BENUTZERHANDBUCH

Bitdefender CONSUMER SOLUTIONS

Mobile Security

Bitdefender Mobile Security

Bedienungsanleitung

Veröffentlichungsdatum: 02.10.2023

Impressum

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle Android-Benutzer, die sich für den Einsatz von Bitdefender Mobile Security als Sicherheitslösung für ihre Mobilgeräte entschieden haben. Die enthaltenen Informationen setzen keine besonderen technischen Kenntnisse voraus, sondern dienen allen im Umgang mit Android-Geräten erfahrenen Benutzern als leicht verständliche Anleitung.

Lesen Sie, wie Sie Bitdefender Mobile Security konfigurieren und einsetzen, um sich vor Bedrohungen und Malware zu schützen. Wir zeigen Ihnen, wie Sie alles aus Bitdefender herausholen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 5)

Starten mit Bitdefender Mobile Security und der Benutzeroberfläche.

Funktionen und Merkmale (Seite 11)

Erfahren Sie, wie Sie sich mit Bitdefender Mobile Security vor Bedrohungen und Malware schützen können, indem Sie sich mit den Funktionen und Merkmalen des Programms vertraut machen.

Hilfe und Support (Seite 52)

Hinweise zu nützlichen Informationen und Hilfestellungen bei unerwarteten Problemen.

Konventionen in diesem Handbuch

Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der untenstehenden Tabelle entnehmen.

Erscheinungsbild	Beschreibung
Beispielsyntax	Syntaxbeispiele werden in einer Schriftart mit fester Laufweite angegeben.
https://www.bitdefender.de	Verweise (Links) auf externe Inhalte auf HTTP- oder FTP-Servern.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z. B. zur Kontaktaufnahme.
Über diese Anleitung (Seite 1)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Dateiname	Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben.

Zusätzliche Hinweise

Zusätzliche Hinweise sind im Text grafisch markiert und liefern ergänzende Informationen zum aktuellen Absatz, die Sie unbedingt beachten sollten.

Hinweis

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Schicken Sie uns Ihre E-Mail an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

1. WAS IST BITDEFENDER MOBILE SECURITY?

Über das Internet kann man schnell und bequem Rechnungen bezahlen, Urlaube buchen sowie Waren und Dienstleistungen erwerben. Die verstärkte Nutzung dieser Online-Dienste geht jedoch auch mit hohen Risiken einher. Ohne die entsprechenden Sicherheitsvorkehrungen können personenbezogene Daten schnell in die falschen Hände gelangen. Was ist also wichtiger, als der Schutz der Daten, die in unseren Online-Konten und Smartphones zu finden sind?

Mit **Bitdefender Mobile Security** können Sie:

- Ihr Android-Smartphone und -Tablet mit minimalen Auswirkungen auf die Akkulaufzeit optimal schützen
- sich vor Handybetrug mit gefährlichen Links schützen
- unser sicheres VPN für schnelles, anonymes und sorgenfreies Surfen im Netz nutzen
- Im Falle von Diebstahl oder Verlust können Sie Ihr Android-Gerät jederzeit per Fernzugriff orten, sperren oder sämtliche Daten löschen
- überprüfen, ob Ihr E-Mail-Konto von Datenpannen oder Datenlecks betroffen ist

2. ERSTE SCHRITTE

2.1. Systemanforderungen

Bitdefender Mobile Security läuft auf allen Geräten ab Android 5.0. Für Bedrohungs-Scans über die Cloud wird eine aktive Internet-Verbindung benötigt.

2.2. So installieren Sie 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. Rufen Sie den Bereich **Meine Geräte** auf.
    4. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann 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.
  - Unter Windows, macOS und iOS
    1. Gehe zu: https://central.bitdefender.com.
    2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
    3. Wähle aus **Meine Geräte** Tafel.
    4. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann 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 aufzurufen und zu installieren.
  Sie können auch den QR-Code einscannen:

  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.

2.3. 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 versuchen, sich automatisch bei diesem Konto anzumelden.

So verknüpfen Sie Ihr Gerät mit einem Bitdefender-Konto:

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 melded 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.

> **Notiz**
> 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.

2.4. Den 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 App 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.

- **Virenscanner**. 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.

2.5. Dashboard

Tippen Sie in der App-Übersicht Ihres Geräts auf das Symbol für Bitdefender Mobile Security, um die App zu öffnen.

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, liefert der Bitdefender-Autopilot 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:

Virenscanner

Hiermit können Sie Bedarf-Scans starten oder Speicher-Scans aktivieren. Weitere Informationen finden Sie im Kapitel Virenscanner (Seite 11).

Internet-Schutz

Lässt Sie sicher im Web surfen, indem er Sie vor potenziell schädlichen Seiten warnt. Weitere Informationen finden Sie im Kapitel Internet-Schutz (Seite 13).

VPN

Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter VPN (Seite 15).

Betrugswarnung

Schützt Sie, indem es Sie vor schädlichen Links warnt, die per SMS, Messaging-Anwendungen und Arten von Benachrichtigungen eingehen. Weitere Informationen finden Sie unter Betrugswarnung (Seite 18).

Diebstahlschutz

Hiermit können Sie die Diebstahlschutzfunktionen aktivieren und deaktivieren und die Einstellungen für den Diebstahlschutz konfigurieren. Weitere Informationen finden Sie im Kapitel Diebstahlschutz-Funktionen (Seite 21).

Kontoschutz

Prüft, ob die Datensicherheit Ihrer Online-Konten kompromittiert wurde. Weitere Informationen finden Sie im Kapitel Kontoschutz (Seite 25).

