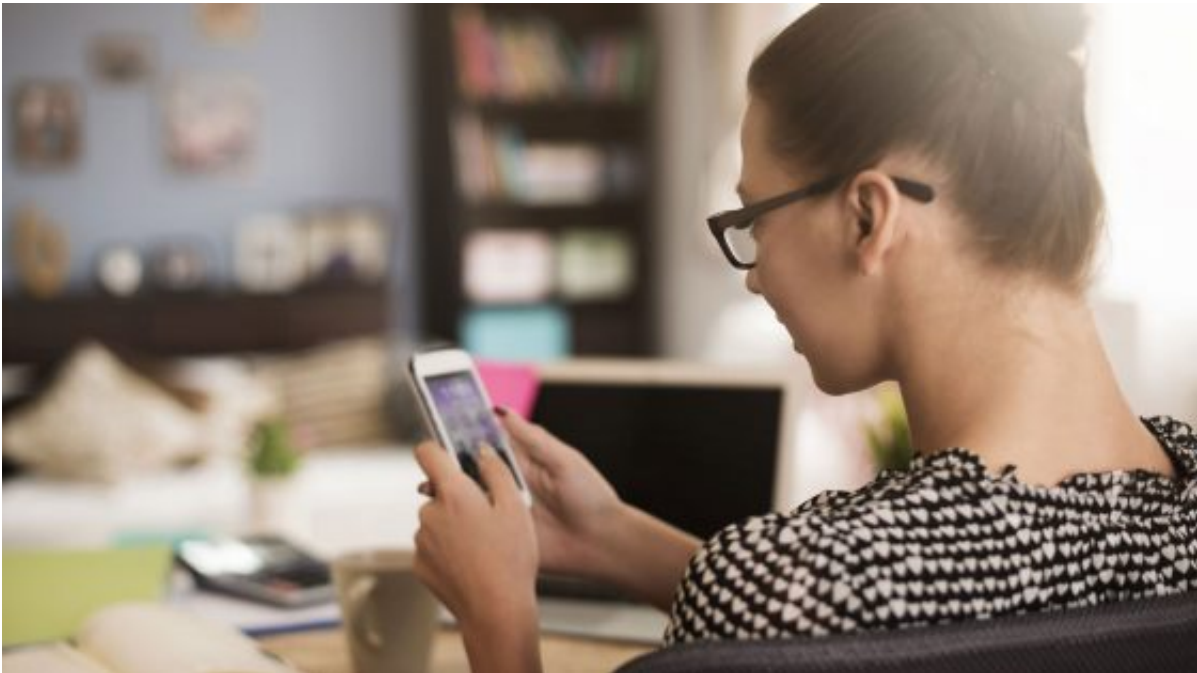


So schützen Sie Ihr Handy vor Viren

10.10.2017 [Redaktion UPDATED](#)



Ihnen springt eine als kostenloses Top-Spiel beworbene App für Ihr Smartphone ins Auge. Die Vorschaubilder sehen vielversprechend aus, die App ist gerade mal zwei Tage online und hat schon dutzende Fünf-Sterne-Bewertungen. Sie starten den Download – und erhalten Augenblicke später einen Alarm Ihres Handy-Virenschanners, denn das vermeintliche Spitzenspiel bringt einen Virus mit. Glück gehabt! UPDATED zeigt Ihnen, welche Scanner Ihr Smartphone vor diesen Schädlingen schützen.

- Virenschanner für Android – brauche ich den wirklich?
- Fünf empfehlenswerte Antiviren-Apps für Android
- Nur einen Virenschanner
- iOS-Geräte vor Viren schützen
- Erste Hilfe bei Virenfund
- Fazit: Auf Dauer virenlos am Smartphone

Virenschanner für Android – brauche ich das wirklich?

Smartphones und Tablet-PCs mit Android-Betriebssystem sind bei Hackern beliebt. Als Marktführer unter den Mobilbetriebssystemen läuft Android auf Hunderten Millionen Geräten, sodass Angriffe für Kriminelle dementsprechend lohnenswert erscheinen. Darüber hinaus weist Googles offenkonstruiertes Betriebssystem, ähnlich wie Windows, einige konzeptionelle Eigenheiten auf, die es Viren und anderen Schadprogrammen immer wieder ermöglichen, ein Gerät zu infizieren. So erlaubt Android die Installation ungeprüfter Apps, die nicht aus dem offiziellen Google Play Store stammen.

