AVG Mobilation

Häufig gestellte Fragen (FAQs)

Inhalt

1. Wieso brauche ich eine Anti-Virus Software?

Heute sind Smartphones und Tablets essenziell mobile PCs; und genau wie stationäre Computer sind sie auch anfällig für Viren und Schadprogramme. Millionen von Menschen speichern vertrauliche Daten auf ihren mobilen Geräten und surfen mit diesen Geräten im Web, lesen eMails und führen damit finanzielle Transaktionen durch. Daher ist es auch nicht überraschend, dass Cyberkriminelle sich diese Geräte zum Ziel machen.

Schadsoftware befällt mobile Geräte auf denselben Wegen wie auch stationäre Computer: Öffnen eines eMail Anhangs, Klicken auf einen Web-Link oder Herunterladen einer Datei bzw. einer App. Mobile Geräte können aber auch von Cyberkriminellen zu DDoS (Distributed Denial of Service)-Angriffen auf das Mobilfunknetz missbraucht werden, genau wie stationäre Computer dazu missbraucht werden, um eine ausgewählte Website "abstürzen" zu lassen , indem die Seite mit Traffic überladen wird.

Um Ihr Gerät vor der zunehmenden Gefahr zu schützen, wird dringend empfohlen eine Anti-Virus Software zu benutzen.

1.1. Was ist AVG Mobilation™ Anti-Virus?

AVG Mobilation™ Anti-Virus ist eines der besten Sicherheits-Apps für mobile Geräte wie Smartphones und Tablets. Der Hauptzweck dieser App ist der Schutz ihres mobilen Geräts vor Sicherheitsbedrohungen und Schadsoftware, welche immer mehr an Beliebtheit im mobilen Bereich gewinnen.

Aber AVG Mobilation™ Anti-Virus geht weit über den bloßen Schutz ihres Geräts hinaus. Mit Features wie App-Sperre, Aufgaben-Killer, Tuneup und dem Anti-Diebstahl Service hilft AVG Mobilation™ Anti-Virus Ihnen auch Ihre Privatsphäre zu wahren, die Leistung Ihres Gerätes zu überwachen und ihr Gerät von fern zu bedienen, falls es verloren gegangen ist oder gestohlen wurde.

1.2. Was sind die Unterschiede zwischen AVG Mobilation™ Anti-Virus und den Anti-Virus Versionen Free und Pro?

AVG Mobilation™ bietet Ihnen zwei Versionen von AVG Mobilation™ Anti-Virus an:

Free und Pro. Die Free-Version bietet Schutz vor Schadsoftware und einige zusätzliche Tools.

Die Pro-Version ist eine Vollversion, welche alle erweiterten Features der App enthält.

Die folgende Tabelle fasst die Unterschiede zwischen den beiden Versionen zusammen.

AVG Mobilation™ Anti-Virus Free	AVG Mobilation™ Anti-Virus Pro
Datei-Scanner	Datei-Scanner
Aufgaben-Killer	Aufgaben-Killer
App-Sperre - 14 Tage Testzeit	App-Sperre
Tuneup	Tuneup
App-Backup - 14 Tage Testzeit	App-Backup
Persönliche Daten löschen	Persönliche Daten löschen
Sicheres Surfen im Internet	Sicheres Surfen im Internet
Support durch FAQs	Erweiterter eMail-Support durch einen Angestellten des Supports (zusätzlich zu den FAQs)
Werbung	keine Werbung

2. Systemvoraussetzungen

2.1. Was sind die Mindestsystemvoraussetzungen, um AVG Mobilation™ Anti-Virus zu installieren?

Um AVG Mobilation™ Anti-Virus zu installieren und betreiben zu können, brauchen Sie ein mobiles Gerät mit Touchscreen und ein lauffähiges Android 2.0 oder höher.

2.2. Was sind die Android-Systemvoraussetzungen, um jedes Feature zu unterstützen?

Einige der Produkt-Features haben bestimmte Systemvoraussetzungen im Bezug auf die Androidversion Ihres Gerätes.

Die folgende Tabelle listet die Systemvoraussetzungen für jede dieser Komponenten:

Feature	**Android OS Voraussetzungen**
App-Backup	2.x oder höher
Tuneup	2.x oder höher
Fernlokalisierung	2.1 oder höher
Fernsperrung	2.2 oder höher
Fernlöschung	2.2 oder höher
Lokalisierungs-Service	2.1 oder höher

2.3. Funktioniert AVG Mobilation™ Anti-Virus auf Android-Tablets?

Ja, AVG Mobilation™ Anti-Virus funktioniert auf Android-Tablets und schützt diese vor Sicherheitsbedrohungen.