App-Sperre

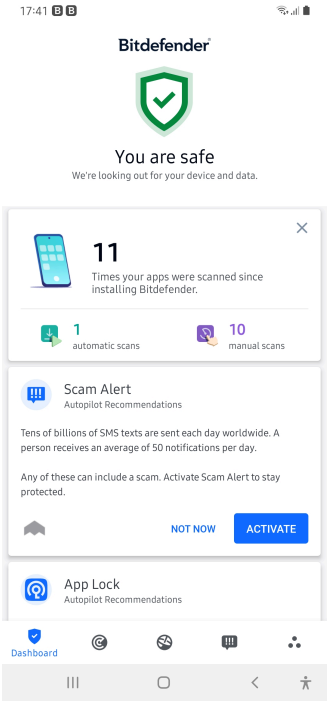
Hiermit können Sie Ihre installierten Anwendungen durch Festlegung einer PIN für den Zugriff schützen. Weitere Informationen finden Sie im Kapitel App-Sperre (Seite 27).

Berichte

Zeichnet alle wichtigen Aktionen, Statusänderungen und andere kritische Meldungen im Zusammenhang mit der Aktivität Ihres Geräts auf. Weitere Informationen finden Sie unter Berichte (Seite 31).

WearON

Kommuniziert mit Ihrer Smartwatch, damit Sie Ihr Telefon schneller wiederfinden können. Weitere Informationen finden Sie im Kapitel WearON (Seite 32).


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

3. FUNKTIONEN UND MERKMALE

3.1. Virenscanner

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

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

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

- **Scans bei Installation**
  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.
- **Bedarf-Scans**
  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 **Virenscanner** in
  2. Tippen Sie auf **SCAN STARTEN**.

Notiz

Für den Virenscanner 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.

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.

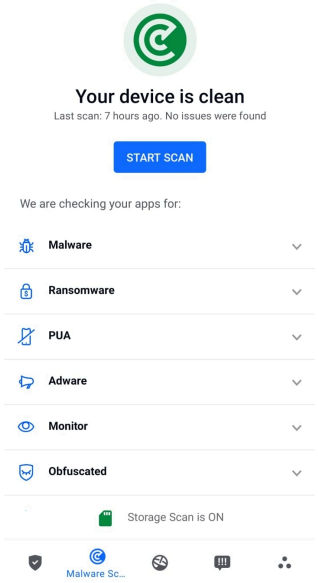
So können Sie die Einstellung Speicher prüfen deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf **Mehr**.
2. Tippen Sie auf **Einstellungen**.
3. Deaktivieren Sie im Bereich Virenscanner 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 Virenscanner-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 Virenscanner 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 .



3.1.1. Erkennung von App-Anomalien

Bitdefender App Anomaly Detection ist eine neuartige Technologie, die in den Bitdefender Malware Scanner integriert ist und durch kontinuierliche Überwachung und Erkennung böswilliger Verhaltensweisen eine zusätzliche Schutzebene bietet und den Benutzer benachrichtigt, wenn verdächtige Aktivitäten erkannt werden.

Die App-Anomalieerkennung von Bitdefender schützt Benutzer auch dann, wenn sie unwissentlich eine gefährliche App installiert haben, die eine Zeit lang inaktiv läuft, oder eine scheinbar vertrauenswürdige App, die ihre Funktionalität beeinträchtigt und böswillig wird.

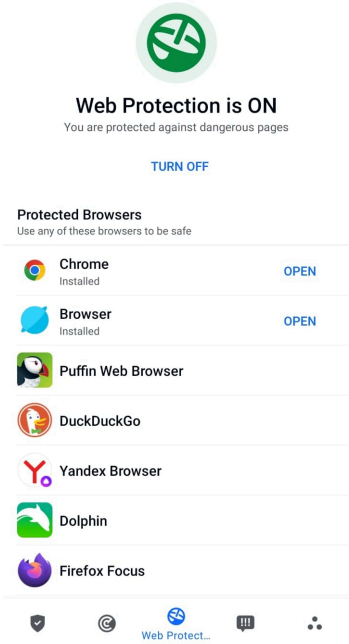
3.2. Internet-Schutz

Der Internet-Schutz nutzt die Bitdefender-Cloud-Dienste, um die von Ihnen im Standard-Android-Browser, in Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser und Dolphin aufgerufenen Webseiten zu überprüfen.

Notiz

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 Internet-Schutz von Bitdefender 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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Internet-Schutz.

3.3. 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 bedauerliche Vorfälle 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 VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

> **Notiz**
> In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, 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 danach 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.

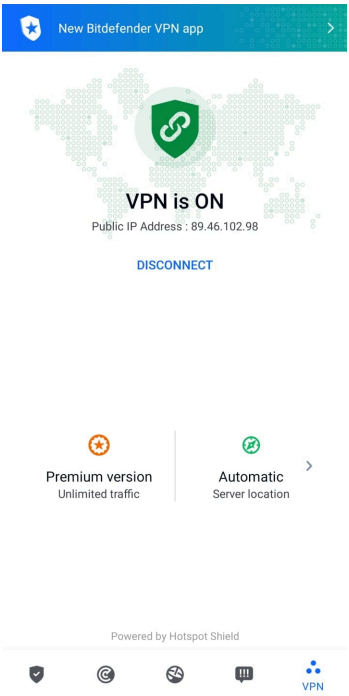
> **Notiz**
> Wenn Sie VPN das erste Mal einschalten, werden Sie gebeten, Bitdefender zu erlauben, eine VPN-Verbindung herzustellen, die den Netzwerkdatenverkehr überwacht. Tippen Sie auf **OK** um fortzufahren.