Auf die App-Zugriffsrechte achten

Manche dubiosen Apps für Android lassen sich schon an der Liste der benötigten Zugriffsrechte erkennen, die Ihnen im Google Play Store bei der Installation der App automatisch angezeigt wird. Fordert eine Nachrichten-App oder ein Spiel zum Beispiel Zugang zu den WLAN-Verbindungsinformationen, die Geräte-ID oder andere Anrufinformationen, sollten zumindest die Alarmglocken klingeln. Um herauszufinden, ob die App in Ordnung ist, empfiehlt es sich, im Web über den App-Namen nach weiteren Informationen suchen.

Erschwerend kommt hinzu, dass **Updates bei Android nicht zentral von Google für alle Smartphones und Tablets verteilt werden**, sondern der jeweilige Hersteller des Geräts für die Auslieferung der Aktualisierungen verantwortlich ist. Es hängt also von Samsung, HTC, Huawei, Sony, Lenovo, LG & Co. ab, ob und zu welchem Zeitpunkt Sicherheits-Updates für die einzelnen Gerätemodelle zur Verfügung stehen. Viele Hersteller reichen neueste Android-Updates oft erst sehr spät an die Nutzer weiter.

Android lässt sich aber ebenso wie Windows verhältnismäßig einfach absichern. Der erste und wichtigste Schritt: Spielen Sie alle Betriebssystem-Updates umgehend ein. In der Regel bekommen Sie die neueste Android-Version als Online-Update. Das bedeutet: Auf Ihrem Handy erscheint eine Meldung, dass ein Update zur Verfügung steht. Mit einem Tastendruck laden Sie die Aktualisierung herunter, die anschließende Installation erfolgt automatisch.

Wenn Sie dann noch die Sicherheitsfunktionen in Android 6.0 und neuer nutzen, um die Zugriffsberechtigungen beim Start von Apps zu prüfen und anzupassen, keine unbekannt Links in Mails anklicken, ausschließlich auf populären Websites surfen und aus dem Google Play Store nur die beliebtesten Apps laden, sind Sie weitgehend auf der sicheren Seite und kommen ohne Virenschutz aus. In allen anderen Konstellationen und insbesondere wenn der Hersteller Ihres Smartphones keine Android-Updates anbietet oder Sie sich bei der Handy-Nutzung möglichst wenig Gedanken um Sicherheitsaspekte machen möchten, gilt die Empfehlung: Besorgen Sie sich einen guten Virens Scanner für Ihr Smartphone oder Tablet.

Fünf empfehlenswerte Antiviren-Apps für Android

AVG, Avira, Kaspersky, Norton, Sophos und einige weitere Unternehmen haben sich als Hersteller von Virens Scannern und Anti-Malware-Tools für Windows-PCs und Server einen Namen gemacht. Sie alle bieten auch Antiviren-Apps für Android an. In der Regel handelt es sich dabei um Sicherheitskomplettlösungen, die aus mehreren Modulen mit einheitlichem Auswahlmenü bestehen. Sie alle besitzen einen Virens Scanner mit Echtzeiterkennung neuer Android-Schädlinge. **Einige der Apps können Sie in einer funktionsreduzierten Version sogar kostenlos nutzen** oder in einer Testversion meist 30 Tage lang ausprobieren. Für die Vollversion mit allen Programmfunktionen wird eine jährliche Pauschale von bis zu 30 Euro erhoben.

So arbeiten Virens Scanner für Android: Auch wenn Android ein offenes System ist, kann ein Virens Scanner technisch bedingt nicht jede einzelne auf dem Smartphone oder Tablet vorhandene Datei überprüfen. Stattdessen scannen die Sicherheitsprogramme alle auf dem Gerät installierten Apps und gleichen diese mit einer Datenbank schädlicher Anwendungen ab. Wird eine installierte App in der Datenbank gefunden, schlägt der Virens Scanner Alarm. Von der Aktualität der Datenbank hängt es also ab, wie gut eine Sicherheits-App schützt.



AVG AntiVirus für Android

Die tschechische Softwareschmiede AVG bietet mit [AVG AntiVirus für Android](#) einen in der Basisvariante werbefinanzierten Schädlingsscanner an, bei dem Sie die Funktionen der Pro-Version nach der Installation 30 Tage lang kostenlos testen können. Gut gefällt der klare Hinweis auf die enthaltenen, überaus deutlich sichtbaren Werbeeinblendungen mit der Möglichkeit, diese direkt zu Beginn für 8,49 Euro im Jahr zu entfernen.

