

F-SECURE MOBILE SECURITY

Schritt für Schritt erklärt

Inhalt

Was ist F-Secure F-Secure Mobile Security?	
Wo kann ich die aktuelle Version von F-Secure Mobile Security herunterladen?	2
Welche Funktionen sind in F-Secure Mobile Security enthalten?	3
Warum kann ich die Diebstahlsicherung unter Mobile Security nicht mehr verwenden?	3
Kann ich mit Mobile Security so im Internet surfen wie auf dem PC?	4
Wie erkenne ich, ob ich beim Online-Banking geschützt bin?	4
Wird mein Gerät auch auf Viren geprüft?	5
Wie kann ich mein Gerät manuell auf Viren prüfen?	5
Kann ich auch einen geplanten Scan erstellen?	5
Kann mein Gerät beim Starten automatisch gescannt werden?	6
Kann ich meine Kinder beim Surfen schützen?	6
Kann ich dieselbe Lizenz auf einem anderen Gerät verwenden?	7
Warum ist Safe Browser als Standardbrowser eingestellt?	7

Sollte Ihnen dieses FAQ eine Frage nicht beantworten können, stehen wir Ihnen gerne persönlich zur Verfügung. Schreiben Sie uns eine E-Mail an hallo@edv-buchversand.de oder kontaktieren Sie uns telefonisch:

0 21 91 99 11 99

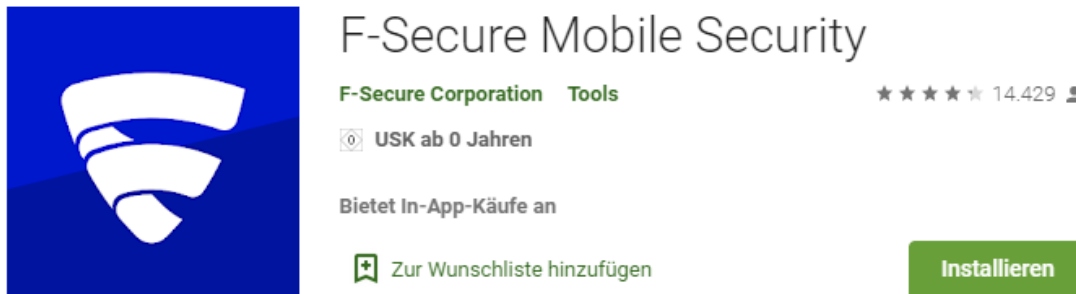
(Mo.-Fr.: 8:30 – 17:00 Uhr)

Was ist F-Secure Mobile Security?

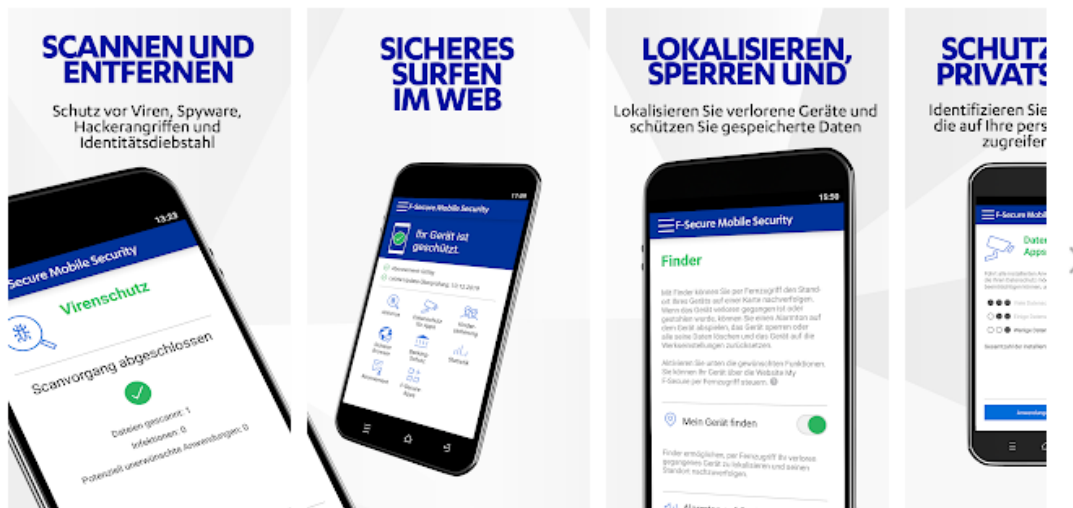
F-Secure Mobile Security ist eine komplette Sicherheits-Lösung für Ihr Android-Smartphone und -Tablet (ab Android 5.0). Es schützt zuverlässig und umfassend die Inhalte Ihres Gerätes, gewährt Ihnen und Ihren Kindern Sicherheit beim Surfen und unterstützt Sie bei Verlust oder Diebstahl Ihres Mobiltelefons.