Auf Geräten ab Android 7.1 können Sie eine Verknüpfung zu Bitdefender VPN nutzen, ohne die Bitdefender Mobile Security-App öffnen zu müssen.

Halten Sie einfach das Symbol Bitdefender auf Ihrem Startbildschirm oder in Ihrem App-Drawer, und wählen Sie dann das Symbol .

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



3.3.1. VPN-Einstellungen

Für eine erweiterte Konfiguration Ihres VPN:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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.

3.3.2. 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 VPN-Fenster auf **Premium aktivieren** tippen.

Das Bitdefender Premium VPN-Abonnement ist nicht an das Bitdefender Mobile Security-Abonnement gebunden, d. h. Sie können es während der gesamten Laufzeit nutzen, unabhängig vom Status Ihres Sicherheitsabonnements. Falls das Bitdefender Premium VPN-Abonnement ausläuft, aber das Abonnement für Bitdefender Mobile Security noch aktiv ist, werden Sie wieder auf die kostenlose Version umgestellt.

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.

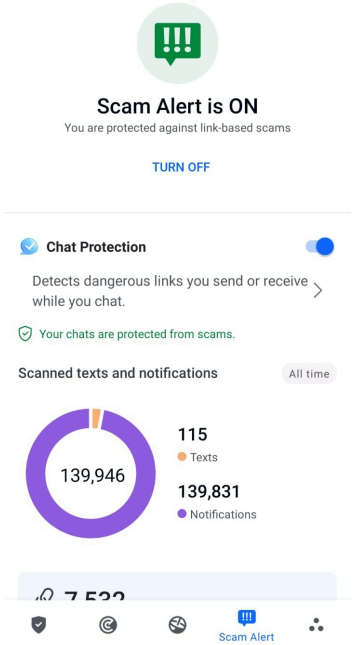
> **Notiz**
> Bitdefender VPN ist auch als eigenständige Anwendung auf allen unterstützten Betriebssystemen einsetzbar, d. h. unter Windows, macOS, Android und iOS.

3.4. Betrugswarnung

Die Betrugswarnung dient der Prävention von potenziell gefährlichen Situationen, bevor sie zum Problem werden können, so auch Malware-Bedrohungen. Die Betrugswarnung überwacht alle eingehenden SMS-Nachrichten und Android-Benachrichtigungen in Echtzeit.

Sie werden per Warnmeldung über den Eingang von Benachrichtigungen mit gefährlichen Links informiert. Bitdefender bietet Ihnen dann zwei Optionen an. Sie können die Information ignorieren oder die **DETAILS ANZEIGEN**. Dadurch erhalten Sie weitere Informationen über den Vorfall sowie wichtige Empfehlungen, wie z. B.:

- Öffnen Sie den gefundenen Link nicht und leiten Sie ihn nicht weiter.
- Löschen Sie im Falle von SMS wenn möglich die gesamte Nachricht.
- Blockieren Sie den Absender, wenn es sich dabei nicht um einen Kontakt handelt, den Sie kennen und dem Sie vertrauen.
- Löschen Sie die App, die gefährliche Links über Benachrichtigungen verschickt.



Notiz

Einschränkungen im Android-Betriebssystem verhindern, dass Bitdefender Textnachrichten löschen oder andere direkte Maßnahmen in Bezug auf SMS-Nachrichten und weitere Quellen gefährlicher Benachrichtigungen ergreifen kann. Wenn Sie die Warnmeldung der Betrugswarnung ignorieren und versuchen, gefährliche Link dennoch zu öffnen, wird der Internet-Schutz von Bitdefender diese automatisch erkennen und verhindern, dass Ihr Gerät infiziert wird.

3.4.1. Aktivieren der Betrugswarnung

Um die Betrugswarnung zu aktivieren, müssen Sie der Bitdefender Mobile Security-App Zugriff auf die SMS-Nachrichten und das Benachrichtigungssystem gewähren:

1. Öffnen Sie die auf Ihrem Android-Telefon oder -Tablet installierte Bitdefender Mobile Security-App.
2. Tippen Sie im Hauptfenster der Bitdefender-App in der unteren Navigationsleiste auf die Option **Betrugswarnung** und dann auf **AKTIVIEREN**.
3. Tippen Sie auf **ZULASSEN**.
4. Setzen Sie Bitdefender Security in der Liste der Apps mit Zugriff auf Benachrichtigungen auf die Position **EIN**.
5. Tippen Sie zur Bestätigung auf **ZULASSEN**.
6. Kehren Sie zum Bildschirm Betrugswarnung zurück und tippen Sie auf **ZULASSEN**, damit Bitdefender eingehende SMS-Nachrichten scannen kann.

3.4.2. Echtzeit-Chat-Schutz

Chat-Nachrichten sind die wohl bequemste Möglichkeit, um mit Freunden und Familie in Kontakt zu bleiben. Sie sind aber auch ein Einfallstor für gefährliche Links.

Wenn Sie die Chat-Schutzfunktion aktivieren, schützt die Betrugswarnung nicht nur Ihre Textnachrichten und Benachrichtigungen, sondern auch Ihre Chats vor linkbasierten Angriffen, indem es gefährliche Links erkennt, die Sie beim Chatten senden oder empfangen.

So aktivieren Sie den Chat-Schutz:

1. Öffnen Sie die auf Ihrem Android-Telefon oder -Tablet installierte Bitdefender Mobile Security-App.
2. Tippen Sie im Hauptfenster der Bitdefender-App in der unteren Navigationsleiste auf die Option **Betrugswarnung**.
3. Oben im Reiter Betrugswarnung finden Sie die Option Chat-Schutz. Setzen Sie den entsprechenden Schalter auf **EIN**.