Allerdings sind für Tablets, die keinen Telefon-Service unterstützen, einige Bedrohungen, die Smartphones betreffen, unwichtig. Deswegen ist das folgende Feature für solche Tablets nicht verwendbar:

Scan von Textnachrichten

2.4. Warum muss für AVG Mobilation™ Anti-Virus so viel zugelassen werden?

Das Hauptziel von AVG Mobilation™ Anti-Virus ist der Schutz Ihres Geräts vor Sicherheitsbedrohung. Eine Sicherheitsbedrohung ist nicht notwendigerweise nur ein Virus oder Schadsoftware, also ein bösartiger Code, der auf Ihrem Gerät läuft. Eine solche Sicherheitsbedrohung kann auch in Verbindung mit Social Engineering stehen, wobei Cyberkriminelle das Ziel haben Sie so zu beeinflussen, dass sie an persönliche Daten gelangen können. Zum Beispiel könnten Sie eine Textnachricht von Ihrer Bank erhalten, in welcher Sie aufgefordert werden einen gesonderten Link zu besuchen und Ihr Passwort zu ändern. Durch den Besuch dieses Links und dem Eintippen Ihres momentanen Passworts könnten Sie aber Cyberkriminellen den Zugang zu Ihrem Bank-Account ermöglichen.

Um Ihr Gerät gegen Sicherheitsbedrohungen, wie bösartigen Code und Angriffe durch Social Engineering, zu schützen, muss AVG Mobilation™ Anti-Virus viele Vorgänge und Datenquellen auf ihrem Gerät genau beobachten. Um dies zu erreichen, benötigt AVG Mobilation™ Anti-Virus mehrere Arten von Rechten, auch welche, die auf den ersten Blick nicht zur Sicherheit beitragen.

Zuzüglich benötigt AVG Mobilation™ Anti-Virus auch andere Rechte, um zusätzliche Funktionen bereitzustellen. Zum Beispiel benötigt das Tuneup-Tool bestimmte Rechte, um dabei zu helfen die Leistung ihres Geräts zu überwachen.

3. Download und Installation

3.1. Wo kann ich AVG Mobilation™ Anti-Virus herunterladen?

Sie können AVG Mobilation™ Anti-Virus von Google Play (empfohlen), von der AVG Mobilation™ Website (www.avgmobilation.com) oder von anderen führenden App-Stores herunterladen.

Download von Google Play:

1. Führen Sie die Google Play App auf ihrem mobilen Gerät aus.
2. Suchen Sie in Google Play nach **AVG**.
3. Klicken Sie, unter den Suchergebnissen, auf das AVG Mobilation™ Anti-Virus Produkt, das Sie herunterladen möchten.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um den Download-Prozess abzuschließen.

Wenn Sie AVG Mobilation™ Anti-Virus von einer Website herunterladen gehen Sie bitte unter „Einstellungen" dort wählen Sie „Anwendungen" und hacken Sie „von Unbekannten Quellen zulassen" an.

3.2. Wie installiere ich AVG Mobilation™ Anti-Virus?

Nach dem Download von AVG Mobilation™ Anti-Virus, wird es automatisch auf Ihrem mobilen Gerät installiert. Um die App zu starten, klicken Sie zuerst auf **Anwendungen** und dann auf das AVG Mobilation™ Anti-Virus Icon und folgen dann den Anweisungen auf dem Bildschirm.

3.3. Warum kann ich AVG Mobilation™ Anti-Virus nicht auf einer SD-Karte installieren oder es auf eine SD-Karte verschieben?

Das Hauptziel von AVG Mobilation™ Anti-Virus ist Ihr Gerät während des Betriebs zu jeder Zeit schützen zu können. Dafür wurde AVG Mobilation™ Anti-Virus so entworfen, dass es als ein Service auf Android-Betriebssystem läuft. Die Installation einer App auf einer SD-Karte wird die App davon abhalten Ihr mobiles Gerät zu schützen, wenn der Zugang zur SD-Karte verwehrt bleibt (z.B., wenn das Gerät an Ihren PC angeschlossen ist oder die SD-Karte herausgenommen wird).

4. Schutz Ihres Gerätes

4.1. Wie scanne ich mein Gerät auf potentielle Bedrohungen und Schadsoftware?

AVG Mobilation™ Anti-Virus bietet Ihnen zwei einfache Wege Ihr Gerät manuell zu scannen:

1. Klicken Sie einfach auf den Hauptbildschirm, um einen manuellen Scan durchzuführen.
2. Oder klicken Sie im App-Menü auf die **Scan**-Taste, um einen manuellen Scan durchzuführen.

Sie können auch einen automatischen Scan auf ihrem Gerät in vordefinierten Abständen durchführen. Für weitere Informationen lesen Sie bitte den Abschnitt Häufigkeit für Auto-Scan.

4.2. Was beinhaltet ein solcher Scan?

AVG Mobilation™ Anti-Virus scannt die folgenden Komponenten auf Ihrem Gerät:

- Apps
- Einstellungen
- Inhalt

Bemerkung:

"Inhalt" und "Medien" wurden in eine einzelne Kategorie zusammengeführt. Infizierte Medien-dateien werden nun unter "Inhalt" angezeigt.