Wo kann ich die aktuelle Version von F-Secure Mobile Security herunterladen?

Sie können das Mobile Security-Installationspaket im [Google Play Store](#) herunterladen.



F-Secure Mobile Security
F-Secure Corporation Tools ★★★★★ 14.429
USK ab 0 Jahren
Bietet In-App-Käufe an
Zur Wunschliste hinzufügen **Installieren**



SCANNEN UND ENTFERNEN
Schutz vor Viren, Spyware, Hackerangriffen und Identitätsdiebstahl
Virenschutz
Scanvorgang abgeschlossen
Daten gesichert: 1
Infektionen: 0
Potenziell unerwünschte Anwendungen: 0

SICHERES SURFEN IM WEB
Ihr Gerät ist geschützt
Viren
Webfilter
VPN
App-Schutz
App-Integrität
App-Integrität

LOKALISIEREN, SPERREN UND
Lokalisieren Sie verlorene Geräte und schützen Sie gespeicherte Daten
Finder
Lokalisieren Sie verlorene Geräte und schützen Sie gespeicherte Daten
Mein Gerät finden
Finder ermöglicht per Fernzugriff ein verlor
gegangenes Gerät zu lokalisieren und sicher
Sturmt zu reaktivieren.

SCHUTZ PRIVATS
Identifizieren Sie die auf Ihre pers
zugreifen
Daten Apps
Lokalisieren Sie verlorene Geräte und schützen Sie gespeicherte Daten

F-Secure Mobile Security für Smartphone & Tablet. JETZT GRATIS TESTEN – werbefrei und bedienerfreundlich!

Welche Funktionen sind in F-Secure Mobile Security enthalten?

BROWSER-SCHUTZ

Schützt die Sicherheit von Webseiten ein – für sicheres Surfen im Internet

BANKING-SCHUTZ

Für sicheres Online-Banking – schützt vor schädlicher Software

KINDERSICHERUNG

Schützen Sie Ihre Kinder vor schädlichen Websites, indem Sie unsichere Seiten oder Apps sperren.

Warum kann ich die Diebstahlsicherung unter Mobile Security nicht mehr verwenden?

Aufgrund von Änderungen der Richtlinien von Google für Benutzerdaten und -berechtigungen im Oktober 2018 können einige der derzeit in F-Secure SAFE für Android und Mobile Security für Android unterstützten Funktionen nicht mehr angeboten werden, andere werden entsprechend den neuen Richtlinien geändert.

Die Einstellung und Entfernung dieser Funktionen aus der Software war unvermeidlich um sicherzustellen, dass die F-Secure Software weiterhin in Google Play angeboten werden kann.

Die davon betroffenen Funktionen sind:

- **Anrufsperr**: Diese Funktion wurde vollständig entfernt. Sie steht in der Benutzeroberfläche nicht mehr zur Verfügung, und Anrufe werden nicht mehr gesperrt.
- **SIM-Wechsel melden**: Diese Funktion wurde vollständig entfernt und wird nicht mehr unterstützt.
- **SMS-gestützte Diebstahlsicherung** als Funktion von Mobile Security für Android: Da die SMS-gestützte Diebstahlsicherung SMS-Berechtigungen nutzt, wurde diese Funktion entfernt und ist nicht mehr verfügbar.

