 4.3 und Android Wear.

Aktivierung von WearON

Zur Verwendung von WearON müssen Sie Ihre Smartwatch mit der Bitdefender Mobile Security-Anwendungen verbinden und die Funktion über den folgenden Sprachbefehl aktivieren:

Start:<Where is my phone>

Bitdefender-WearON kennt zwei Befehle:

1. Mobile-Warnung

Mit der Phone-Alert-Funktion können Sie Ihr Smartphone schnell wiederfinden, wenn Sie sich zu weit davon entfernt haben.

Wenn Sie eine Smartwatch nutzen, erkennt diese automatisch die App auf Ihrem Telefon und vibriert, wenn die Entfernung zwischen Smartwatch und Gerät zu groß wird und die Bluetooth-Verbindung unterbrochen wird.

Öffnen Sie zur Aktivierung dieser Funktion Bitdefender Mobile Security, tippen Sie im Menü auf **Allgemeine Einstellungen** und wählen Sie im Bereich WearON den entsprechenden Schalter aus.

2. Scream

Es war noch nie so einfach, Ihr Telefon aufzuspüren. Sie haben vergessen, wo Ihr Telefon liegt? Tippen Sie einfach auf den Scream-Befehl auf Ihrer Uhr, um den Scream-Alarm auszulösen.



11. INFO ÜBER

Gehen Sie folgendermaßen vor, um Informationen zur installierten Bitdefender Mobile Security-Version abzurufen, die Abonnementvereinbarung und Datenschutzerklärung aufzurufen und zu lesen und die Open-Source-Lizenzen anzuzeigen:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Tippen Sie im Bereich Über auf die gewünschte Option.



12. BITDEFENDER CENTRAL

Bitdefender Central stellt Ihnen eine Web-Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben per Fernzugriff auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über <https://central.bitdefender.com> können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender-Konto anmelden. Alternativ können Sie auf Ihren Android- und iOS-Geräten auch die Bitdefender Central-App nutzen.

So können Sie die Bitdefender Central-App auf Ihren Geräten installieren:

- **Android** - Suchen Sie Bitdefender Central in Google Play, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.
- **iOS** - Suchen Sie Bitdefender Central im App Store, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.

Nachdem Sie sich angemeldet haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
 - Bitdefender Mobile Security
 - Bitdefender Mobile Security for iOS
 - Bitdefender Antivirus for Mac
 - Die Bitdefender-Windows-Produktlinie
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Hinzufügen neuer Geräte zu Ihrem Netzwerk und Fernverwaltung dieser Geräte.
- Mit dem **Diebstahlschutz** schützen Sie Ihre Netzwerkgeräte und die darauf gespeicherten Daten vor Verlust und Diebstahl.

Aufrufen Ihres Bitdefender-Benutzerkontos.

Es gibt zwei Möglichkeiten zum Aufrufen von Bitdefender Central



- Über Ihren Web-Browser:
 1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
 2. Gehen Sie zu: <https://central.bitdefender.com>.
 3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Konto an.
- Über Ihr Android- oder iOS-Gerät:

Öffnen Sie die bei Ihnen installierte Bitdefender Central-App.



Beachten Sie

Hier finden Sie alle Optionen und Anleitungen, die Ihnen über die Web-Plattform zur Verfügung gestellt werden.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung fügt Ihrem Bitdefender-Benutzerkonto eine weitere Sicherheitsebene hinzu, indem sie zusätzlich zu Ihren Anmeldeinformationen einen Authentifizierungscode anfordert. Auf diese Weise verhindern Sie unbefugten Zugriff auf Ihr Benutzerkonto und schützen sich vor Cyberangriffen wie Keylogger-, Brute-Force- oder Wörterbuchangriffen.

Aktivieren der Zwei-Faktor-Authentifizierung

Durch die Aktivierung der Zwei-Faktor-Authentifizierung wird Ihr Bitdefender-Benutzerkonto deutlich besser abgesichert. Sie müssen Ihre Identität für jede Anmeldung über ein neues Gerät erneut bestätigen, so zum Beispiel wenn Sie eines der Bitdefender-Produkte installieren, Ihren Abonnementstatus einsehen oder per Fernzugriff Aufgaben auf Ihren Geräten ausführen.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben rechts auf dem Bildschirm auf das Symbol .
3. Tippen Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Tippen Sie auf **Zwei-Faktor-Authentifizierung**.