4.3. Scanergebnisse: Wie behandele ich Bedrohungsmeldungen, die die Apps betreffen?

Wenn AVG Mobilation™ Anti-Virus' Sicherheits-Engine ein potenziell bösartiges App auf ihrem Gerät identifiziert, wird der Bildschirm mit den Scanergebnissen den Namen dieser App anzeigen und es Ihnen erlauben besagte App zu deinstallieren.

Im Gegensatz zu bösartigen Programmen und Viren auf einem stationären Computer, wo der Benutzer versuchen kann ein infiziertes Programm oder eine Datei zu "säubern", ist auf einem mobilem Gerät eine Deinstallation die einzig mögliche Option.

4.4. Scanergebnisse: Wie behandele ich Bedrohungsmeldungen, die die Einstellungen betreffen?

AVG Mobilation™ Anti-Virus' Sicherheits-Engine durchsucht die allgemeinen Einstellungen auf Ihrem Gerät nach potenziellen Gefahren. Die folgende Tabelle listet die potentiellen Bedrohungen und die dafür empfohlenen Lösungen auf.

Bedrohung	Ort in den Einstellungen	Potenzielles Risiko	Lösungsvorschlag
"USB.Debugging" ist aktiviert	Einstellungen → Apps → Entwicklung → USB-Debugging	Wenn diese Option aktiviert ist, können Hacker die Verbindung zwischen dem stationären PC und dem mobilen Gerät ausnutzen, um eigene Befehle oder Viren vom PC auf das mobile Gerät zu übermitteln.	Es wird empfohlen die Markierung der Checkbox "USB Debugging" aufzuheben, damit diese Einstellung deaktiviert wird.
"Unbekannte Herkunft" ist aktiviert	Einstellungen → Apps → Unbekannte Herkunft	Wenn diese Option aktiviert ist, können Andoid-Apps von nicht vertrauenswürdigen Internetquellen heruntergeladen und installiert werden.	Es wird empfohlen die Markierung der Checkbox "Unbekannte Herkunft" aufzuheben, damit diese Einstellung deaktiviert wird.
Das Gerät läuft im privilegiertem Modus (rooted)		Das bedeutet, dass das Gerät gerooted ist.	Lesen Sie unter Rooted Device weiter.

4.5. Scanergebnisse: Wie behandele ich Bedrohungsmeldungen, die den Inhalt betreffen?

AVG Mobilation™ Anti-Virus' Sicherheits-Engine sucht nach potenziellen Risiken in folgenden Inhalten:

1. Dateien – Wenn verdächtige Dateien gefunden werden, wird Ihnen geraten diese zu löschen.

2. Textnachrichten (SMS) – Wenn verdächtige Textnachrichten gefunden werden, können Sie diese mit einer Kopf- und Fußzeile versehen. Für weitere Informationen über Echtzeit-Scannen von Textnachrichten lesen Sie bitte den Abschnitt Textnachrichten Scan.

3. Mediendateien – Wenn solche Dateien gefunden werden, wird Ihnen geraten diese zu löschen.

4.6. Was bedeutet die Checkbox "Nicht mehr anzeigen" im Anzeigebildschirm der Scanergebnisse?

Wenn die Bedrohung während eines AVG Mobilation™ Anti-Virus Scans gefunden wird, liefert der Anzeigebildschirm der Scanergebnisse entsprechende Empfehlungen für die Handhabung der Bedrohung. Jedoch bietet der Anzeigebildschirm dem Benutzer auch an, die Bedrohung in zukünftigen Scans zu ignorieren. Durch Auswählen der **Nicht mehr anzeigen**-Checkbox gibt der Benutzer an, dass er nicht mehr über diese Bedrohung benachrichtigt werden möchte.

4.7. Wo kann ich mehr Informationen über Bedrohungen und Viren für Android finden?

AVG Mobilation™ Security Center ist der Ort, wo unser Security-Forschungsteam die neuesten Entdeckungen im Bereich der mobilen Sicherheit und professioneller Analyse von potenziellen Gefahren publiziert. Für weitere Informationen besuchen Sie bitte folgenden Link: http://www.avgmobilation.com/securitycenter.

Sie können auch die offizielle Seite des AVG Blogs auf http://viruslab.blog.avg.com besuchen.

Einstellungen

Was ist Jetzt Aktualisieren?

Jetzt Aktualisieren lässt Sie ein manuelles Update der Security-Signaturen von AVG Mobilation™ Anti-Virus durchführen. Sollten keine neuen Updates verfügbar sein, werden Sie darüber benachrichtigt, dass bei Ihnen bereits die neuesten Updates installiert sind.