Anmerkung: Wir raten Kunden mit Mobile Security für Android dringend dazu, zu F-Secure SAFE zu wechseln. F-Secure SAFE bietet Diebstahlschutzfunktionen wie den https-basierten Finder mit einem Verwaltungsportal.

Alle Infos zu F-Secure SAFE finden Sie direkt [hier](#)

Kann ich mit Mobile Security so im Internet surfen wie auf dem PC?

Ja! Mithilfe des **sicheren Browsers** können Sie sicher im Internet surfen und verhindern, dass Sie schädliche Websites unbeabsichtigt öffnen. Zusätzlich wird Ihr Webbrowser bei Online-Banking-Sitzungen durch eine zusätzliche Sicherheitsschicht geschützt.

Sobald Sie eine Website besuchen, prüft das Produkt automatisch deren Sicherheit. Ist die Website als verdächtig oder gefährlich eingestuft, blockiert das Produkt den Zugriff auf diese Website. Die Sicherheitseinstufung einer Website basiert auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partner von F-Secure.

Wie erkenne ich, ob ich beim Online-Banking geschützt bin?

Sicheres Banking erhöht die Sicherheit, sobald Sie eine Banking-Website besuchen, und hindert schädliche Software daran, Ihre persönlichen Daten zu versenden.

Sobald **Sicheres Browsen** in Ihrem Produkt aktiviert ist, wird es automatisch gestartet, wenn Sie einen unterstützten Webbrowser öffnen.

1. Starten Sie einen der folgenden Webbrowser im Android Launcher:

- F-Secure Safe-Browser
- Dolphin

2. Öffnen Sie eine Banking-Website.

Sicheres Browsen informiert Sie darüber, dass Sie eine vertrauenswürdige Banking-Website geöffnet haben.

Wird mein Gerät auch auf Viren geprüft?

Ja! Mobile Security scannt Ihr Gerät auf Viren, schädliche Inhalte und andere Gefahren für Ihr Gerät oder Ihre Daten. Es überprüft installierte Programme und verwendete Speicherkarten automatisch auf Viren, Spyware und Riskware.

Sie können das Gerät und die Speicherkarte jederzeit manuell scannen. Darüber hinaus können Sie festlegen, dass Scans in regelmäßigen Intervallen durchgeführt werden.

Tipp: Wir empfehlen Ihnen, Ihr Gerät nach Gefahren zu scannen, sobald das Produkt Sie dazu auffordert. Sie können auch die **Security Cloud** aktivieren, um so über einen schnelleren und präziseren Schutz vor Gefahren zu verfügen.

Wie kann ich mein Gerät manuell auf Viren prüfen?

Sie können Ihr Gerät zu jedem beliebigen Zeitpunkt auf Viren und anderen böartigen Code überprüfen.

1. Navigieren Sie zum Bildschirm **Anti-Virus**
2. Tippen Sie auf „*Jetzt scannen*“ – der Anti-Virus-Scan wird gestartet
3. Nach dem Scan-Vorgang zeigt das Produkt die folgenden Informationen an:
 - Die Anzahl der gescannten Dateien
 - Die Anzahl der entdeckten Infektionen.
 - Potenziell unerwünschte Anwendungen
4. Tippen Sie auf „*Fertig*“, um den Scan zu beenden

Kann ich auch einen geplanten Scan erstellen?

Ja! Sie können eine Zeit festlegen, zu der Ihr Gerät automatisch in regelmäßigen Intervallen auf Viren und anderen schädlichen Code überprüft wird – z. B. täglich, wöchentlich oder monatlich.

