

# Virens Scanner für Android - brauche ich das?

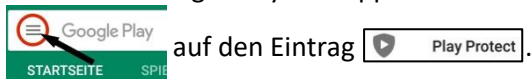
Nach Windows und macOS haben die Hersteller von Anti-Viren-Programmen schon seit geraumer Zeit Android als neuen Markt für sich entdeckt. Tatsächlich finden sich fast alle großen Sicherheitssuiten aus der Windows-Welt mittlerweile auch im Google Play Store. Avira, G-Data, Avast und Konsorten versprechen, Ihr Android-Smartphone vor Malware und anderen Sicherheitsbedrohungen zu schützen. Doch brauchen Sie wirklich eine dauerhaft laufende App, um sich zuverlässig vor Android-Viren zu schützen?

## Google Play Protect: So nutzen Sie den integrierten Virens Scanner von Android

Seit Sommer 2017 verteilt Google mit Google Play Protect eine neue Sicherheitslösung für Android. Google Play Protect prüft automatisch alle bereits installierten sowie alle neuen Apps auf Sicherheitsbedrohungen. Erkennt der Dienst ein Sicherheitsproblem, warnt er Sie automatisch und entfernt die gefährlichen Apps. Der Clou dabei: Play Protect kommt durch ein automatisches Update der Google-Play-Dienste auf alle Androiden, Sie müssen die Sicherheitslösung also nicht manuell installieren und aktivieren.

Um den Status und die Verfügbarkeit von Play Protect zu prüfen, gehen Sie folgendermaßen vor:

Starten Sie Google Play und tippen Sie im Menü



auf den Eintrag

Play Protect zeigt nun den aktuellen Sicherheitsstatus sowie die zuletzt geprüften Apps. Achten Sie darauf, dass die Option „Gerät auf Sicherheitsbedrohungen prüfen“ eingeschaltet ist. Optional können Sie auch via „Erkennung von schädlichen Apps verbessern“ weitere Infos an Google übermitteln. Diese umfassen unter anderem Apps, die Sie aus alternativen Quellen installiert haben, sowie deren Herkunft.

In neueren Android-Versionen taucht Google Play Protect nicht nur im Play Store, sondern auch als neues **Untermenü in den Systemeinstellungen** auf. Hier fasst Android ab Android 8.0 auch den aktuellen Sicherheitsstatus deines Smartphones zusammen.

## 5 Tipps: So schützen Sie Ihr Android-Smartphone vor Schadsoftware

1. Keine Apps aus unbekannten Quellen installieren:  
Die meisten Malware-Apps verbreiten sich nicht über den Google Play Store, sondern über alternative Downloadportale. Auch „Drive-by-Downloads“, also bösartige Apps, die sich über korruptierte Webseiten auf Ihr Handy schmuggeln, sind eine reale Gefahr – zumindest, wenn Sie die Installation erlauben. Denn: Ab Werk unterbindet Android die Installation von Apps außerhalb des Play Stores. Um sicherzustellen, dass dies der Fall ist, werfen Sie einen Blick in die Einstellungen Ihres Smartphones. Sie finden die Option zur Installation von Apps aus unbekannten Quellen im Bereich „Sicherheit“. Deaktivieren Sie sie, um unbefugte Installationen zu verhindern.  
Der Nachteil dieser wichtigen Sicherheitsmaßnahme: Sie müssen auch auf seriöse Alternativ-Quellen wie den Open-Source-Marktplatz **F-Droid** oder das App-Archiv **APKMirror** verzichten. Bei Bedarf können Sie die Einstellung vorübergehend deaktivieren. Übrigens: Ab Android 8.0 alias „Oreo“ gibt es die Einstellung nicht mehr. Hier fragt Android bei jeder Installation aus fremden Quellen nach, ob Sie die Installation erlauben wollen oder nicht. So können Sie von Fall zu Fall entscheiden, ob Sie der App trauen oder nicht.
2. Android-Updates installieren:  
Nicht nur installierte Apps können Ihr Smartphone gefährden. Wie jedes Betriebssystem tauchen in Android immer wieder Sicherheitslücken auf, die Angreifer ausnutzen können. Google liefert aus diesem Grund regelmäßige Sicherheitsupdates für sein Mobilsystem – leider kommen diese nur selten auf allen Geräten an. Abseits von Googles Nexus- und Pixel-Smartphones hängen viele Geräte auf alten Android-Versionen fest. Wenn es ein Update für Ihr Smartphone gibt, sollten Sie es aber dennoch installieren. Ob ein Update verfügbar ist, können Sie in den Smartphone-Einstellungen überprüfen. Suchen Sie hier nach einem Eintrag wie „Systemupdates“ oder ähnlichen und befolgen die Anweisungen, um Ihren Androiden zu ak-

tualisieren. Infos über den aktuellen Stand der Android-Sicherheitsupdates bekommen Sie direkt von den Android-Entwicklern unter <https://source.android.com/security/bulletin/>.