4.8. Was ist Häufigkeit für Auto-Scan?

Häufigkeit für Auto-Scan erlaubt es ihnen die gewünschte Häufigkeit für den automatischen Scan auf Ihrem mobilen Gerät einzustellen. Die vorhandenen Einstellungsmöglichkeiten sind:

- Einmal täglich
- Einmal wöchentlich
- nie

Der Scan wird, gemäß Ihren Einstellungen, automatisch durchgeführt. Nachdem der Scan abgeschlossen ist, wird Ihnen diesbezüglich eine Benachrichtigung angezeigt. Das Klicken auf diese Benachrichtigung öffnet einen Bildschirm mit den Scanergebnissen.

4.9. Was ist Echtzeit-Scanner?

Textnachrichten scannen erlaubt es Ihnen einen Mechanismus zu aktivieren, der verdächtige eingehende Textnachrichten (SMS) markiert. Diese Textnachrichten werden in Echtzeit mit einer Kopf- und Fußzeile gekennzeichnet, z.B.:

Wenn diese Einstellung aktiviert ist, fügt AVG Mobilation™ Anti-Virus lediglich die Kopf- und Fußzeile zu der Textnachricht hinzu. Es liegt am Benutzer zu entscheiden, ob er manuell die Nachricht löschen oder die Warnung ignorieren möchte.

Bitte beachten Sie, dass Textnachrichten automatisch während eines Scans gescannt werden. **Textnachrichten scannen** stellt aber auch das Scannen von Textnachrichten in Echtzeit zur Verfügung.

4.10.Was ist Sicheres Surfen im Internet?

Sicheres Surfen im Internet benutzt die AVG LinkScanner™-Engine, um den Benutzer vor bösartigen Web-Links zu schützen, indem die Web-Links automatisch, während der Benutzer im Internet surft, überprüft werden. AVG LinkScanner™ prüft die Webseiten in Echtzeit und hilft Ihnen verdächtige Webseiten zu meiden.

Bemerkung: Um dieses Feature nutzen zu können, muss der **Echtzeit-Scanner** aktiviert sein.

4.11.Was ist Sprache?

Sprache ermöglicht es Ihnen die Sprache der App-Oberfläche zu wählen. Die App unterstützt zur Zeit 15 verschiedene Sprachen: Englisch (voreingestellt), Koreanisch, Französisch, Spanisch, Chinesisch, Niederländisch, Deutsch, Japanisch, Russisch, Hebräisch, Italienisch, Polnisch, Portugiesisch, Arabisch und Tschechisch.

5. Extras

5.1. Welche zusätzlichen Tools bietet AVG Mobilation™ Anti-Virus an?

Zusätzlich zu den grundlegenden Schutz-Features bietet AVG Mobilation™ Anti-Virus eine Vielseitigkeit an fortgeschrittenen Tools an. Diese beinhalten Tools, die dazu entworfen wurden, um:

Ihren Schutz zu verbessern, wie Datei-Scanner.

Ihre Privatsphäre zu gewährleisten, wie App-Sperre.

Ihnen zu helfen die Ressourcen Ihres Gerätes zu überwachen, wie TuneUp.

Die folgenden FAQ-Abschnitte bieten Ihnen weitere Informationen über die fortgeschrittenen Tools von AVG Mobilation™ Anti-Virus.

5.2. Was ist Dateiscanner?

Dateiscanner ermöglicht es Ihnen ein Sicherheitsfile, in bestimmten Speicherstellen auf Ihrem Gerät, zu scannen. Scanziele können Ihre SD-Karte, Root, Downloads, Bilder, Musik oder Videos sein. Nachdem Sie ein Ziel ausgewählt haben, können Sie weiter spezifische Ordner, Unterordner oder Dateien als Ziel wählen. Die Scanergebnisse werden Ihnen angezeigt, sobald der Scan abgeschlossen ist.

Der SD-Karten Scan ist nun verbessert und erweitert -

Durch Aktivieren dieser neuen Option unter der App "Einstellungen" wird der Virusscan nun auch APK Dateien enthalten, die auf der SD-Karte gespeichert sind.

5.3. Kann ich APK Dateien, die nicht von Google Play sind, vor der Installation scannen?

Ja, bevor Sie neue Applikationen auf Ihrem Gerät installieren, wird AVG Mobilation Anti-Virus Sie auffordern einen Scan der application package Datei (APK) durchzuführen.

5.4. Was ist Aufgaben-Killer?

Sollte Ihr Gerät langsamer werden oder nicht mehr reagieren, so können Sie **Aufgaben-Killer** benutzen, um eine App zu stoppen.

5.5. Was ist App-Sperre?

App-Sperre ermöglicht es Ihnen installierte Apps vor Missbrauch zu schützen, indem diese mit einem Passwort abgesichert werden. Ein App, dass von App-Sperre geschützt wird, kann nur mit Hilfe dieses Passwortes gestartet und somit nicht missbraucht werden. Das Passwort kann leicht durch eine eMail wiederhergestellt werden.

App-Sperre wurde nur zum Passwortschutz einzelner Apps entworfen. Um das mobile Gerät selbst vor Missbrauch zu schützen, können Sie die **Bildschirmsperre** benutzen, welche schon im Android-Betriebssystem enthalten ist.