Auf Wunsch scannt AVG Ihr Smartphone einmal täglich, ansonsten lassen sich Suchläufe über das Hauptmenü per Klick auf den runden Scan-Button anwerfen. Ob neben Viren auch potenziell unerwünschte Programme und werbefinanzierte Apps gemeldet werden, ist einstellbar. Mit dem Dateiscanner prüfen Sie Ordner wie das Stammverzeichnis des internen Speichers, Ihre Downloads, Bilder, Musik oder eine Speicherkarte auf Schädlinge.

An Extras gibt es eine Handy-Suche über Google Maps, einen Task-Manager zum Beenden von Apps und Optimierungsmöglichkeiten für die Akku- und Speichernutzung sowie eine Datensperre- und Verschlüsselungsfunktion. Speziell für Android-Tablets gibt's noch das kostenlose [AVG AntiVirus FREE für Tablet](#).



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)

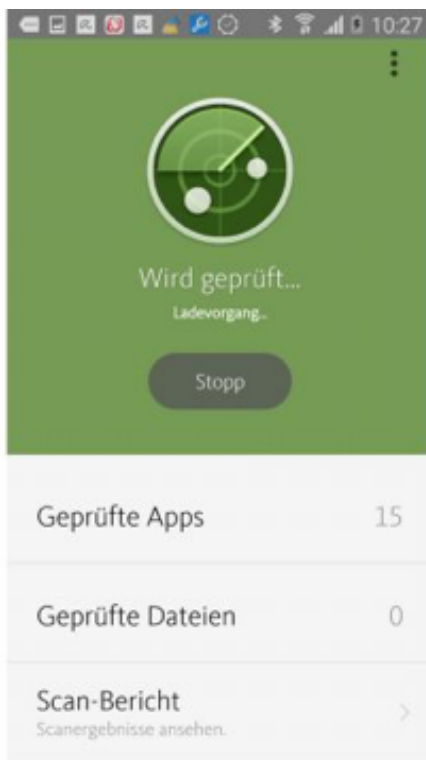
Avira Antivirus Security

Die [Sicherheits-Suite von Avira](#) besteht im Kern **aus einem Malware-Scanner mit einem Arsenal angedockter Security-Tools**. Dazu gehören die Anzeige von Apps, die persönliche Daten ausspionieren, das Sperren beliebiger Apps mit einem Passwort, ein Facebook-Schutz und eine Ortungsfunktion einschließlich Sperr- und Fernlöschmöglichkeit für ein verlorenes Smartphone. Die Bedienoberfläche ist ein Pluspunkt der App: Die großen Schaltflächen lassen sich auch auf kleinen Displays und aus einiger Entfernung gut ablesen. Neben dem internen Gerätespeicher werden bei der Prüfung auch Speicherkarten berücksichtigt.

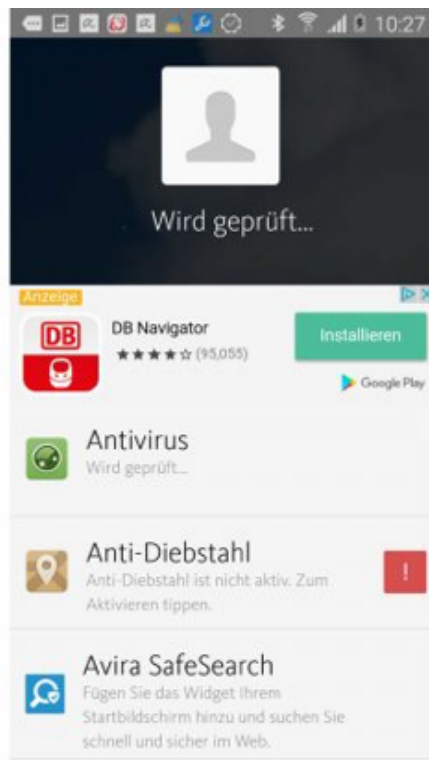
Die kostenlose Version des Avira-Scanners finanziert sich wie üblich durch Werbung. Die Werbeeinblendungen erfolgen an prominenter Stelle. So wurde uns auf unserem Testgerät ständig ein Button für die Installation des Bahn-Navigators vorgeschlagen, auf den wir vermutlich früher oder später versehentlich geklickt hätten.