3. App-Berechtigungen prüfen:  
Allen Sicherheitsbemühungen seitens Google zum Trotz: Android-Apps können bei Bedarf auf viele sensible Daten zugreifen. Davon macht natürlich auch Malware fleißig Gebrauch. Zum Glück finden Sie im Play Store unter „Berechtigungsdetails“ alle Zugriffe, die eine App auf Ihrem Smartphone braucht. Hier sollten Sie aufmerksam sein: Will ein simples Handy-Spiel beispielsweise Ihre SMS oder gar E-Mails lesen, sollten Sie skeptisch sein. Seriöse App-Entwickler erklären in der Play-Store-Beschreibung, warum die Berechtigungen nötig sind.
4. Augen auf bei App-Updates:  
Auch nach der Installation sollten Sie Ihre Android-Apps im Auge behalten. Das gilt erst recht, wenn Sie sie später aktualisieren. Es gab in der Vergangenheit mehrere Fälle, in denen Malware-Entwickler zunächst harmlose Programme per Update zum Android-Schädling gemacht haben. Prüfen Sie also vor allem bei „kleineren“ Apps vor der Aktualisierung, was diese mit sich bringt. Besonders aufmerksam sollten Sie sein, wenn eine App für ein Update neue Zugriffsrechte auf Ihrem Smartphone verlangt. Android weist in diesem Fall darauf hin. Sie sollten dann im Changelog der App prüfen, wofür die neuen Rechte nötig sind.
5. Informiert bleiben:  
Die Kombination aus Google Play Protect und unseren Sicherheitstipps sollten Ihr Smartphone vor so gut wie allen Android-Gefahren schützen. Dennoch schadet es nicht, in Sachen Android-Sicherheit auf dem neuesten Stand zu bleiben. Webseiten wie Heise Security oder das offizielle Android Security Center informieren regelmäßig über aktuelle Bedrohungen und wie Sie sich dagegen schützen können.

## Sind Android-Virens Scanner überflüssig?

Die Frage, ob separate Virens Scanner unter Android völlig überflüssig sind, lässt sich dennoch nicht so pauschal beantworten. Wenn Sie regelmäßig Apps aus fremden Quellen installieren, kann eine „zweite Meinung“ in Sachen Sicherheit gegebenenfalls sinnvoll sein. Auch das Verschicken von E-Mails über das Smartphone kann zum Sicherheitsproblem werden, wenn potentiell infizierte Anhänge ohne Überprüfung weitergeleitet werden. Viele Sicherheitssuiten für Android bieten Zusatzfunktionen, die das Basis-System nicht bietet. So können sie beispielsweise bestimmte Anrufe blockieren oder per Firewall-Funktion Apps daran hindern, im Hintergrund Daten zu verschicken. Außerdem bieten die Suiten oft erweiterte Funktionen, um verlorene oder gestohlene Smartphones wiederzufinden oder bei Bedarf aus der Ferne zu löschen.

Einiges davon kann Android zwar auch mit Bordmitteln, je nach Smartphone und Android-Version, doch gegebenenfalls sind die Extra-Features die Installation wert. Größere Nachteile in Sachen Akkulaufzeit und Performance entstehen unseren Erfahrungen nach durch die Installation von Android-Malware-Scannern nur selten. Dennoch sollten Sie darauf achten, dass die Sicherheitslösungen nicht ihrerseits durch übertriebene Datensammelei oder nervige Werbung auffallen. Ist dies der Fall, schmeißen Sie die App lieber wieder von Ihrem Smartphone – einen größeren Sicherheitsmalus erleiden Sie dadurch nicht.

Um nach Antivirenprogrammen zu suchen, geben Sie in das Suchfeld des Google Play Store das Wort „Antivirus“ ein.