Notiz

Derzeit ist der Chat-Schutz mit den folgenden Anwendungen kompatibel:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

3.5. 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.

Notiz

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 Diebstahlschutz-Funktionen:

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, auf welche Weise Bitdefender den Standort bestimmt:

- 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 eine lauten Ton abspielen lassen. Der Ton wird abgespielt, auch wenn das Gerät auf lautlos gestellt ist.

3.5.1. 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. Klopfen **Mehr** in der unteren Navigationsleiste.
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:

Notiz

Für den Diebstahlschutz werden unter Android 6 zusätzliche Berechtigungen benötigt.

Um sie zu aktivieren, gehen Sie folgendermaßen vor:

a. Tippen Sie 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 Fingerabdruckerkennung 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. Gehe zu: https://central.bitdefender.com.

ii. Melden Sie sich bei Ihrem Konto an.

iii. Wähle aus **Meine Geräte** Tafel.

iv. Wählen Sie Ihr Android-Gerät aus und wechseln Sie dann zum Reiter **Diebstahlschutz**.

v. Tippen Sie neben **Aufnahmen einsehen** auf ⋮, um die zuletzt aufgenommenen Fotos anzuzeigen.
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.

3.5.2. Zugriff auf Diebstahlschutz-Funktionen über Bitdefender Central

> **Notiz**
> 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. Wähle aus **Meine Geräte** Tafel.
3. Wählen Sie im Fenster **MEINE GERÄTE** die gewünschte Gerätekarte, indem Sie auf die entsprechende Schaltfläche **Details anzeigen** tippen.
4. Wechseln Sie zum Reiter **Diebstahlschutz**.
5. Tippen Sie auf die Schaltfläche, die der gewünschten Funktion entspricht:
   Orten - zeigt den Standort Ihres Geräts auf Google Maps.
   IP ANZEIGEN - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.
   Alarm - Sie können eine Nachricht eingeben, die auf dem Bildschirm Ihres Geräts angezeigt werden soll, und/oder das Gerät einen Alarmton abspielen lassen.
   Sperren - Ihr Gerät sperren und einen PIN-Code zum Entsperren festlegen.

Daten löschen - alle Daten von Ihrem Gerät löschen.

> **Wichtig**
> Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

3.5.3. Diebstahlschutz-Einstellungen

So können Sie die Fernbefehle aktivieren oder deaktivieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Diebstahlschutz**.
3. Aktivieren oder deaktivieren Sie die gewünschten Optionen.

3.6. Kontoschutz

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. 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. Klopfen **Mehr** in der unteren Navigationsleiste.
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.
- Verwendenden 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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Konto Privatsphäre**.
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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Kontoschutz.

3.7. 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.

Die biometrische Authentifizierung (z. B. Bestätigung per Fingerabdruck oder Gesichtserkennung) kann anstelle des festgelegten PIN-Codes verwendet werden.

3.7.1. 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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf **App-Sperre**.
3. Klopfen **ANMACHEN**.
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**.

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

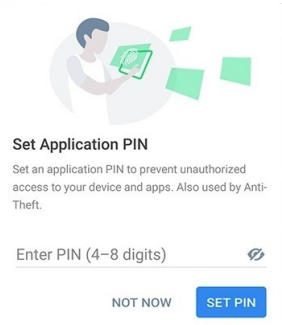
7. Aktivieren Sie die Option Foto aufnehmen, um Eindringlinge zu erwischen, die versuchen, auf Ihre privaten Daten zuzugreifen.

> **Notiz**
> 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.

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



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

3.7.3. App-Sperre-Einstellungen

Für eine erweiterte Konfiguration der App-Sperre:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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.

3.7.4. 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.

> **Notiz**
> Diese Funktion steht nur auf Telefonen mit Frontkamera zur Verfügung.

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

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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. Gehe zu: https://central.bitdefender.com.
2. Melden Sie sich bei Ihrem Konto an.
3. Rufen Sie den Bereich **Meine Geräte** auf.
4. Wählen Sie Ihr Android-Gerät und dann die **Diebstahlschutz** Tab.
5. Klopfen neben **Überprüfen Sie Ihre Schnappschüsse** , um die zuletzt aufgenommenen Fotos anzuzeigen.

Nur die beiden neuesten Fotos werden gespeichert.

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

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.

3. Deaktivieren Sie im Bereich Foto aufnehmen die Option **Fotos hochladen**.

3.7.5. 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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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.

3.8. 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. Klopfen **Mehr** in der unteren Navigationsleiste.
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. Klopfen **Mehr** in der unteren Navigationsleiste.
  2. Klopfen **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. Klopfen **Mehr** in der unteren Navigationsleiste.
  2. Klopfen **Einstellungen**.
  3. Tippen Sie auf **Aktivitätsprotokoll löschen** und danach auf **LÖSCHEN**.

3.9. WearON

Mit Bitdefender WearON können Sie Ihr Smartphone schnell und einfach wiederfinden, egal ob Sie es bei der Arbeit im Besprechungsraum oder unter eine 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.

Notiz
Diese Funktion benötigt Android 4.3 und Android Wear.

3.9.1. 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: <Wo ist mein Telefon>

Bitdefender WearON verfügt über zwei Befehle:

1. **Telefonalarm**
   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.