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)

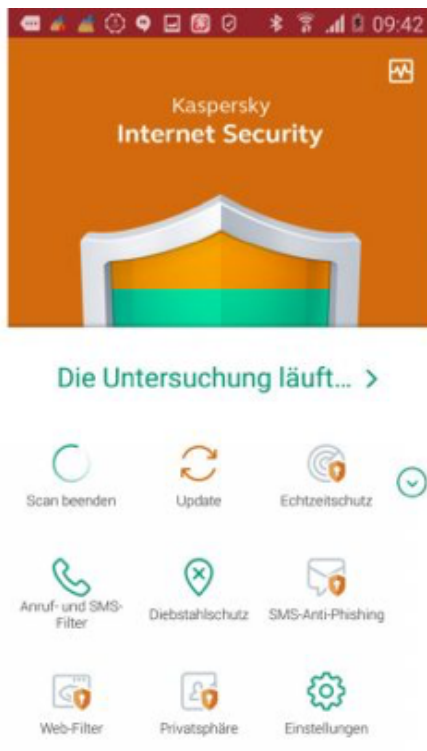


(© 2017 Screenshot/UPDATED)

Kaspersky Antivirus & Security

Die ehemals unter dem Namen Kaspersky Internet Security for Android angebotene Lösung heißt jetzt [Kaspersky Antivirus & Security](#). **Bei der Inbetriebnahme zeichnet sich die App durch eine Vielzahl an Einstellmöglichkeiten aus**, ohne dadurch überfrachtet oder unübersichtlich zu wirken. Der aktuelle Sicherheitsstatus des Android-Smartphones ist anhand der Farbe des raumfüllenden Kaspersky-Schildes am Display leicht zu erkennen. Grün bedeutet alles in Ordnung, Orange zeigt an, dass Sie etwas überprüfen sollten und Rot signalisiert „Malware gefunden“. Wie bei Virensuch-Apps üblich, können Sie auch das Kaspersky-Tool 30 Tage lang mit aktivierten Premiumfunktionen testen, bevor es in den funktionsreduzierten Scan-only-Modus wechselt. Mit 10,95 Euro für ein Premium-Jahr zählt Kaspersky zu den teureren Antiviren-Apps.

Abseits des eigentlichen Scanners gibt es an zusätzlichen Sicherheitsfunktionen Anruf- und SMS-Filter, Schutz vor betrügerischen Webseiten, Telefonortung und eine Vorbeugung vor Identitätsdiebstahl. Interessant für Nutzer einer Android-Smartwatch ist die Unterstützung von Android-Wear.



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)



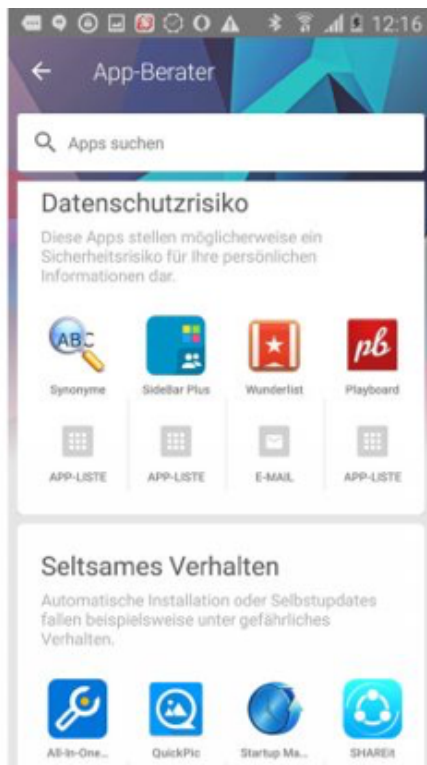
(© 2017 Screenshot/UPDATED)

Norton Antivirus & Sicherheit

Im Lieferumfang unterscheidet sich die App [Norton Antivirus & Sicherheit](#), die am traditionell im Unternehmens-Gelb umrandeten Vorhängeschloss-Icon erkennbar ist, nur unwesentlich von der Konkurrenz: **Neben der Hauptfunktion zum Aufspüren von schadhaften Apps** schützt die Norton-Software vor infizierten Webseiten sowie gefälschten Mails und kann ein geklautes oder verlorengegangenes Handy aus der Ferne sperren. Auch eine Backup-Funktion für Kontakte ist vorhanden.

Beim Preis belegt Norton Antivirus & Sicherheit allerdings den Spitzenplatz: **Stolze 29,99 Euro für ein Jahr verlangt der Hersteller Symantec für seine App.** Auch die Zweijahreslizenz ist umgerechnet nicht viel günstiger, hier werden 49,99 Euro fällig.