6. Tippen Sie auf **ERSTE SCHRITTE**.

Wählen Sie eine der folgenden Methoden aus:

- **Authentifizierungs-App** - Verwenden Sie eine Authentifizierungs-App, um für jede Anmeldung bei Ihrem Bitdefender-Konto einen Code zu generieren.

Wenn Sie eine Authentifizierungs-App verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit den von uns empfohlenen Authentifizierungs-Apps auswählen.

- a. Tippen Sie zunächst auf **AUTHENTIFIZIERUNGS-APP VERWENDEN**.
- b. Um sich auf einem Android- oder iOS-Gerät anzumelden, verwenden Sie Ihr Gerät, um den QR-Code zu scannen.

Zur Anmeldung auf einem Laptop oder Computer können Sie den angezeigten Code manuell eingeben.

Tippen Sie auf **WEITER**.

- c. Geben Sie den von der App generierten bzw. den im vorherigen Schritt angezeigten Code ein, und tippen Sie dann auf **AKTIVIEREN**.

- **E-Mail** - Bei jeder Anmeldung an Ihrem Bitdefender-Konto wird ein Bestätigungscode an Ihre E-Mail-Adresse gesendet. Überprüfen Sie Ihr E-Mail-Konto, und geben Sie dann den erhaltenen Code ein.

- a. Tippen Sie zunächst auf **E-MAIL VERWENDEN**.
- b. Überprüfen Sie Ihr E-Mail-Konto, und geben Sie den erhaltenen Code ein.

Bitte beachten Sie, dass Sie fünf Minuten Zeit haben, Ihr E-Mail-Konto aufzurufen und den generierten Code einzugeben. Nach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.

- c. Tippen Sie auf **AKTIVIEREN**.
- d. Sie erhalten zehn Aktivierungs-codes. Sie können die Liste entweder kopieren, herunterladen oder ausdrucken und für den Fall verwenden, dass Sie Ihre E-Mail-Adresse verlieren oder sich nicht mehr anmelden können. Jeder Code kann nur einmal verwendet werden.
- e. Tippen Sie auf **FERTIG**.



Gehen Sie folgendermaßen vor, wenn Sie die Zwei-Faktor-Authentifizierung nicht mehr nutzen möchten:

1. Tippen Sie auf **ZWEI-FAKTOR-AUTHENTIFIZIERUNG DEAKTIVIEREN**.
2. Sehen Sie in die App oder rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.

Falls Sie sich für den Empfang des Authentifizierungscode per E-Mail entschieden haben, haben Sie fünf Minuten Zeit, um Ihre E-Mails abzurufen und den generierten Code einzugeben. Nach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.

3. Bestätigen Sie Ihre Auswahl.

Hinzufügen vertrauenswürdiger Geräte

Um sicherzustellen, dass nur Sie auf Ihr Bitdefender-Konto zugreifen können, fragen wir unter Umständen zunächst einen Sicherheitscode ab. Wenn Sie bei Anmeldungen über das gleiche Gerät diesen Schritt überspringen möchten, empfehlen wir, dass Sie ein vertrauenswürdiges Gerät festzulegen.

So können Sie Geräte als vertrauenswürdige Geräte festlegen:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben rechts auf dem Bildschirm auf das Symbol .
3. Tippen Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Tippen Sie auf **Vertrauenswürdige Geräte**.
6. Es wird eine Liste mit Geräten angezeigt, auf denen Bitdefender installiert ist. Tippen Sie auf das gewünschte Gerät.

Sie können beliebig viele Geräte hinzufügen, vorausgesetzt, dass Bitdefender auf ihnen installiert ist und Sie über ein gültiges Abonnement verfügen.

Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Geräteiname, der Sicherheitsstatus



angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann oben rechts auf .
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und tippen Sie danach auf **SPEICHERN**.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann oben rechts auf .
4. Wählen Sie **Profil**.
5. Tippen Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen und einen Geburtstag eingeben.
6. Tippen Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und tippen Sie auf **ZUORDNEN**.

Wählen Sie die entsprechende Gerätekachel aus, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Wählen Sie eine Gerätekachel aus, um die folgenden Reiter anzuzeigen:

- **Dashboard**. In diesem Fenster werden Details zum ausgewählten Gerät angezeigt sowie sein Sicherheitsstatus, der Status des Bitdefender-VPN und wie viele Bedrohungen in den vergangenen 7 Tagen blockiert wurden.



Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt, gelb, wenn es etwas gibt, was Ihre Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Wenn Probleme bestehen, tippen Sie auf das Klappenmenü oben im Statusbereich, um mehr Details dazu anzuzeigen. Hier können Sie dann Probleme beheben, die die Sicherheit Ihrer Geräte gefährden.