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

4. ÜBER BITDEFENDER CENTRAL

Bitdefender Central ist die Plattform, über die Sie Zugriff auf sämtliche Online-Funktionen und -Dienste des Produkts haben und über die Sie wichtige Aktionen auch per Fernzugriff auf Geräten ausführen können, auf denen Bitdefender installiert ist. Unter https://central.bitdefender.com können Sie sich von jedem mit dem Internet verbunden Computer oder Mobilgerät aus bei Ihrem Bitdefender-Konto anmelden. Auf Android- und iOS-Geräten können Sie Bitdefender Central auch über die dazugehörige App aufrufen.

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 for Android
  - Bitdefender Mobile Security for iOS
  - Die Bitdefender-Produktlinie für Windows
  - Bitdefender Antivirus for Mac
- 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.

4.1. Aufrufen von Bitdefender Central

Sie haben zwei Möglichkeiten zum Aufrufen von Bitdefender Central

- Über Ihren Web-Browser:
  1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
  2. Gehe 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 von Ihnen installierte Bitdefender Central-App.

  Notiz
  Hier finden Sie alle Optionen, die Ihnen über die Web-Oberfläche zur Verfügung gestellt werden.

4.2. Zwei-Faktor-Authentifzierung

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.

4.2.1. 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. Zugang Bitdefender-Zentrale.
2. Tippen Sie oben rechts auf dem Bildschirm auf das Symbol .
3. Tippen Sie im Schiebemenü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.

5. Klopfen **LOSLEGEN**.
   Wählen Sie eine der folgenden Methoden aus:

   - **Authentifizierungsanwendung** - Verwenden Sie eine Authentifizierungsanwendung, 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 **AUTHENTIFIZIERUNGSANWENDUNG 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 **Fortfahren**

     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. Rufen Sie Ihre E-Mails ab und verwenden Sie den erhaltenen Code.

     a. Tippen Sie zunächst auf **E-MAIL VERWENDEN**.

     b. Rufen Sie Ihre E-Mails ab, 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 Aktivierungscodes. 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 Authentifizierungscodes 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.

4.3. 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. Zugang Bitdefender-Zentrale.
2. Tippen Sie auf die Symbol oben rechts auf dem Bildschirm.
3. Klopfen **Bitdefender-Konto** im Folienmenü.
4. Wähle aus **Passwort und Sicherheit** Tab.
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.

4.4. 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.

4.4.1. Hinzufügen eines neuen Geräts

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Mobile Security installieren. Gehen Sie dazu wie folgt vor:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Bedienfeld und tippen Sie dann auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:

   - **Schützen Sie dieses Gerät**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.

   - **Schützen Sie andere Geräte**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
     Klicken Sie auf **DOWNLOAD LINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken 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.
     Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und tippen Sie dann auf die entsprechende Download-Schaltfläche.

4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

4.4.2. Persönliche Anpassungen

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

1. Zugang Bitdefender Central.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Wählen Sie **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und klicken Sie dann auf **SPEICHERN**.

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

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekarte und dann auf ⋮ Symbol in der oberen rechten Ecke des Bildschirms.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie im Anschluss die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen, einen Geburtstag auswählen und eine E-Mail-Adresse sowie eine Telefonnummer eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der Liste der **Gerätebesitzer** den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

4.4.3. Fernzugriffsaktionen

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Tafel.

3. Tippen Sie auf die gewünschte Gerätekarte und dann auf ⋮ Symbol in der oberen rechten Ecke des Bildschirms.
4. Wählen Sie **Update**.

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

Klicken Sie auf eine Gerätekarte, 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, klicken Sie auf das Klappmenü oben im Statusbereich, um mehr Details dazu anzuzeigen. Hier können Sie
- **Schutz.** Von diesem Fenster aus können Sie Quick- und System-Scans 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.
- **Optimierung.** Hier können Sie per Fernzugriff die Leistung eines Geräts verbessern, indem Sie nicht mehr benötigte Dateien schnell und einfach aufspüren und entfernen. Klicken Sie auf **START** und wählen Sie dann die Bereiche aus, die Sie optimieren möchten. Klicken Sie erneut auf **START**, um den Optimierungsvorgang zu starten. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht mit Informationen zu den behobenen Probleme aufzurufen.
- **Diebstahlschutz.** Falls Sie Ihr Gerät verlegen oder verlieren oder sollte es gestohlen werden, hilft Ihnen die Diebstahlschutzfunktion Ihr Gerät zu orten und per Fernzugriff bestimmte Aktionen durchzuführen. Klicken Sie auf **ORTEN**, um den Standort des Geräts zu ermitteln. Der letzte bekannte Standort wird zusammen mit Uhrzeit und Datum angezeigt.
- **Schwachstelle**. Um ein Gerät auf Schwachstellen wie fehlende Windows-Updates, veraltete Anwendungen oder unsichere Passwörter zu überprüfen, klicken Sie im Reiter Schwachstellen auf **SCANNEN**.

Schwachstellen können nicht per Fernzugriff behoben werden. Falls eine Schwachstelle gefunden wird, müssen Sie einen erneuen Scan auf dem Gerät durchführen und dann die empfohlenen Maßnahmen ergreifen. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht über die gefundenen Probleme aufzurufen.

4.5. Aktivität

Im Bereich Aktivität können Sie Informationen zu den Geräten einsehen, auf denen Bitdefender installiert ist.

Im Fenster **Aktivität** können Sie auf die folgenden Kacheln zugreifen:

- **Meine Geräte.** Hier können Sie die Anzahl der verbundenen Geräte sowie ihren jeweiligen Schutzstatus anzeigen. Um per Fernzugriff Probleme auf den erkannten Geräten zu beheben, klicken Sie auf **Probleme beheben** und dann auf **SCANNEN UND PROBLEME BEHEBEN**.

  Um Details zu den erkannten Problemen anzuzeigen, klicken Sie auf **Probleme anzeigen**.

