

Bitdefender® Mobile Security



BENUTZERHANDBUCH



Bitdefender Mobile Security **Benutzerhandbuch**

Veröffentlicht 06.06.2018

Copyright© 2018 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuchs 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. Kontoschutz	10
5. Internet-Schutz	12
6. VPN	14
7. Diebstahlschutz-Funktionen	18
8. App-Sperre	24
9. Berichte	29
10. WearON	30
11. Einstellungen	31
12. Info über	32
13. Bitdefender Central	33
14. Häufig gestellte Fragen	37
15. Hilfe erhalten	43



1. SICHERHEITSFUNKTIONEN

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

- Virens Scanner
- Kontoschutz
- Internet-Schutz
- VPN
- Diebstahlschutz:
 - Fern-Gerätortung
 - Fern-Gerätesperrung
 - Fern-Gerätelöschung
 - Fern-Tonsignale
- 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 4.0.3. 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 das -Symbol und wählen Sie danach **Meine Geräte** aus.
4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
5. Wählen Sie **Bitdefender Mobile Security** aus der Liste und tippen Sie danach auf **ZU GOOGLE PLAY**.
6. Tippen Sie im Google-Play-Fenster 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 in der oberen linken Bildschirmcke auf das -Symbol und wählen Sie danach **Meine Geräte** aus.
4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
5. Klicken Sie auf Windows- und macOS-Geräten auf den Link **Auf einem anderen Gerät**.
Tippen Sie auf iOS-Geräten auf **Möchten Sie weitere Geräte schützen?**
6. Wählen Sie **Android** aus.
7. Wählen Sie **Bitdefender Mobile Security** aus der Liste und tippen Sie danach auf **FORTFAHREN**.



8. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie dann auf **SENDEN**.
9. Greifen Sie über Ihr Android-Gerät auf Ihr E-Mail-Konto zu und tippen Sie auf **Jetzt über Google Play herunterladen**.
Sie werden zur **Google Play**-App weitergeleitet.
- 10 Tippen Sie im Google-Play-Fenster auf **INSTALLIEREN**.

● Über Google Play

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

Sie können auch den QR-Code einscannen:



Zum Abschluss des Installationsvorgangs 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- 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. Bitdefender Mobile Security öffnen.
2. 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.
3. 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.

Aktivierung von Bitdefender Mobile Security

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.

So können Sie Bitdefender Mobile Security aktivieren:

1. Bitdefender Mobile Security öffnen.
2. Die Anwendung zeigt Informationen zum aktuellen Abonnementstatus an.
Tippen Sie auf **ICH HABE EINEN CODE**.
3. Geben Sie einen Aktivierungscode in das entsprechende Feld ein und tippen Sie danach auf **AKTIVIEREN**.

So können Sie ein verfügbares Abonnement verlängern:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Mein Konto** aus der Liste aus.



3. Geben Sie unter **Abonnement verlängern** einen Aktivierungscode ein und tippen Sie danach auf **AKTIVIEREN**.

Alternativ können Sie Ihr aktuelles Abonnement auch über die aufgeführten Angebote verlängern.

Dashboard

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

Das Dashboard zeigt Informationen zum Sicherheitsstatus Ihres Geräts an und lässt Sie komfortabel sämtliche Sicherheitsfunktionen verwalten.

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 Bitdefender Mobile Security-Funktionen zugreifen und über die **Menu**-Schaltfläche oben links im Fenster bequem zwischen den einzelnen Bereichen wechseln:

Virenschanner

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

Kontoschutz

Prüft, ob die Datensicherheit Ihrer Online-Konten kompromittiert wurde. Weitere Informationen finden Sie unter „*Kontoschutz*“ (S. 10).

Internet-Schutz

Hiermit können Sie den Internet-Schutz aktivieren und deaktivieren. Weitere Informationen finden Sie unter „*Internet-Schutz*“ (S. 12).

VPN

Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter „*VPN*“ (S. 14).

Diebstahlschutz

Hiermit können Sie die Diebstahlschutzfunktionen aktivieren und deaktivieren und die Einstellungen für den Diebstahlschutz konfigurieren. Weitere Informationen finden Sie unter „*Diebstahlschutz-Funktionen*“ (S. 18).