- **Schutz.** Von diesem Fenster aus können Sie einen Scan auf Ihrem Gerät durchführen. Klicken Sie dazu auf **SCANNEN**. Hier können Sie auch einsehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht mit den wichtigsten Informationen zum letzten Scan aufrufen.
- **Diebstahlschutz.** Falls Sie Ihr Gerät verlegt haben, können Sie es mit der Diebstahlschutzfunktion wiederfinden und aus der Ferne steuern. Klicken Sie auf **ORTEN**, um die Position des Gerätes zu bestimmen. Die letzte bekannte Position wird mit Datum und Zeitpunkt angezeigt. Weitere Details zu dieser Funktion finden Sie unter „*Diebstahlschutz-Funktionen*“ (S. 16).

Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Abonnements** aus.

Hier werden alle Informationen zur Verfügbarkeit Ihrer Abonnements und die Anzahl der Geräte angezeigt, auf denen diese verwendet werden.

Klicken Sie auf eine Abonnementkarte, um Ihrem Abonnement ein neues Gerät hinzuzufügen oder es zu verlängern.

Ein neues Gerät hinzufügen

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Mobile Security installieren. Weitere Informationen dazu finden Sie im Abschnitt „*Installation von Bitdefender Mobile Security*“ (S. 2).



Renew subscription

Wenn in Ihrem Abonnement noch weniger als 30 Tage verbleiben und Sie sich gegen eine automatische Verlängerung entschieden haben, können Sie Ihr Abonnement wie folgt auch manuell verlängern:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Abonnements** aus.
3. Wählen Sie die gewünschte Abonnementkarte aus.
4. Klicken Sie zum Fortfahren auf **VERLÄNGERN**.

In Ihrem Web-Browser wird eine neue Seite geöffnet, über die Sie Ihr Bitdefender-Abonnement verlängern können.



13. HÄUFIG GESTELLTE FRAGEN

Wieso benötigt Bitdefender Mobile Security eine Internet-Verbindung?

Die Anwendung muss mit den Bitdefender-Servern kommunizieren, um den Sicherheitsstatus der Anwendungen, die gescannt werden, und der Webseiten, die Sie besuchen, zu bestimmen. Darüber hinaus erhält es so die Befehle, die bei Verwendung der Diebstahlschutzfunktionen über Ihr Bitdefender-Konto verschickt werden.

Wofür werden die einzelnen Berechtigungen von Bitdefender Mobile Security benötigt?

- Internet-Zugang -> für die Cloud-Kommunikation.
- Gerätstatus und Identität ermitteln -> hiermit wird ermittelt, ob Ihr Gerät mit dem Internet verbunden ist, und bestimmte Geräteinformationen ausgelesen, die nötig sind, um eine einzigartige ID für die Kommunikation mit der Bitdefender-Cloud zu erstellen.
- Browser-Lesezeichen anlegen und benutzen -> Der Surfschutz löscht schädliche Websites aus dem Browser-Verlauf.
- Protokolle lesen -> Bitdefender Mobile Security kann anhand der Android-Protokolle Bedrohungsaktivitäten erkennen.
- Ortung -> für die Fern-Geräteortung.
- Kamera -> wird für die Funktion Foto aufnehmen benötigt.
- Speicher -> wird benötigt, um dem Virens scanner die Prüfung der SD-Karte zu erlauben.

Wie unterbinde ich die Übermittlung von Informationen zu verdächtigen Apps an Bitdefender?

Bitdefender Mobile Security übermittelt standardmäßig Berichte über von Ihnen installierte verdächtige Apps an die Bitdefender-Server. Diese Informationen sind für die Verbesserung der Gefahrenerkennung unerlässlich und können uns helfen, unser Produkt noch besser zu machen. Gehen Sie folgendermaßen vor, wenn Sie nicht mehr möchten, dass Informationen über verdächtige Apps an uns übermittelt werden:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.



3. Deaktivieren Sie im Bereich Virenschanner die Option **In-the--Cloud-Erkennung**.

Wo kann ich Einzelheiten zu den Aktivitäten der App einsehen?

Bitdefender Mobile Security führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere wichtige Nachrichten über eigene Aktivitäten. So können Sie die Aktivitäten der App einsehen:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Berichte**.

Im Fenster WOCHENBERICHTE können Sie auf die Berichte zugreifen, die jede Woche erstellt werden, und im Fenster AKTIVITÄTSPROTOKOLL können Sie Informationen über die Aktivität Ihrer Bitdefender-App anzeigen.