App-Sperre ist AVG Mobilation™ Anti-Virus Pro Nutzern ohne Einschränkungen zugänglich. Für Benutzer von AVG Mobilation™ Anti-Virus Free ist dieses Feature für eine 14-Tägige Probezeit zugänglich.

5.6. Kann ich App-Sperre benutzen, um die allgemeinen Einstellungen des Geräts zu schützen?

Nein, AVG Mobilation™ Anti-Virus kann nicht selbst durch **App-Sperre** passwort-geschützt werden, da dies eine Einschränkung der Sicherheit Ihres Gerätes bedeuten würde.

5.7. Was ist Tuneup?

Tuneup stellt auf einen Blick die wesentlichen Leistungsparameter dar, damit Sie die Systemleistung besser beobachten können.

1. **Batterie** – zeigt wie lange die derzeitige Aufladung der Batterie für verschiedene Aktivitäten reicht; Ein/Ausschalten der Stromspar-Optionen; setzen einer Benachrichtigung, sobald die Batterieaufladung eine gewählte Grenze erreicht

2. **Speicher** – betrachten und verwalten Sie Ihre Speicherorte (z.B.: interne SD-Karte).

3. **Traffic** – betrachten und überprüfen Sie die Nutzung Ihres mobilen Datenverkehrs und setzen Sie eine Notiz, wenn dies einen Grenzwert erreicht.

5.8. Was ist App-Backup?

App-Backup bietet Ihnen die Option ein Backup Ihrer Apps auf die SD-Karte zu erstellen. Durch das so erstellte Backup lassen sich die Apps zu einem später Zeitpunkt wiederherstellen.

App-Backup sichert keine persönlichen Daten, die im Zusammenhang mit den Apps stehen, wie Passwörter oder Einstellungen.

App-Backup ist AVG Mobilation™ Anti-Virus Pro Nutzern ohne Einschränkungen zugänglich. Für Benutzer von AVG Mobilation™ Anti-Virus Free ist dieses Feature für eine 14-Tägige Probezeit zugänglich.

5.9. Was ist Persönliche Daten löschen?

Persönliche Daten löschen lässt Sie verschiedene Arten von Informationen, die auf Ihrem mobilen Gerät gespeichert sind, löschen. Das Löschen ist irreversibel – einmal gelöscht, können die gelöschten Daten nicht mehr wiederhergestellt werden. Die Daten können nach Speicherort oder nach Typ gelöscht werden, wie folgend:

- **lösche SD-Karte** – formatiert die SD-Karte

- **lösche Gerät** – Diese Option ist zu einem Zurücksetzen auf Werkseinstellungen äquivalent

- **lösche Daten nach Kategorie** – löscht alle Logs, SMS, MMS, Account-Syncronisationen und Browser-Daten

6. Anti-Diebstahl Service

6.1. Was ist das Web-Interface des Remote Management?

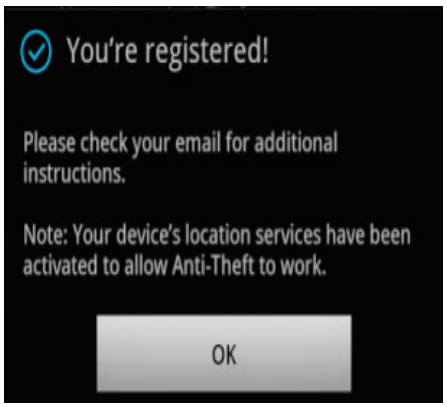
Der Anti-Diebstahl Service wurde entworfen, um Nutzern von AVG Mobilation™ Anti-Virus zu helfen und sie zu unterstützen, sollte deren mobiles Gerät verloren gehen oder gestohlen werden. Durch die Registrierung für den Anti-Diebstahl Service kann der Nutzer sich in die AVG Web-Seite einloggen und das vermisste Gerät fernsteuern, indem er das Interface der Fernverwaltung nutzt. Für weitere Informationen über Fernverwaltung lesen Sie bitte folgenden Abschnitt über Fernverwaltung.

6.2. Wie kann ich mich für den Anti-Diebstahl Service registrieren?

Klicken Sie dazu auf Ihrem mobilen Gerät auf **Menü → Anti-Diebstahl → Registrierung**.

Tragen Sie Ihre Google-Account eMail in das Dialogfenster ein und klicken Sie auf **OK**.

Nachdem der Registrierungsvorgang abgeschlossen ist, wird folgende Nachricht erscheinen:



Klicken Sie auf **OK**, um das Nachrichtenfenster zu schließen.

Eine eMail Nachricht wird automatisch an die eMail Adresse Ihres Google-Accounts, die Sie für die Registrierung benutzt haben, geschickt. Diese eMail wird einen Überblick über den Anti-Diebstahl Service, das Web-Interface der Fernverwaltung und Instruktionen, wie diese benutzt werden, enthalten.