App-Sperre

Hiermit können Sie Ihre installierten Anwendungen durch Festlegung einer PIN für den Zugriff schützen. Weitere Informationen finden Sie unter „*App-Sperre*“ (S. 24).

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. 29).

WearON

Kommuniziert mit Ihrer Smartwatch, damit Sie Ihr Telefon schneller wiederfinden können. Weitere Informationen finden Sie unter „*WearON*“ (S. 30).



3. VIRENSCANNER

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



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.

Dieser Scan-Typ wird über die Autopilot-Funktion bereitgestellt. Der Autopilot ist ein intelligenter Scanner, der alle Apps überprüft, die Sie installieren oder aktualisieren, und so Bedrohungen rechtzeitig aufhält.

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.

Tippen Sie zum Durchführen eines Bedarf-Scans in der Virenschanner-Kachel im Dashboard auf **SCAN STARTEN**.

Alternativ können Sie einen Scan folgendermaßen durchführen:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Virenschanner** aus der Liste aus.
3. Tippen Sie auf **SCAN STARTEN**.



Beachten Sie

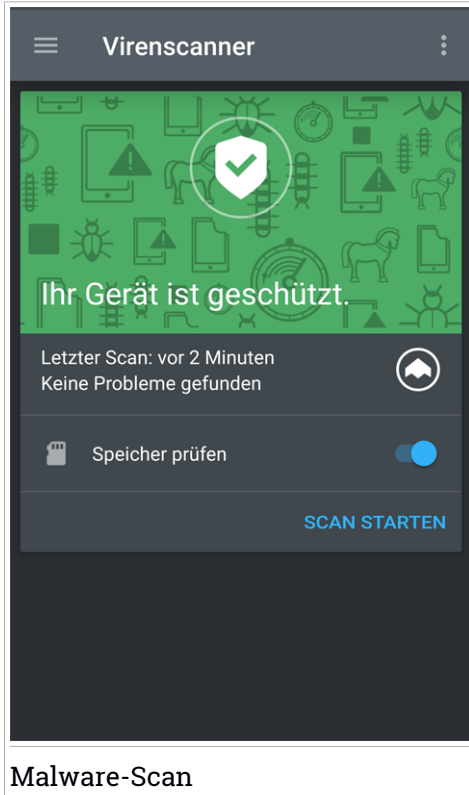
Für den Virenschanner werden unter Android 6 zusätzliche Berechtigungen benötigt. Tippen Sie auf **SCAN STARTEN** und wählen Sie danach **Zulassen** für folgende Anfragen aus:

- Zulassen, dass der **Virenschutz** Anrufe tätigt und verwaltet?



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

Der Scanvorgang wird angezeigt. Sie können ihn jederzeit abbrechen.




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 aktivieren oder deaktivieren Sie die Option Speicher prüfen:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Virens scanner** aus der Liste aus.



3. Tippen Sie auf den entsprechenden Schalter.

Sie können den Speicher-Scan auch über die **Einstellungen** aktivieren oder deaktivieren. Tippen Sie dazu zunächst auf die -Schaltfläche und danach auf den entsprechenden Schalter.

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

Die Virenschanner-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.



4. 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, Datenpannen gab. 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 Datenpannen bekannt werden, die eines Ihrer bestätigten E-Mail-Konten betreffen.

So können Sie Ihre persönlichen Daten schützen:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Kontoschutz** aus der Liste aus.
3. Tippen Sie auf den blauen Kreis unten rechts auf dem Bildschirm.
4. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.

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.

5. 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 Datenpannen 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 Datenpanne betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als **Gelöst** markieren. Gehen Sie dazu wie folgt vor:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Kontoschutz** aus der Liste aus.
3. Tippen Sie auf das Konto, das Sie gerade gesichert haben.
4. Streichen Sie im Bereich **Datenpannen** nach links über die Datenpanne, für die Sie das Konto gesichert haben.
5. Tippen Sie auf das Symbol .
6. Die Karte **Als gelöst markieren** wird angezeigt.