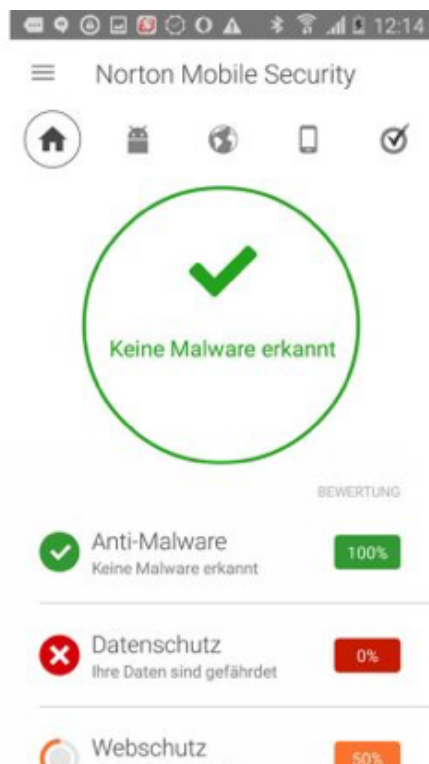
Die App glänzt mit kurzen Update-Intervallen und einer erfahrungsgemäß kurzen Reaktionszeit beim Erscheinen neuer Android-Schädlinge.



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)

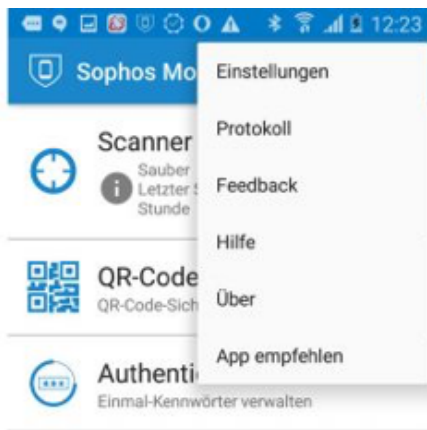


(© 2017 Screenshot/UPDATED)

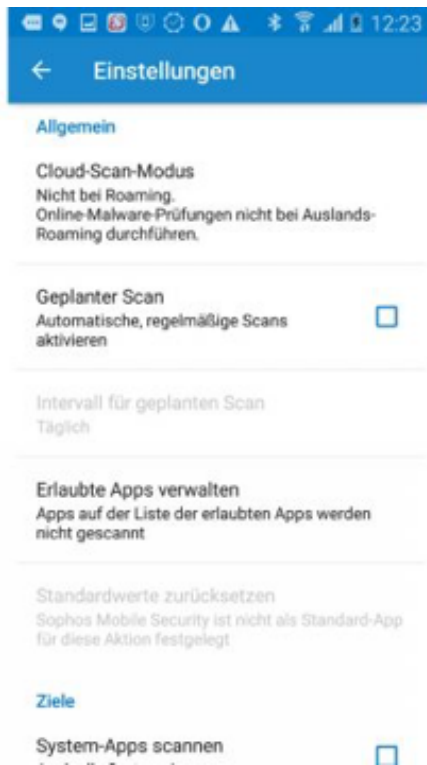
Sophos Mobile Security für Android

Komplett kostenlos und ohne Werbung ist [Sophos Mobile Security für Android](#). In diesem Punkt unterscheidet sich die Sicherheits-App vom Konkurrenzumfeld. Nach der Einrichtung der App werden Sie zur Installation eines ebenfalls kostenlosen Add-ons aufgefordert, das für die Hintergrundüberwachung zuständig ist.

Anschließend präsentiert sich die App mit einem unscheinbaren Hauptmenü. Hier starten Sie den Einzel-Scan, richten nach dem Tippen auf den Button mit den drei Punkten in den Einstellungen eine intervallgetaktete Prüfung ein und starten den Sicherheitsberater, der Tipps zu potenziell unsicheren Android-Einstellungen bietet. Zu den weiteren Funktionen zählen ein Webfilter, ein Privatsphärenberater und die Möglichkeit, sein Mobilgerät im Falle eines Verlusts wiederzufinden, zu sperren und in letzter Konsequenz zu löschen.