Ich habe den PIN-Code vergessen, mit dem ich meine Anwendung geschützt habe. Was kann ich tun?

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben links auf  und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann oben rechts auf .
4. Tippen Sie auf **Einstellungen**.
5. Sie können den PIN-Code im Feld **Anwendungs-PIN** abrufen.

Wie kann ich den PIN-Code ändern, den ich für die App-Sperre und den Diebstahlschutz festgelegt habe?

So können Sie den PIN-Code ändern, den Sie für die App-Sperre und den Diebstahlschutz festgelegt haben:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **Einstellungen**.
3. Tippen Sie im Bereich Diebstahlschutz auf **Sicherheits-PIN**.
4. Geben Sie den aktuellen PIN-Code ein.
5. Geben Sie den neuen PIN-Code ein.

Wie kann ich die App-Sperre deaktivieren?



Es gibt keine eigene Option zur Deaktivierung der App-Sperre, Sie müssen dazu lediglich die Kästchen neben den ausgewählten Apps deaktivieren. Dazu wird die festgelegte PIN oder der Fingerabdruck abgefragt.

Wie kann ich ein weiteres WLAN-Netzwerk als vertrauenswürdig einstufen?

Sie müssen Ihr Gerät zunächst mit dem Drahtlosnetzwerk verbinden, das Sie als vertrauenswürdig festlegen möchten. Gehen Sie danach wie folgt vor:

1. Tippen Sie in der unteren Navigationsleiste auf  **Mehr**.
2. Tippen Sie auf  **App-Sperre**.
3. Tippen Sie oben rechts auf .
4. Tippen Sie neben dem Netzwerk, das Sie als vertrauenswürdig festlegen möchten, auf **HINZUFÜGEN**.

Wie deaktiviere ich die Anzeige von Fotos, die mit meinem Gerät aufgenommen wurden?

So können Sie die Anzeige von Fotos deaktivieren, die mit Ihren Geräten aufgenommen wurden:

1. Rufen Sie **Bitdefender Central** auf.
2. Tippen Sie oben rechts auf .
3. Tippen Sie im Menü auf **Mein Konto**.
4. Wechseln Sie zum Reiter **Einstellungen**.
5. Deaktivieren Sie die Option **Mit Ihren Geräten aufgenommene Fotos anzeigen/nicht anzeigen**.

Wie kann ich sicher im Netz einkaufen und bezahlen?

Online-Einkäufe sind mit großen Risiken verbunden, wenn einige Details übersehen werden. Um zu verhindern, dass auch Sie zum Betrugsopfer werden, sollten Sie folgende Empfehlungen beachten:

- Halten Sie Ihre Sicherheitslösung immer auf dem neuesten Stand.
- Stellen Sie bei Online-Zahlungen sicher, dass Käuferschutz gewährleistet wird.
- Nutzen Sie in öffentlichen und ungesicherten WLAN-Netzwerken eine VPN-Verbindung zur Verbindung mit dem Internet.



- Prüfen Sie die Passwörter Ihrer Online-Benutzerkonten. Stellen Sie sicher, dass sie neben Groß- und Kleinbuchstaben auch Zahlen und Sonderzeichen (@, !, %, # usw.) enthalten.
- Übermitteln Sie Informationen ausschließlich über sichere Verbindungen. Achten Sie darauf, dass die Adresse der Website mit HTTPS:// und nicht mit HTTP:// beginnt.

Wann sollte ich Bitdefender VPN nutzen?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um beim Surfen im Netz jederzeit geschützt zu sein, empfehlen wir die Nutzung von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob zuhause oder im Ausland
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?

Bitdefender VPN wurde entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und um regionale Zugangsbeschränkungen für Inhalte zu umgehen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zu Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

Kann ich das Bitdefender-Konto ändern, das mit meinem Gerät verknüpft ist?



Ja, Sie können jederzeit Ihrem Gerät ein anderes Bitdefender-Konto zuordnen. Gehen Sie dazu folgendermaßen vor:

1. Tippen Sie in der unteren Navigationsleiste auf **Mehr**.
2. Tippen Sie auf Ihre E-Mail-Adresse.
3. Tippen Sie auf **Melden Sie sich bei Ihrem Konto ab**. Wenn ein PIN-Code festgelegt wurde, werden Sie aufgefordert, ihn einzugeben.
4. Bestätigen Sie Ihre Auswahl.
5. Geben Sie die E-Mail-Adresse und das Passwort Ihres Benutzerkontos in die entsprechenden Felder ein und tippen Sie auf **ANMELDEN**.