So legen Sie einen planmäßigen Scanvorgang fest:

1. Navigieren Sie zum Bildschirm **Anti-Virus**.
2. Tippen Sie auf dem Bildschirm **Anti-Virus** auf „*Einstellungen*“.
3. Wählen Sie „*Geplanten Scan aktivieren*“, um den Scanvorgang zu aktivieren.
4. Wählen Sie unter „*Scanhäufigkeit*“, wie oft Sie Ihr Gerät scannen möchten:
 - **Täglich** – Das Gerät wird täglich überprüft.
 - **Wöchentlich** – Das Gerät wird jede Woche an einem ausgewählten Tag überprüft.
 - **Monatlich** – Das Gerät wird am ersten Tag jedes Monats überprüft.
5. Legen Sie unter „*Tag festlegen*“ fest, wann der Scan starten soll. Der planmäßige Scanvorgang startet automatisch und wird im Hintergrund ausgeführt.

Eine Benachrichtigungsmeldung informiert Sie über Beginn und Ende jedes geplanten Scanvorgangs.

Kann mein Gerät beim Starten automatisch gescannt werden?

Ja! Sie können festlegen, dass der Antivirus-Schutz Ihr Gerät beim Einschalten immer überprüft.

1. Tippen Sie auf dem Bildschirm **Anti-Virus** auf „*Einstellungen*“ – der Bildschirm der Anti-Virus-Einstellungen wird geöffnet.
2. Wählen Sie **Boot-Scan**, um den Scan zu aktivieren, der den Startvorgang Ihres Geräts jedes Mal überprüft, wenn das Gerät gestartet wird.

Kann ich meine Kinder beim Surfen schützen?

Ja! Mobile Security hilft dabei, Ihre Kinder vor unangemessenen Inhalten im Internet zu schützen. Das Internet bietet eine Vielzahl interessanter Websites, birgt jedoch auch zahlreiche Risiken für Kinder, wenn diese, in der Regel ohne Aufsicht, mit ihren Mobilgeräten im Internet surfen. Viele Websites enthalten Inhalte, die Sie womöglich als unangemessen für Ihre Kinder betrachten. Darüber hinaus können sie unbeabsichtigt Malware herunterladen, die das Gerät schädigt, oder sie könnten belästigende Nachrichten erhalten, nachdem sie unsichere Websites besucht haben.

Mit dem **Familienmanager** können Ihre Kinder mit ihren Mobilgeräten sicher im Internet surfen, indem Sie den **Zugriff auf unerwünschte Inhalte blockieren**. Sie können zudem auch Ihre Kinder schützen, indem Sie **unerwünschte Apps blockieren**.

[Kann ich dieselbe Lizenz auf einem anderen Gerät verwenden?](#)

Die Lizenz ist gerätespezifisch. Sie können dieselbe Lizenz nicht gleichzeitig auf zwei Geräten verwenden. Wenn derselbe Abonnementschlüssel beim Aktivieren einer neuen Konfiguration verwendet wird, wird die Lizenz auf die neue Konfiguration übertragen. **Sie können die Lizenz bis zu dreimal auf ein anderes Telefon übertragen.** Nach drei Übertragungen kann der Abonnementschlüssel nicht mehr auf einem neuen Gerät aktiviert werden. Außerdem wird das Abonnement auch während der Reputations-Update-Prüfung überprüft. Wenn Sie denselben Abonnementschlüssel auf zwei Geräten verwenden, wird der Abonnementschlüssel nach drei Updates auf dem letzten Gerät gesperrt.

[Warum ist Safe Browser als Standardbrowser eingestellt?](#)

Safe Browser ist als Standardbrowser eingestellt, wenn die Kindersicherung aktiviert ist. Nur dann können wir Sie gegen böartige Websites wie Phishing-Websites und Identitätsdiebstahl schützen. Beispielsweise werden viele Phishing-Nachrichten als Link per E-Mail oder SMS verschickt, und das Betriebssystem öffnet diese Nachrichten im Standardbrowser, sobald der Benutzer auf den Link klickt.