(© 2017 Screenshot/UPDATED)



(© 2017 Screenshot/UPDATED)

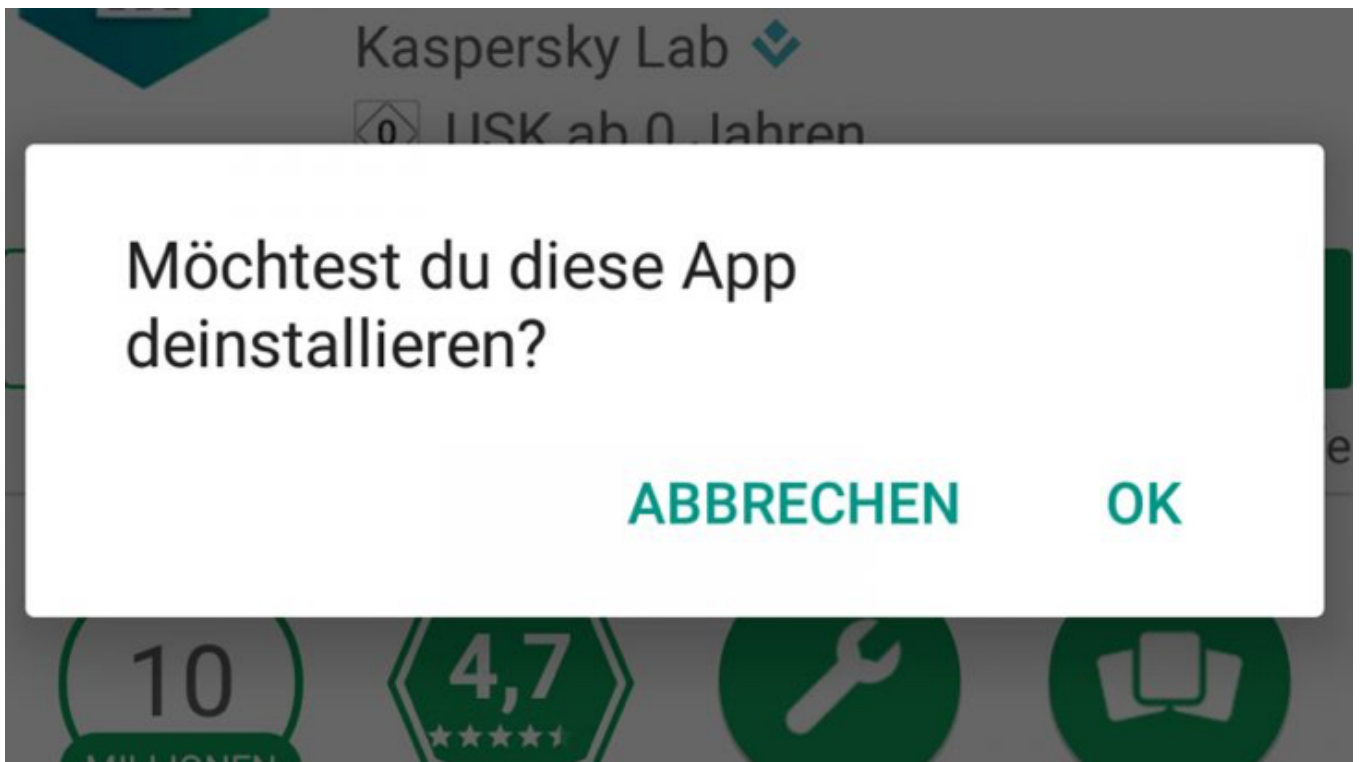


(© 2017 Screenshot/UPDATED)

Nur einen Virenschanner

Viel hilft viel – diese Binsenweisheit gilt nicht bei Virenschannern für Ihr Handy. So verlockend es sein mag, sich vor den zunehmenden Internet-Bedrohungen durch zwei und mehr parallel installierte Android-Virenschanner zu schützen, Ihr Smartphone wird dadurch nicht besser, sondern eher schlechter vor Schädlingen geschützt.

Da die Sicherheits-Apps parallel im Hintergrund arbeiten, kommen sie sich bei den Zugriffsrechten zwangsweise in die Quere. Außerdem belasten die Programme den Prozessor und Arbeitsspeicher Ihres Smartphones, das dadurch langsamer wird und träge reagiert. Wenn Sie einen neuen Virenschanner ausprobieren, empfiehlt es sich, **zunächst den alten über den Google Play Store zu deinstallieren**, bevor Sie die neue App herunterladen.