Tippen Sie auf **BESTÄTIGEN**, um zu bestätigen, dass das Konto gesichert wurde.

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



5. INTERNET-SCHUTZ

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

Wenn eine URL auf eine bekannte Phishingversuche oder andere Arten von Betrug oder auf schädliche Inhalte wie Spyware oder Viren, wird die Webseite vorübergehend blockiert und eine Warnung angezeigt.

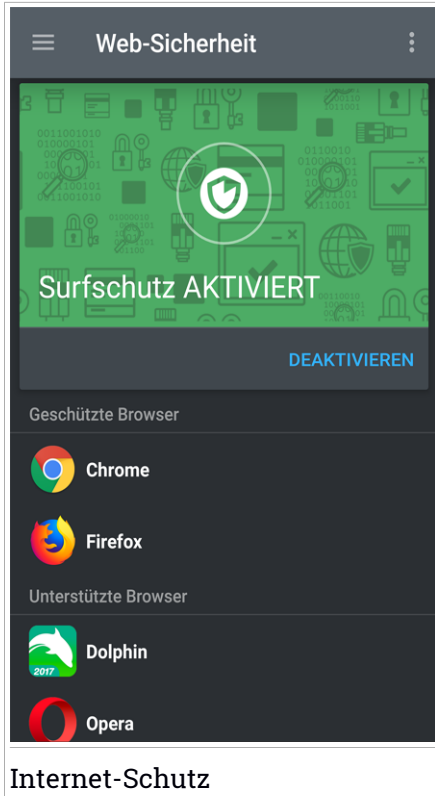
Sie können dann die Benachrichtigung ignorieren und die Webseite besuchen oder zu einer sicheren Seite zurückkehren.



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.





6. 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 im Dashboard auf die Ein/Aus-Schaltfläche. Der Status von Bitdefender VPN wird angezeigt.
- Tippen Sie auf **Menü** und wählen Sie **VPN** aus der Liste aus. 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.



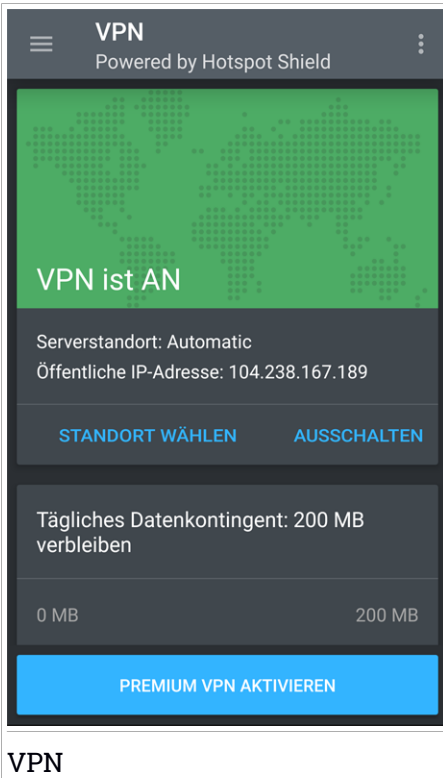
Beachten Sie

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.

Das  Symbol wird bei aktivem Bitdefender VPN in der Statusleiste angezeigt.

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 **STANDORT WÄHLEN** und wählen Sie den gewünschten Standort aus. Weitere Details zu den VPN-Abonnements finden Sie unter „**Abonnements**“ (S. 16).




VPN



Tippen Sie in der VPN-Kachel im Dashboard auf **WEITERE INFORMATIONEN**, um auf die Funktion zuzugreifen. Hier können Sie:

- Anzeigen, wie viel von Ihrem täglichen Datenvolumen Sie bereits verbraucht haben, oder auf die Premium-Version upgraden - Informationen dazu finden Sie in der kostenlosen VPN-Version.
- Den Server auswählen, mit dem Sie eine Verbindung herstellen möchten und die verbleibende Laufzeit Ihres Abonnements anzeigen - Informationen dazu finden Sie in der Premium-VPN-Version.

VPN-Einstellungen

Tippen Sie auf die -Schaltfläche im VPN-Menü und wählen Sie danach **Einstellungen** für die erweiterten App-Sperre-Optionen.