Nach dem die Registrierung abgeschlossen ist, wird Ihnen dringend empfohlen sich in das Web-Interface der Fernverwaltung einzuloggen und sich mit dessen Features vertraut zu machen.

6.3. Was ist der Location-Service (Ortungsservice)?

Wenn der Benutzer sein Gerät für den Anti-Diebstahl Service registriert, ist die Checkbox des Location-Service automatisch ausgewählt und das Gerät schickt automatisch seine derzeitige Position an das Web-Interface der Fernverwaltung, für den Fall, dass es verloren geht oder gestohlen wird.

Bitte beachten Sie, dass diese Checkbox standardmäßig automatisch ausgewählt wird, wenn der Benutzer sich erfolgreich für den Anti-Diebstahl Service registriert. Jedoch kann der Benutzer dieses Feature jederzeit auf seinem Gerät deaktivieren.

Die Benutzung des Location-Service ist Bestandteil der Datenschutzerklärung von AVG. Der Ort des Gerätes wird nur dann ermittelt, wenn der Benutzer sich in das Web-Interface der Fernverwaltung einloggt und dort im Web-Interface auf die Option Gerät orten klickt. AVG speichert nicht den Bewegungsverlauf des Geräts.

Beachten Sie bitte, dass einige frühere Versionen von Android-Betriebssystemen Ortungsbasierte-Services nicht unterstützen. In solchen Fällen wird Ihnen die folgende Nachricht angezeigt:

"Der Location-Service wird vom derzeitigen Betriebssystem nicht unterstützt".

6.4. Ich habe versucht mich für den Anti-Diebstahl Service zu registrieren, jedoch wurde mir mitgeteilt, dass meine Registrierung fehlschlug. Was soll ich tun?

Der Registrieungsprozess kann wegen eines Kommunikationsproblems zwischen Ihrem Gerät und dem Internet oder dem nachgeschalteten Anti-Diebstahl Server fehlschlagen. In diesem Fall gibt es für Sie keinen Grund den Registrierungsprozess zu wiederholen. AVG Mobilation™ Anti-Virus hat einen eingebauten Mechanismus, der 3 weitere Versuche durchführen wird, um den Registrierungsprozess abzuschließen, sobald das Kommunikationsproblem behoben ist.

7. Fernverwaltung (Remote Management)

7.1. Was ist das Web-Interface des Remote Management?

Das Web-Interface der Fernverwaltung auf der AVG Web-Seite von AVG Mobilation™ Anti-Virus stellt dem Benutzer mehrere Optionen für die Fernverwaltung seines vermissten Geräts bereit, indem es ihm ermöglicht bestimmte Befehle an sein gerät zu senden. Die folgende Tabelle listet diese Optionen auf:

Option	Beschreibung
Shout	Lässt das Gerät einen Alarmton abspielen (selbst, wenn das Gerät auf "stumm" geschaltet ist), um Ihnen zu helfen es zu finden.
Locate	Lässt das Gerät dessen Position an den Web-Server der Fernverwaltung schicken, um Ihnen zu helfen es zu finden.
Lock	Sichern Sie Ihr Gerät mit einem Passwort, um es vor Missbrauch zu schützen. Diese Option lässt Sie zudem eine Lock Nachricht schreiben, die auf dem gesperrten Gerät angezeigt wird. Beachten Sie bitte, dass dies eine einmalige Aktion ist: wird das gerät entsperrt (sei es per Fernsteuerung oder lokal), muss es erst wieder gesperrt werden, wenn Sie es weiterhin gesperrt haben wollen.
Unlock	Entsperrt Ihr Gerät unter Benutzung des Passworts. Der Sperrbildschirm wird nicht mehr länger auf dem Gerät angezeigt.
Wipe	Löscht alle persönlichen Daten und formatiert die SD-Karte. Diese Handlung ist irreversibel – die gelöschten Daten können nicht mehr wieder hergestellt werden.
Scan	Scant Ihr Gerät nach Sicherheitsbedrohungen.
Remove device	Entfernt das Gerät von der Liste der verwalteten Geräte, unter der Benutzung des Web-Interface der Fernverwaltung.
Device Name Edit	Erlaubt es dem Gerät einen Nicknamen zu geben.

7.2. Wie logge mich in das Web-Interface des Remote Management ein?

Besuchen Sie auf Ihrem PC die Seite www.avgmobilation.com.

Klicken Sie auf **Login** und tragen dort Ihre Google-Account eMail Adresse und Passwort ein, die Sie benutzt haben, um sich für den Anti-Diebstahl Service zu registrieren. Klicken Sie dann auf **Sign in**.

Das Web-Interface des Remote Management wird Ihnen darauf angezeigt.

7.3. Werden alle Features des Remote Management von allen Version des Android-Betriebssystems unterstützt?

Einige der Features der Fernverwaltung haben bezüglich der Androidversion auf Ihrem Gerät bestimmte Systemvoraussetzungen.