Deinstallieren Sie einen vorhandenen Virenschanner, bevor Sie eine neue Antiviren-App für Android herunterladen. (© 2017 Screenshot/UPDATED)

Verseuchte Apps erkennen

Ein Großteil der erfolgreichen Schädlingsattacken auf Android-Smartphones basiert auf verseuchten Apps im Google Play Store. Manche Anwender installieren wahllos im Play Store angebotene Anwendungen und Spiele, wenn sie nur halbwegs Spannung versprechen oder gute Nutzerbewertungen erzielt haben. Neben vielen Tausenden unauffälliger Apps schaffen es jedoch regelmäßig auch schädliche Programme in den Store. Deren Hintermänner sorgen mit technischen Tricks dafür, dass diese Apps dank gefälschter Positivbewertungen von möglichst vielen Nutzern wahrgenommen und auf ihren Geräten geladen werden. Dabei ist es gar nicht so schwer, potenziell gefährliche Apps auszumachen. **Achten Sie dabei auf diese bei jeder App im Google Play Store angegebenen Kriterien:**

- Wie lange ist die App bereits im Google Play Store zu haben?
- Wie viele Nutzer haben sie bereits heruntergeladen?
- Wie bewerten andere Nutzer die App?

Stolpern Sie im Play Store über eine brandneue App, die erst wenige Tage angeboten wird, die bislang nur von einer Handvoll Nutzer installiert wurde

und sehr positive, wenngleich nichtssagende Bewertungen hat, empfiehlt es sich, mit dem Download besser ein paar Tage zu warten, um nicht auf eine App-Fälschung oder eine virenverseuchte App hereinzufallen.

Es gibt jedoch immer wieder Apps, die bereits seit Längerem im App Store angeboten wurden, dementsprechend von vielen Anwendern genutzt werden und urplötzlich mit einem Virus verseucht sind. In solchen Fällen helfen die aktuellsten Nutzerkommentare. Haben Sie Zweifel an einer App, empfiehlt es sich, zunächst einmal im Web nach weiteren Informationen zu dieser App suchen.

iOS-Geräte vor Viren schützen

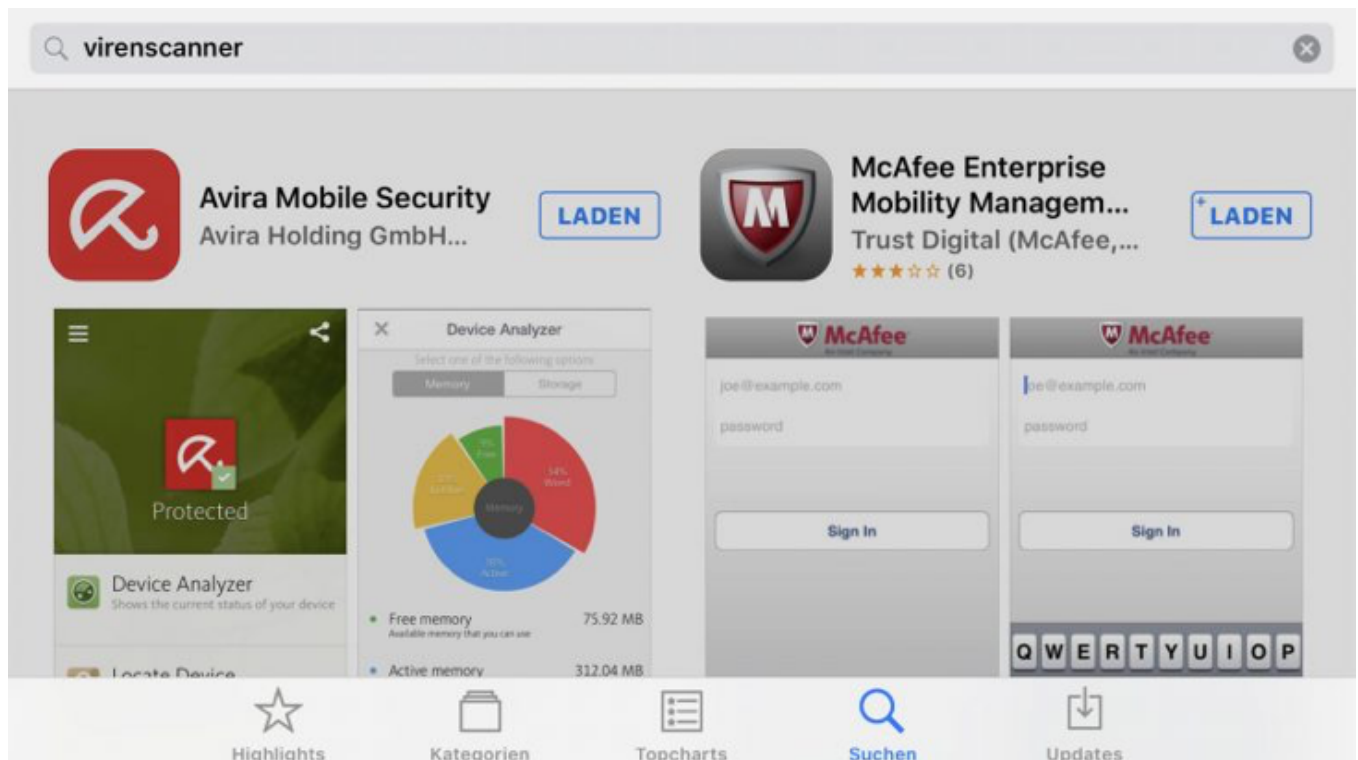
Antivirus-Apps sind in iOS aufgrund der Abschottung des Betriebssystems nicht wirksam und damit überflüssig. Dennoch finden sich im App Store vermeintliche Virens Scanner und Security-Suiten teils von namhaften Herstellern, die den Anschein erwecken, Malware vom iPhone oder iPad fernzuhalten. Anders als in Android laufen die einzelnen Apps in iOS und das Betriebssystem selbst abgeschottet voneinander. Dadurch ist ein Virens Scanner nicht in der Lage, andere laufende Programme oder gar das Gesamtsystem nach Schädlingen abzusuchen. Virens Scanner, die den Speicher und die Apps untersuchen, funktionieren in iOS schlichtweg nicht.