Im die **VPN-Einstellungen** können Sie folgende Optionen konfigurieren:

- VPN-Schnellzugriff-Benachrichtigung – eine Benachrichtigung wird in der Statusleiste angezeigt, über die Sie VPN schnell einschalten können.
- Benachrichtigung bei Verbindung mit offenem WLAN – jedes Mal, wenn Sie eine Verbindung zu einem offenen WLAN herstellen, werden Sie in der Statusleiste darauf hingewiesen, dass Sie VPN einschalten können.
- Benachrichtigung beim Zugriff auf Online-Banking-Seiten – jedes Mal, wenn Sie eine Online-Banking-Seite aufrufen, werden Sie in der Statusleiste darauf hingewiesen, dass Sie VPN einschalten können.

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 oder in der VPN-Benutzeroberfläche auf **PREMIUM VPN 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.



7. 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.

Durch den Versand von **SMS-Befehlen** von jedem beliebigen Mobiltelefon auf Ihr Smartphone können Sie Ihr Gerät sogar dann noch schützen, wenn Sie nicht auf das Internet zugreifen können.

Bitdefender Mobile Security bietet die folgenden Diebstahlschutzfunktionen:

Fern-Gerätortung

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.

IP anzeigen

Zeigt die letzte IP-Adresse für das ausgewählte Gerät. Tippen Sie zum Anzeigen auf **IP ANZEIGEN**.

Fernlöschung

Löschen Sie alle persönlichen Daten von Ihrem Gerät.

Fernsperrung

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



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. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Diebstahlschutz** aus der Liste aus.
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. So können Sie ihn aktivieren:

- Tippen Sie zunächst auf **Diebstahlschutz aktivieren** und danach auf **AKTIVIEREN**.
- Erteilen Sie die folgenden Berechtigungen:
 - a. Zulassen, dass der **Virenschutz** SMS-Nachrichten versendet und liest?
 - b. Zulassen, dass der **Virenschutz** auf den Gerätestandort zugreift?
 - c. Zulassen, dass der **Virenschutz** auf Ihre Kontaktliste zugreift?

a. Administratorrechte erteilen



Diese Rechte sind für den Betrieb des Diebstahlschutzmoduls unbedingt erforderlich und müssen eingeräumt werden, um diesen Vorgang fortzusetzen.

b. **Anwendungs-PIN festlegen**

Um sicherstellen zu können, dass Änderungen an den Diebstahlschutzeinstellungen von Ihnen autorisiert sind, muss eine PIN festgelegt werden. Diese PIN wird zur Bestätigung von Änderungen an den Diebstahlschutzeinstellungen abgefragt. Anstelle der PIN ist bei Geräten mit Fingerabdrucksensor auch eine Bestätigung per Fingerabdruck möglich.



Beachten Sie

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

c. **Foto aufnehmen aktivieren**

Ist Foto aufnehmen aktiviert, nimmt Bitdefender bei jedem unautorisierten Zugriff auf Ihre installierten Anwendungen ein Foto der jeweiligen Person auf. Weitere Informationen zu dieser Funktion finden Sie unter „**Foto aufnehmen**“ (S. 26).

d. **Vertrauenswürdige Nummer für den Diebstahlschutz vergeben**

Tippen Sie auf den Reiter **SMS-STEUERUNG**, geben Sie die Telefonnummer einer vertrauten Person ein oder wählen Sie sie aus den Kontakten aus und tippen Sie danach auf **NUMMER SPEICHERN**. Die Nummer sollte einen Ländercode enthalten und es kann sich dabei um die Nummer eines Freundes oder eines anderen von Ihnen genutzten Telefons handeln.

Wird eine neue SIM-Karte in Ihr Gerät eingelegt, schickt Bitdefender Mobile Security Ihnen automatisch eine Textnachricht mit der neuen Telefonnummer an die vertrauenswürdige Nummer.

Über diesen Weg können Sie SMS Nachrichten an Ihr Telefon versenden, obwohl die SIM Karte geändert wurde und die Nummer anders ist.