  Von iOS-Geräten können keine Informationen zu erkannten Bedrohungen abgerufen werden.

- **Bedrohungen blockiert.** Hier können Sie ein Diagramm mit einer Gesamtstatistik mit Informationen über die blockierten Bedrohungen der letzten 24 Stunden bzw. 7 Tage anzeigen. Die angezeigten Informationen werden abhängig von dem schädlichen Verhalten abgerufen, das bei den aufgerufenen Dateien, Anwendungen und URLs erkannt wurde.

- **Benutzer mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Anwendern anzeigen, bei denen die meisten Bedrohungen gefunden wurden.

- **Geräte mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Geräten anzeigen, auf denen die meisten Bedrohungen gefunden wurden.

4.6. Meine Abonnements

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

4.6.1. Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Zugang Bitdefender Central.
2. Rufen Sie den Bereich **Meine Abonnements** auf.

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.

> **Hinweis**
> Es ist möglich, eine oder mehrere Abonnements unter einem Benutzerkonto zu vereinen, vorausgesetzt, dass diese für verschiedene Plattformen (Windows, macOS, iOS oder Android) gültig sind.

4.6.2. Abonnement aktivieren

Sie können ein Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Sobald die Aktivierung abgeschlossen ist, beginnt die Laufzeit des Abonnements.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. 2Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert.

4.6.3. Abonnement verlängern

Falls Sie die automatische Verlängerung Ihres Bitdefender-Abonnements deaktiviert haben, können Sie es auch selbst verlängern. Gehen Sie dazu wie folgt vor:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.
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.

4.7. Benachrichtigungen

Über das -Symbol bleiben Sie immer auf dem Laufenden, was auf den mit Ihrem Konto verbundenen Geräten passiert. Ein Klick auf dieses Symbol gibt Ihnen einen groben Überblick über die Aktivitäten der Bitdefender-Produkte, die auf Ihren Geräten installiert sind.

5. HÄUFIG GESTELLTE FRAGEN

Wofür 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 benötigt Bitdefender Mobile Security die einzelnen Berechtigungen?

- Internet-Zugang -> dient der Kommunikation mit der Cloud.
- 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 -> erlaubt dem Internet-Schutz schädliche Websites aus dem Browser-Verlauf zu löschen.
- Protokolle lesen -> anhand der Android-Protokolle kann Bitdefender Mobile Security Malware-Aktivität erkennen.
- Standort -> dient der Standortermittlung per Fernzugriff.
- Kamera -> wird für die Funktion Foto aufnehmen benötigt.
- Speicher -> wird benötigt, um dem Virenscanner 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. Falls Sie uns keine Informationen über verdächtige Anwendungen mehr schicken möchten. Gehen Sie wie folgt vor, falls Sie uns keine Informationen über verdächtige Apps mehr übermitteln möchten:

1. Klopfen **Mehr** in der unteren Navigationsleiste.

2. Klopfen **Einstellungen**.
3. Deaktivieren Sie im Bereich Virenscanner 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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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. Zugang Bitdefender-Zentrale.
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekachel und dann oben rechts auf ⋮.
4. Wählen **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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **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. Zugang Bitdefender-Zentrale.
2. Tippen Sie oben rechts auf dem Bildschirm auf .
3. Klicken Sie im Schiebemenü auf **Einstellungen**.
4. 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 verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz 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 Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Warum 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 zum 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 mit meinem Gerät verknüpfte Bitdefender-Konto ändern?

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

1. Klopfen **Mehr** in der unteren Navigationsleiste.
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**.

Welche Auswirkungen hat Bitdefender Mobile Security auf die Leistung und die Batterielebensdauer meines Geräts?

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 ein Geräteadministrator?

Geräteadministrator ist eine Android-Funktion, über die Bitdefender Mobile Security die Berechtigungen erhält, die es zur Ausführung bestimmter Aktionen per Fernzugriff benötigt. Ohne diese Berechtigungen könnte die Fernsperrung nicht funktionieren und die Fernlöschung könnte Ihre Daten nicht löschen. Sollten Sie die App entfernen wollen, müssen Sie vor der Deinstallation diese Berechtigungen wieder entziehen unter **Einstellungen > Sicherheit > Geräteadministratoren auswählen**.

Behebung des "Kein Google-Token"-Fehlers, der bei der Anmeldung bei Bitdefender Mobile Security 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:

- Rufen Sie Android-Einstellungen > Anwendungen > Anwendungen verwalten > Bitdefender Mobile Security auf und tippen Sie auf **Daten löschen**. Melden Sie sich dann erneut an.
- Ihr Gerät muss mit einem Google-Konto verknüpft sein.
  Sie können das überprüfen, indem Sie Einstellungen -> Konten & Synchronisierung aufrufen und dort nachsehen, ob unter **Konten verwalten** ein Google-Konto aufgeführt ist. Fügen Sie Ihr Konto hinzu, falls es nicht aufgeführt ist, starten Sie 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 erhältlich?

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
- Schwedisch

- Thai
- Türkisch
- Vietnamesisch

Weitere Sprachen werden in zukünftigen Versionen hinzukommen. Um die Sprache der Bitdefender Mobile Security-Oberfläche zu ändern, rufen Sie die Einstellungen **Sprache & Tastatur** Ihres Geräts auf und legen Sie die gewünschte Sprache fest.