Auch aus diesem Grund gilt iOS unter Sicherheitsexperten derzeit im Hinblick auf klassische Viren als ein weitgehend sicheres Mobilbetriebssystem. Im Unterschied zu Android, das als offenes System konzipiert wurde, sind Angriffe durch Schadprogramme auf Apples geschlossenen iOS-Kosmos zwar nicht unmöglich, aber das System ist insgesamt weniger anfällig dafür.

Auch Gefahr für iOS durch virenverseuchte Mailanhänge droht normalerweise nicht, denn solche Viren können in der Mail-App in iOS keinen Schadcode ausführen. **Denkbar sind allerdings virenverseuchte Mailanhänge,** die Windows-PCs infizieren und sich auf die dort installierte iTunes-Software stürzen, mögliche Sicherheitslücken ausnutzen und so beim nächsten Synchronisieren aufs iPhone oder iPad gelangen. Sie schützen sich bestmöglich davor, indem Sie iTunes und iOS regelmäßig aktualisieren. iTunes-

Updates spielen Sie in macOS über den App Store ein, in Windows erhalten Sie beim Start von iTunes einen Update-Hinweis, sobald eine neuere Version verfügbar ist. Auf Updates für iOS weist Sie Ihr iPhone und iPad automatisch hin.

Ein Jailbreak, unter dem das Entfernen von Nutzungsbeschränkungen zu verstehen ist und der alle von Apple in iOS eingebaute Sicherheitsmechanismen aushebt, bedeutet ein drastisch erhöhtes Risiko eines Befalls mit schädlichen Programmen.



Sicherheits-Tools für iOS bieten allerlei Funktionen, jedoch keinen richtigen Virens scanner, da iOS Scans auf andere Dateien und Apps unterbindet. (© 2017 Screenshot/UPDATED)

Erste Hilfe bei Virenfund

Hat ein Virus den Weg auf Ihr Smartphone oder Tablet gefunden, haben Sie mehrere Möglichkeiten, den Schädling loszuwerden. Wenn Sie bereits einen Virens scanner auf Ihrem Gerät installiert haben, der Ihnen den Schädlingsfund meldet, **folgen Sie den Anweisungen der App zur Entfernung des digitalen Parasiten**. Am sichersten ist es, den Infektionsherd direkt vom Virens scanner löschen zu lassen. Ist noch kein Virens scanner aktiv, installieren Sie einen.

Besonders hartnäckige Viren setzen sich so im System fest, dass eine Entfernung fehlschlagen kann. In diesem Fall empfiehlt sich **ein Zurücksetzen des Geräts auf die Werkseinstellungen**. Dabei wird der gesamte Speicherinhalt gelöscht und damit ebenfalls die Malware bzw. der Virus beseitigt.

Fazit: Auf Dauer virenlos am Smartphone

Gefahren für Smartphones und Tablets drohen von vielen Seiten: Verseuchte Apps oder schädliche Webseiten könnten Sicherheitslücken ausnutzen und infolgedessen Daten stehlen oder manipulieren. Auch die Anzahl an Mails mit virenverseuchtem Anhang steigt kontinuierlich. Da ist es eine gute Idee, das eigene Android-Smartphone mit einem aktuellen Virenschanner zu schützen. Wichtig ist es, die Antiviren-App selbst auf dem neuesten Stand zu halten, um deren Sicherheit zu gewährleisten.