Wichtig

Es ist keine Pflichtangabe, aber es wird empfohlen, die vertrauenswürdige Nummer beim initialen Setup anzugeben.



Nach Aktivierung des Diebstahlschutzes können Sie die Funktionen zur Web- und SMS-Steuerung durch Antippen der entsprechenden Schaltflächen im Diebstahlschutzmenü einzeln aktivieren oder deaktivieren.



Nutzung der Diebstahlschutzfunktionen über Bitdefender Central (Web-Steuerung)



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 das -Symbol 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 das -Symbol 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.



Nutzung der Diebstahlschutzfunktionen über SMS-Befehle (SMS-Steuerung)

Ist der SMS Befehl erstmal freigegeben, können Sie folgende Nachrichten von jedem beliebigen Telefon via SMS an Ihr Smartphone versenden.

- **LOCATE** - Senden einer Nachricht an die Rufnummer des Geräts, von dem der Befehl gesendet wurde, die den Standort des Geräts benennt. Die Nachricht beinhaltet einen Google Maps Link, welcher über den Mobile-Browser des Mobiltelefons geöffnet werden kann.
- **SCREAM** - Abspielen eines lauten Signales auf dem Gerätelautsprecher.
- **LOCK** - Den Gerätebildschirm mit der von Ihnen festgelegten PIN sperren.
- **WIPE** - alle Daten vom Gerät löschen.



Wichtig

Der Befehl zum LÖSCHEN kann nur über die vertrauenswürdige Nummer verschickt werden.

- **CALLME** - Wählt die Telefonnummer von der aus der Befehl verschickt wurde mit eingeschaltetem Lautsprecher. So können Sie unbemerkt die Person belauschen, die Ihr Telefon hat.
- **HELP** - Senden einer Nachricht, die alle verfügbaren Befehle zu der Rufnummer sendet, von der diese gesendet wurde.
- **SIM Change** - An die von Ihnen festgelegte vertrauenswürdige Telefonnummer wird bei Austausch Ihrer SIM-Karte eine SMS mit der neuen Nummer gesendet. Tippen Sie auf die Option **Vertrauenswürdige Nummer**, um die Telefonnummer eines Freundes festzulegen. Sie können die Nummer von Hand eingeben oder die Person aus Ihren Kontakten auswählen.

Alle SMS Befehle müssen das folgende Format verwenden:

bd-<PIN> <command>



Beachten Sie

Die Klammern kennzeichnen Variable und sollen nicht im Befehl erscheinen.



Wenn Sie beispielsweise den Sicherheitspin auf 123456 eingestellt haben und Sie wollen eine Nachricht mit dem Standort empfangen, senden Sie die folgende Textnachricht an Ihre Rufnummer:

BD-123456 LOCATE



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. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Tippen Sie auf **AKTIVIEREN** und erlauben Sie danach Bitdefender den Zugriff auf die Nutzungsdaten, indem Sie die entsprechende Kästchen aktivieren.



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.

4. 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.



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






Sperrmodus

Hier können Sie entscheiden, wann die App-Sperre die auf Ihrem Gerät installierten Anwendungen schützen soll.

Ihnen stehen die folgenden Optionen zur Auswahl:

- **Jedes Mal sperren** - PIN oder Fingerabdruck werden für jeden Zugriff auf die gesperrten Apps abgefragt.
- **Bis zur Bildschirmabschaltung entsperrt lassen** - Sie können bis zur nächsten Bildschirmabschaltung auf die Apps zugreifen.
- **Kurzzeitiges Verlassen erlauben** - Sie können entsperrte Apps verlassen und innerhalb von 30 Sekunden wieder aufrufen.
- **Intelligentes Entsperren** - Bei Aktivierung dieser Option und Verbindung mit einem als vertrauenswürdig eingestuften Netzwerk sind die anderen Einstellungen nicht verfügbar. Beim Zugriff auf gesperrte Apps werden PIN oder Fingerabdruck also nicht abgefragt.

App-Sperre-Einstellungen

Tippen Sie auf die -Schaltfläche im App-Sperre-Menü und wählen Sie danach **Einstellungen** für die erweiterten App-Sperre-Optionen.