Die folgende Tabelle listet die Systemvoraussetzungen für jede dieser Komponenten auf:

Feature	Android OS Voraussetzungen
Locate	2.1 oder höher
Lock	2.2 oder höher
Wipe	2.2 oder höher

7.4. Wie viele Geräte können mit einem einzigen Google-Account verwaltet werden?

Diese Nachricht erscheint in den folgenden Fällen:

- Sie versuchen sich mit Ihrem mobilen Gerät in das Web-Interface der Fernverwaltung einzuloggen, ohne sich vorher für den Anti-Diebstahl Service registriert zu haben. Um dieses Problem zu lösen, stellen Sie bitte sicher, dass Sie den Registrierungsprozess auf dem Gerät beendet haben bevor Sie sich einloggen.

- Sie versuchen sich in das Web-Interface der Fernverwaltung mit einem Google-Account einzuloggen, welcher nicht derselbe ist mir dem Sie sich für den Anti-Diebstahl Service registriert haben. Um dieses Problem zu lösen, loggen Sie sich bitte mit demselben Google-Account ein, mit dem Sie sich auch für den Anti-Diebstahl Service registriert haben.

7.5. Wie lokalisiert das Web-Interface des Remote Management das Gerät?

Mehrere Verfahren werden eingesetzt, um die derzeitige Position Ihres Geräts zu lokalisieren, wie zum Beispiel GPS, Mobilfunkstationen ID und Wi-Fi Netzwerke.

Wenn der Benutzer sich registriert, wird der **Location-Service** aktiviert. Wenn der Benutzer auf die Ortungsoption im Web-Interface des Remote Management klickt, wird ein Befehl an das mobile Gerät gesandt. Im Gegenzug meldet das Gerät seinen Aufenthaltsort auf einem oder mehreren der genannten Verfahren. Diese Daten werden bearbeitet und die derzeitige Position des Geräts wird auf einer Karte angezeigt. Der Nutzer kann zu jedem Zeitpunkt den Location-Service auf seinem Gerät deaktivieren.

Bemerkung:

- Damit der Location-Service funktioniert, muss die Checkbox des **Location-Service** auf der App ausgewählt sein.

- Damit das Gerät exakte GPS-Datem senden kann, wird Sky-View vorausgesetzt.

- Damit das Gerät Daten über das Wi-Fi Netzwerk übertragen kann, muss die Checkbox folgendermaßen ausgewählt sein: **Einstellungen →Ort → Benutze Wireless Networks** (empfohlen).

8. Das AVG Anti-Virus Widget

8.1. Was ist ein Widget?

Ein Widget, wobei es sich um App Verknüpfungen handelt, gibt Ihnen direkten Zugriff, auf die Hauptfunktionen von der App, direkt von Ihrem Startbildschirm. Es ermöglicht dem Benutzer auch dynamische Aktualisierungen von dem aktuellen Status von der gewählten Hauptfunktion in Bezug auf Sicherheit, Leistung und Datenschutz. Außerdem, erlaubt es Ihnen das direkte öffnen des Konfigurations-/ Eigenschaftsmenü in Bezug auf die gewählte Verknüpfung.

8.2. Wie füge ich ein Widget hinzu?

Zum Hinzufügen des Widget, tippen Sie auf dem Telefon den Menü-Knopf oder tippen und halten Sie auf dem Startbildschirm und wählen anschließend „Widget hinzufügen". Von der Liste von Widgets, tippen Sie auf „AntiVirus" und ziehen es zu einem Startbildschirm ihrer Wahl.

8.3. Kann ich anpassen welche Verknüpfungen in dem Widget angezeigt werden?

Ja. Klicken Sie den „Einstellung" Knopf (welcher aussieht wie ein Zahnrad) in der rechten oberen Ecke des Widgets und es öffnet sich der Einstellungsbildschirm. Wählen Sie die Verknüpfung die Sie ersetzen wollen und tippen auf diese. Eine Liste von zusätzlich verfügbaren Verknüpfungen wird geöffnet. Tippen Sie auf die neue Verknüpfung welche sie haben wollen und wählen „Fertig".

9. Lizenz und Abrechnung

9.1. Ich habe AVG Mobilation™ Anti-Virus Pro erworben. Wie aktiviere ich das Produkt?

Das Verfahren der Lizenzaktivierung hängt von der Art und Weise, wie das Produkt erworben, wurde ab.

Ein Produkt, das von Google Play erworben wurde, wird automatisch heruntergeladen und auf dem Gerät installiert – es besteht kein Grund einen Lizenzschlüssel für eine Aktivierung einzugeben.

Wenn aber ein Produkt von www.avgmobilation.com direkt erworben wird, dann wird Ihnen, nach Einkaufsbestätigung, eine eMail mit dem Download-Link und dem Lizenzschlüssel für die Aktivierung zugesandt. Gehen Sie mit Ihrem mobilen Gerät auf den Download-Link und folgen Sie den Anweisungen auf dem Bildschirm, um Ihren Lizenzschlüssel einzugeben und die App zu aktivieren.