6. HILFE UND SUPPORT

6.1. Hier wird Ihnen geholfen

Bitdefender bietet seinen Kunden einen konkurrenzlos schnellen und kompetenten Support. Wenn Sie ein Problem oder eine Frage zu Ihrem Bitdefender-Produkt haben, können Sie verschiedene Online-Ressourcen nutzen, um eine Lösung bzw. eine Antwort zu finden. Darüber hinaus können Sie sich jederzeit an den Bitdefender-Kundendienst wenden. Unsere Support-Mitarbeiter werden Ihre Fragen zeitnah beantworten und Ihnen die notwendige Unterstützung bieten.

6.2. Online-Ressourcen

Bei Problemen und Fragen in Zusammenhang mit Bitdefender stehen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:
  https://www.bitdefender.de/consumer/support/
- Die Bitdefender Expert Community:
  https://community.bitdefender.com/de
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Weitere Informationen über Computersicherheit, Bitdefender-Produkte und unsere Firma finden Sie über Ihre Lieblingssuchmaschine.

6.2.1. 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.

Die Bitdefender Support Center ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische

Grundlagen und Fachwissen über unsere Produkte zu erlangen. Alle berechtigen 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 ist jederzeit unter der folgenden Adresse erreichbar: https://www.bitdefender.de/consumer/support/.

6.2.2. Die Bitdefender Experten Community

Die Experten-Community ist eine Plattform, auf der sich Bitdefender-Experten, -Anwender und -Fans einbringen, Ideen austauschen, sich gegenseitig unterstützen und ihr Wissen und ihre Lösungen mit anderen teilen. Hier werden zudem viele Ideen geboren und unsere Entwickler finden wichtiges Feedback. Unsere Community-Mitglieder sind erfahrene Bitdefender-Anwender, die Freude daran haben, anderen zu helfen. Dank ihres unschätzbaren Beitrags und ihres freiwilligen Engagements konnten wir eine Wissensdatenbank schaffen, in der Anwender nützliche Antworten und Anleitungen finden können, aber auch das Zwischenmenschliche seinen Platz hat.

Hier können Sie in einen echten Austausch mit Menschen treten, die Bitdefender selbst auf ihren Geräten nutzen. Die Community verbindet Sie mit unseren Mitgliedern und verschafft Ihrer Stimme Gehör. Hier werden Sie sich gerne einbringen, weil Sie wissen, dass Ihre Meinung und Ihr Beitrag respektiert und geschätzt werden. Als Anbieter Ihrer Wahl sind wir stets bestrebt, Ihnen beispiellos schnellen und kompetenten Support zu bieten und möchten Sie an unserer Seite wissen. Darum haben wir diese Community geschaffen.

Hier geht's zur Website unserer Expert Community:

https://community.bitdefender.com/de

6.2.3. Bitdefender Cyberpedia

In der Bitdefender Cyberpedia finden Sie alles Wissenswerte zu den neuesten Cyberbedrohungen. Hier teilen Bitdefender-Experten Tipps und Tricks, wie Sie sich vor Hackern, Datenpannen, Identitätsdiebstahl und Identitätsbetrug in den sozialen Medien schützen können.

Die Bitdefender Cyberpedia finden Sie hier:

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

6.3. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Bereits seit 2001 setzt BITDEFENDER alles daran, die bereits hochgesteckten Erwartungen unserer Kunden und Partner immer wieder zu übertreffen und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen deshalb gerne zur Verfügung. Kontaktieren Sie uns dazu einfach über unser **Bitdefender Support Center**.

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

6.3.1. Lokale Vertriebspartner

Die Bitdefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen Bitdefender Distributor in Ihrem Land:

1. Mehr dazu unter https://www.bitdefender.de/partners/partner-locator.html.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.

GLOSSAR

Aktivierungscode

Dabei handelt es sich um einen eindeutigen Schlüssel, der käuflich erworben und zur Aktivierung eines Produkts oder eines Dienstes verwendet werden kann. Mit einem Aktivierungscode kann ein gültiges Abonnement für einen bestimmten Zeitraum und eine bestimmte Anzahl an Geräten aktiviert werden. Zudem kann mit einem solchen Code eine Abonnement verlängert werden, solange es sich auf das gleiche Produkt oder den gleichen Dienst bezieht.

ActiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben. Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Advanced Persistent Threat

Advanced Persistent Threat (APT) nutzen Sicherheitslücken im System, um wichtige Daten zu stehlen und an ihre Quellen zu übermitteln. Organisationen, Unternehmen und Regierungsbehörden sind eine große Zielgruppe, die von dieser Bedrohung ins Visier genommen wird. Advanced Persistent Threats sollen so lange wie möglich unentdeckt bleiben. Während dieser Zeit sollen sie das System überwachen und wichtige Daten sammeln, ohne dabei die Zielcomputer zu beschädigen. Die Bedrohung wird durch PDF-Dateien oder Office-Dokumente in das Netzwerk eingebracht, die keinen Verdacht erregen, so dass jeder Benutzer diese Dateien ausführen kann.

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-

Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor. Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Hintertür

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Eine Bedrohung, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird diese Bedrohung im Arbeitsspeicher aktiviert. Bei jedem Neustart wird die Bedrohung so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Botnet

Der Begriff "Botnet" setzt sich aus den Wörtern "Robot" und "Network" zusammen. Bei Botnets handelt es sich um ein Netz aus mit Bedrohungen infizierten Geräten, die mit dem Internet verbunden und für den Versand von Spam, den Diebstahl von Daten, die Fernsteuerung von anfälligen

Geräten oder die Verbreitung von Spyware, Ransomware und anderen Bedrohungsarten verwendet werden. Ziel ist es, möglichst viele mit dem Internet verbundene Geräte zu infizieren, so z. B. PCs, Server, Mobilgeräte oder IoT-Geräte in den Netzwerken großer Unternehmen oder Branchen.