In den App-Sperre-**Einstellungen** ist Folgendes möglich:

- Foto nach 3 fehlgeschlagenen Entsperroversuchen aufnehmen aktivieren.
- Sperrbenachrichtigungen für neu installierte Apps.
- Ändern Sie Ihre 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 konfigurieren Sie die Foto-aufnehmen-Funktion:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Tippen Sie auf die -Schaltfläche im App-Sperre-Menü und wählen Sie **Einstellungen** aus.
4. Aktivieren Sie die Option **Foto nach 3 fehlgeschlagenen Entsperrversuchen aufnehmen**

Die Fotos, die nach Eingabe einer falschen PIN aufgenommen werden, werden im App-Sperre-Menü 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 das -Symbol und wählen Sie danach **Meine Geräte** aus.
4. Wählen Sie Ihr Gerät über das Fenster **MEINE GERÄTE** und den Reiter **Diebstahlschutz** aus.

Die Fotos werden angezeigt.

Es werden nur die 3 aktuellsten Fotos gespeichert.

Intelligentes Entsperrn

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

Mit der Funktion für das intelligente Entsperrn 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 das Intelligente Entsperren aktivieren:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Rufen Sie den Reiter **SPERRMODUS** auf und aktivieren Sie den entsprechenden Schalter.

Das gerade verwendete WLAN-Netzwerk wird angezeigt.

Tippen Sie auf das -Symbol, um die aktuell genutzte WLAN-Verbindung als vertrauenswürdig einzustufen.



Beachten Sie

Um diese Einstellung vorzunehmen, muss das intelligente Entsperren aktiviert sein.

Falls Sie es sich anders überlegen, können Sie die Funktion jederzeit deaktivieren. Alle bisher als vertrauenswürdig eingestuftes 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. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Berichte** aus der Liste aus.

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.

- **AKTIVITÄTSPROTOKOLL** - Hier können Sie ausführliche Informationen zu den Aktivitäten Ihrer Bitdefender Mobile Security-App seit Installation auf Ihrem Android-Gerät einsehen.

Tippen Sie auf die -Schaltfläche oben rechts auf Ihrem Bildschirm und wählen Sie danach **Aktivitätsprotokoll leeren** aus, um das vorliegende Aktivitätsprotokoll zu löschen.



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-Anwendung 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 Ihre Smartwatch tragen, erkennt sie automatisch die Anwendung auf Ihrem Telefon und vibriert, sobald Sie sich mehr als zehn Meter von Ihrem Telefon entfernen.

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. EINSTELLUNGEN

Im Bereich Einstellungen können Sie die folgenden Optionen anpassen:

- **Sicherheits-PIN** - Hier können Sie den PIN-Code ändern, den Sie für die App-Sperre oder die Diebstahlschutzbefehle festgelegt haben.
- **Virenschanner** - Hier können Sie festlegen, ob der Speicher geprüft werden soll.
- **In-the-Cloud-Erkennung** - Hier können Sie festlegen, ob uns Berichte übermittelt werden, die uns bei der Verbesserung der Cloud-Erkennung unterstützen.
- **Kontoschutz** - Hier können Sie festlegen, ob Sie auch informiert werden möchten, wenn Ihre Benutzerkonten von Datenpannen nicht betroffen sind.
- **App-Sperre** - Hier können Sie festlegen, ob für neu installierte Apps Sperrbenachrichtigungen angezeigt werden sollen.
- **Foto aufnehmen** - Hier können Sie festlegen, ob nach drei fehlgeschlagenen App-Aufrufen ein Foto aufgenommen werden soll.
- **Diebstahlschutz** - Hier können Sie die vertrauenswürdige Telefonnummer ändern, die Sie für den Fall angegeben haben, dass Ihr Gerät in fremde Hände gerät.
- **Berichte** - Hier können Sie festlegen, ob Sie Benachrichtigungen zu Berichten erhalten möchten.
- **Anonyme Nutzungsstatistiken senden** - Hier können Sie festlegen, ob uns Berichte mit Informationen zu Ihrer Produktnutzung übermittelt werden. Diese Information leisten einen wichtigen Beitrag zur Verbesserung des Produkts und helfen uns, die Benutzererfahrung immer weiter zu verbessern.