Wenn ein Produkt von einem fremden App-Store erworben wurde, wird ein ähnliches Verfahren benutzt – Sie werden eine eMail vom Online-Store mit allen relevanten Aktivierungsinformationen erhalten.

Ein Produkt, das bei einem Händler erworben wurde, wird eine beigefügte Lizenzkarte und Aktivierungsanweisungen enthalten.

9.2. Wo trage ich den Lizenzschlüssel ein?

Um den Lizenzschlüssel einzugeben, klicken Sie auf **Menü → Hilfe → Lizenzaktivierung**.

9.3. Ich habe AVG Mobilation™ Anti-Virus Pro erworben. Auf wie vielen Geräten kann ich es installieren?

Die Anzahl der Geräte auf denen Sie die App installieren können ist Bestandteil der Einkaufpolitik des Geschäfts von dem die App erworben wurde.

9.4. Ich habe ein neues mobiles Gerät. Muss ich AVG Mobilation™ Anti-Virus nochmals erwerben?

Ob Sie AVG Mobilation™ Anti-Virus nochmal erwerben müssen, hängt von der Einkaufpolitik des Geschäfts ab von dem die App erworben wurde.

10. Rooted Devices

10.1.Was ist ein Rooted Device (verankertes Gerät)?

Ein Gerät wird im Allgemeinen als ein Rooted Device bezeichnet, wenn der Benutzer einen Zugang zum Android-Betriebssystem mit hohen Zugriffsrechten hat ("root Zugriff"). Rooting ist im Grunde der Prozess des "Einhackens" ins Gerät, um volle administrative Kontrolle über alle Ordner, Programme und Einstellungen des Betriebssystems zu erhalten, welche normalerweise vor dem Zugriff des Nutzers geschützt sind.

10.2.Der Anzeigebildschirm der Scanergebnisse beinhaltet einen Alarm, den unsicheren Privileg Mode (Privilegierten Modus) betreffend. Was soll ich tun?

Der folgende Alarm im Bildschirm der Scanergebnisse bedeutet, dass Ihr Gerät gerootet ist:

Unsicherer privilegierter Modus wurde entdeckt. Das Gerät läuft im privilegiertem Modus (ist gerootet).

AVG empfiehlt nicht gerootete Geräte zu nutzen, also Geräte mit ursprünglichen Werkseinstellungen. Da das "Unrooting" eines gerooteten Gerätes kommt einem Zurücksetzen des Geräts auf Werkseinstellungen gleich, was alle bis dahin gespeicherten Daten auf dem Gerät löscht und das bestehende Betriebssystem austauscht, wird dieses Verfahren nicht von AVG Mobilation™ Anti-Virus unterstützt. Es liegt am Benutzer diese Entscheidung zu treffen und dementsprechend zu handeln.

Für weiteren Support, was den Prozess des "Unroorting" eines gerooteten Geräts angeht, empfiehlt AVG das Unternehmen oder das Geschäft von dem Sie das Gerät ursprünglich erworben haben zu kontaktieren.

11. Hilfe und Support

11.1.Welcher Support wird für AVG Mobilation™ Anti-Virus angeboten?

Alle Benutzer sind eingeladen unsere FAQ, welche ständig mit neuen Fragen und Antworten aktualisiert wird, zu lesen.

AVG Mobilation™ Anti-Virus Pro Nutzer können außerdem unseren Produkt-Support nutzen, indem Sie ein Support-Ticket öffnen, wie im nächsten Abschnitt beschrieben.

11.2.Ich benutze AVG Mobilation™ Anti-Virus Pro. Wie öffne ich ein Support-Ticket?

Um ein Support-Ticket zu öffnen, klicken Sie auf Menü → Hilfe → Nehmen Sie Kontakt mit uns auf.

Um das Support-Ticket abzuschicken, geben Sie bitte die erforderlichen Informationen in der Vorlage ein, die ihnen dargestellt wird.

11.3.Wohin kann ich ein Malware Exemplar schicken?

Wenn Sie denken, dass Sie eine bösartige Android App gefunden haben, leiten Sie diese bitte zur Untersuchung an uns weiter. Die eMail Adresse für die Appeinsendung ist {malware@avgmobilation.com}.

Versuchen Sie bitte folgende Informationen mitzugeben:

1. Was ist der Name der App
2. Von wo haben Sie sie heruntergeladen
3. Wie sieht die App aus
4. Was ist das unerwartete Verhalten der App
5. Wie sieht das Icon der App aus
6. Was ist der Name der APK Datei

11.4.Wo kann ich die Datenschutzerklärung von AVG Mobilation™ nachlesen?

Um unsere Datenschutzerklärung zu lesen, klicken Sie bitte hier.

11.5.Wo kann ich die Nutzungsbedingungen von AVG Mobilation™ nachlesen?

Um unsere Nutzungsbedingungen zu lesen, klicken Sie bitte hier.