Browser

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Brute-Force-Angriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem in schneller Abfolge häufige Passwortkombinationen durchprobiert werden.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Cookies

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick"

verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Cybermobbing

Wenn Altersgenossen oder Fremde absichtlich Kinder misshandeln, um sie körperlich zu verletzen. Um emotionale Schäden anzurichten, schicken die Täter verletzende Nachrichten oder unvorteilhafte Fotos, so dass sich ihre Opfer von anderen isolieren oder entmutigt werden.

Wörterbuchangriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem alle möglichen Wörter aus einem Wörterbuch als potenzielle Passwörter eingegeben werden. Dieselbe Methode wird auch verwendet um Schlüssel für verschlüsselte Nachrichten oder Dokumente zu erraten. Wörterbuchangriffe funktionieren, weil viele Benutzer kurze, leicht zu erratende Wörter als Passwörter benutzen.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann. Ein Festplatten-Laufwerk liest und beschreibt Festplatten. Ein Disketten-Laufwerk liest und beschreibt Disketten. Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignisse

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel

Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Exploits

Eine Möglichkeit, Fehler oder Schwachstellen in Computersoftware und -hardware für seine Zwecke auszunutzen. So können Hacker die Kontrolle über Computer oder Netzwerke übernehmen.

Fehlalarme

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Dateinamenerweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind. Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Heuristik

Eine Methode, um neue Bedrohungen zu identifizieren. Diese Scan-Methode benötigt keine konkreten Bedrohungsinformationen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante einer alten Bedrohung getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

Honeypot

Ein Computersystem, das als Köder dient, um Hacker anzulocken und danach ihr Verhalten zu beobachten. Daraus lassen sich Schlüsse ziehen, mit welchen Methoden Sie Daten sammeln. Besonders Unternehmen und Konzerne setzen auf den Einsatz dieser "Honigtöpfe", um ihren Sicherheitslage zu verbessern.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java-Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet. Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Makrovirus

Eine Bedrohungsart, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen. Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Mail-Client

Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Nicht-heuristisch

Diese Scan-Methode benötigt konkrete Bedrohungsinformationen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einer Scheinbedrohung getäuscht werden kann und so Fehlalarme verhindert.

Online-Missbrauch

Wenn Personen versuchen, Minderjährige oder Jugendliche anzusprechen, um sie in illegale sexuelle Aktivitäten zu verwickeln. Soziale Netzwerke sind der ideale Ort, um verletzlichen Kindern nachzustellen und sie zu sexuellen Aktivitäten zu verführen, sei es online oder persönlich.

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, sodass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm zum Komprimieren von Dateien würde jedoch die Leerzeichen durch ein spezielles Zeichen der Leerzeichenreihe, gefolgt von der Anzahl der zu ersetzenden Leerzeichen, ersetzen. In diesem Fall würden für die zehn Leerzeichen nur zwei Bytes benötigt. Dies ist nur eine Komprimierungstechnik - es gibt noch viele weitere.

Pfad

Zeigt die Stelle an, an der sich eine Datei auf einem Computer befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses von oben nach unten.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs

oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen der Sicherheitslösung auf die Systemleistung zu minimieren. Durch die Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

Polymorphic virus

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Port

Eine Schnittstelle an einem Computer, an die ein Gerät angeschlossen werden kann. PCs haben verschiedene Arten von Anschlüssen. Intern gibt es mehrere Anschlüsse für den Anschluss von Laufwerken, Bildschirmen und Tastaturen. Extern haben PCs Anschlüsse für den Anschluss von Modems, Druckern, Mäusen und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Ransomware

Ransomware ist bösartige Software, die das System des Opfers sperrt und nur gegen ein Lösegeld wieder entfernt wird. CryptoLocker, CryptoWall und TeslaWall sind einige bekanntere Beispiele für Ransomware.

Die Infektion kann sich durch das Aufrufen eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Berichtsdatei

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit

Ein Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf ein System auf Administratorebene ermöglichen. Der Begriff wurde erstmals für UNIX-Betriebssysteme verwendet und bezog sich auf neu kompilierte Tools, die Eindringlingen administrative Rechte verschafften und es ihnen ermöglichten, ihre Anwesenheit zu verbergen, um der Erkennung durch den Systemadministrator zu entgehen.

Die Hauptaufgabe von Rootkits besteht darin, Prozesse, Dateien, Logins und Protokolle zu verbergen. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, wenn sie die entsprechende Software enthalten.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Bedrohungen zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit anderen Bedrohungen stellen Rootkits eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Beiträge in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Systemstartelemente

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die beim Systemstart abgespielt wird, ein Erinnerungskalender oder auch Apps sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Abonnement

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

Taskleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Bedrohung

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

Update der Bedrohungsinformationen

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

Bitdefender verfügt über eine eigene Update-Funktion, über die Sie manuell nach Updates suchen oder das Produkt automatisch aktualisieren lassen können.

Virtual Private Network (VPN)

Mit dieser Technologie ist es möglich, eine zeitlich begrenzte und verschlüsselte direkte Verbindung mit einem bestimmten Netzwerk auch über ein weniger gut gesichertes Netzwerk aufzubauen. Auf diese Weise können Daten sicher und verschlüsselt versandt und empfangen werden und sind für neugierige Augen nur schwer einsehbar. Bei einem Sicherheitsnachweis handelt es sich um eine Authentifizierung, die ausschließlich über einen Benutzernamen und ein Passwort erfolgen kann.

Wurm

Ein Programm, das sich selbst über ein Netzwerk ausbreitet und sich dabei selbst reproduziert. Es kann sich nicht an andere Programme anhängen.