12. INFO ÜBER

Informationen zur installierten Bitdefender Mobile Security-Version finden Sie im Bereich **Info über**. Hier können Sie uns auch mit Support-Anfragen kontaktieren, die Abonnementvereinbarung sowie die Datenschutzrichtlinie aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.



13. 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 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. Nachdem Sie es aufgerufen 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.

Aufrufen Ihres Bitdefender-Benutzerkontos.

So können Sie Ihr Bitdefender-Benutzerkonto bequem aufrufen:



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.

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 Gerätename, 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 das -Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und tippen Sie dann 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 das -Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
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 die Schaltfläche **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. 18).

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 das -Symbol 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).



Abonnement verlängern

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 das -Symbol 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.



14. 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.
- SMS lesen/schreiben, Kontakte, Kontoinformationen und externe Speicher -> wird für die Fernlöscher-Funktion benötigt.
- Ortung -> für die Fern-Geräteortung.
- Kamera -> wird für die Funktion Foto aufnehmen benötigt.
- Speicher -> wird benötigt, um dem Virenschanner die Prüfung der SD-Karte zu erlauben.

Wo kann ich Einzelheiten zu den Aktivitäten der App einsehen?

Bitdefender Mobile Security führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Rufen Sie diese Informationen auf, indem Sie Bitdefender Mobile Security öffnen und auf die **Menü**-Schaltfläche tippen. Wählen Sie **Berichte** aus der Liste aus.

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 das -Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Sie können den PIN-Code im Feld **Anwendungs-PIN** abrufen.

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.

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?


So können Sie ein weiteres WLAN-Netzwerk als vertrauenswürdig festlegen:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Rufen Sie den Reiter **SPERRMODUS** auf und tippen Sie danach auf das -Symbol.
4. Bestätigen Sie Ihre Auswahl mit Ihrer PIN oder Ihrem Fingerabdruck.
5. Tippen Sie auf das -Symbol neben dem Netzwerk, das Sie als vertrauenswürdig einstufen möchten.

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 dem Bildschirm auf das Symbol .
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. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Mein Konto** aus der Liste aus.
3. Tippen Sie auf **ABMELDEN** und bestätigen Sie Ihre Auswahl.
4. Tippen Sie auf **CENTRAL-KONTO VERWENDEN** und geben Sie danach Ihre neue Bitdefender-E-Mail-Adresse und Ihr Passwort ein.

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**.

Wofür wird die vertrauenswürdige Nummer benötigt?



Falls Ihr Telefon jemandem in die Hände fällt, der keinerlei Absichten hat, es dem rechtmäßigen Besitzer zurückzugeben, ist es sehr wahrscheinlich, dass Ihre SIM-Karte umgehend ausgetauscht wird. Sobald Bitdefender Mobile Security erkennt, dass die SIM-Karte in Ihrem Telefon ausgetauscht wurde, schickt es automatisch eine Textnachricht mit der neuen Nummer an die von Ihnen festgelegte Nummer. So können Sie auch nach Austausch der SIM-Karte SMS-Befehle an die neue Nummer Ihres Telefons schicken. Sie können dafür die Nummer einer vertrauten Person oder auch die Nummer eines weiteren von Ihnen genutzten Telefons verwenden.

Kann die vertrauenswürdige Nummer später auch wieder geändert werden?

So legen Sie eine neue vertrauenswürdige Nummer fest:

1. Bitdefender Mobile Security öffnen.
2. Tippen Sie auf **Menü** und wählen Sie **Einstellungen** aus der Liste aus.
3. Tippen Sie im Bereich **Diebstahlschutz** auf **Vertrauenswürdige Nummer**.

Bevor Sie die vertrauenswürdige Nummer ändern können, müssen Sie die PIN eingeben.

Was kostet mich der Versand von SMS-Befehlen?

SMS-Befehle werden als herkömmliche Textnachrichten versandt und werden auch als solche von Ihrem Anbieter abgerechnet. Durch Bitdefender entstehen Ihnen keine zusätzlichen Kosten.

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
- Spanish
- 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.



15. 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/>.