Wie wirkt sich Bitdefender Mobile Security auf die Systemleistung und Akkulaufzeit meines Geräts aus?

Die Auswirkungen sind minimal. Die Anwendung läuft nur, wenn es absolut notwendig ist, d.h. wenn Sie sie installieren, wenn Sie die Anwendung aufrufen oder eine Sicherheitsprüfung durchführen. Bitdefender Mobile Security läuft nicht im Hintergrund, wenn Sie Ihre Freunde anrufen, Nachrichten schreiben oder Spiele spielen.

Was ist Geräteadministratoren?

Geräteadministrator ist eine Android-Funktion, die Bitdefender Mobile Security die benötigten Rechte einräumt, um bestimmte Aufgaben per Fernzugriff durchzuführen. Ohne diese Rechte würde die Fernsperrung nicht funktionieren und die Gerätelöschung wäre nicht in der Lage, Ihre Daten aus der Ferne vollständig zu löschen. Sollten Sie die App entfernen wollen, müssen Sie vor der Deinstallation diese Rechte wieder entziehen über **Einstellungen > Sicherheit > Geräteadministratoren auswählen**.

So beheben Sie den "Keine Google-Token"-Fehler, der bei der Bitdefender Mobile Security-Anmeldung auftritt.

Dieser Fehler tritt auf, wenn das Gerät mit keinem Google-Konto verknüpft ist oder wenn es zwar mit einem Konto verknüpft ist, es aber wegen eines vorübergehenden Problems keine Verbindung zu Google herstellen kann. Die folgenden Schritte können das Problem beheben:

- Gehen Sie zu Android-Einstellungen > Anwendungen > Anwendungen verwalten > Bitdefender Mobile Security, und tippen Sie auf **Daten löschen**. Melden Sie sich dann erneut an.
- Ihr Gerät muss mit einem Google-Konto verknüpft sein.



Ob es das ist, können Sie wie folgt überprüfen: Gehen Sie zu Einstellungen > Konten & Synchronisierung, und sehen Sie nach, ob unter **Konten verwalten** ein Google-Konto aufgeführt ist. Tragen Sie Ihr Konto ein, falls es nicht aufgeführt ist, starten Sie dann das Gerät neu und melden Sie sich erneut bei Bitdefender Mobile Security an.

- Starten Sie Ihr Gerät neu, und versuchen Sie es dann erneut.

In welchen Sprachen ist Bitdefender Mobile Security verfügbar?

Bitdefender Mobile Security ist derzeit in den folgenden Sprachen verfügbar:

- Brasilianisch
- Tschechisch
- Niederländisch
- Englisch
- Französisch
- Deutsch
- Griechisch
- Ungarisch
- Italienisch
- Japanisch
- Koreanisch
- Polnisch
- Portugiesisch
- Rumänisch
- Russisch
- Spanisch
- Schwedisch
- Thai
- Türkisch
- Vietnamesisch

Weitere Sprachen werden in zukünftigen Versionen hinzugefügt. Sie können die Sprache von Bitdefender Mobile Security ändern, indem Sie unter **Sprache & Tastatur** die gewünschte Sprache für Ihr Gerät einstellen.



14. HILFE ERHALTEN

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:

<http://www.bitdefender.de/support/consumer.html>

- Bitdefender Support-Forum: <http://forum.bitdefender.com>

- Das Computer-Sicherheitsportal HOTforSecurity:

<https://www.hotforsecurity.com/>

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Bitdefender-Support-Center

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

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigten Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung: <https://www.bitdefender.com/support/>.

Bitdefender Support-Forum

Das Bitdefender Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben.



Falls Ihr Bitdefender-Produkt nicht richtig funktioniert, bestimmte Bedrohungen nicht von Ihrem Gerät entfernen kann oder wenn Sie Fragen über die Funktionsweise haben, stellen Sie Ihr Problem oder Frage in das Forum ein.

Support-Techniker von Bitdefender überwachen das Forum auf neue Einträge, um Ihnen zu helfen. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter <http://forum.bitdefender.com>. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter Tippen Sie bitte auf **Schutz für Privatanwender**.

Das Portal HOTforSecurity

Das HOTforSecurity-Portal bietet umfangreiche Informationen rund um das Thema Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internet-Verbindung ausgesetzt ist (Malware, Phishing-Versuche, Spam, Online-Kriminelle). Das nützliche Wörterbuch liefert Definitionen für Begriffe aus der Online-Sicherheit, die Ihnen bisher noch nicht bekannt waren.

Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist <https://hotforsecurity.bitdefender.com/>.