Android sicher machen - 10 Tipps die Sie beachten sollten

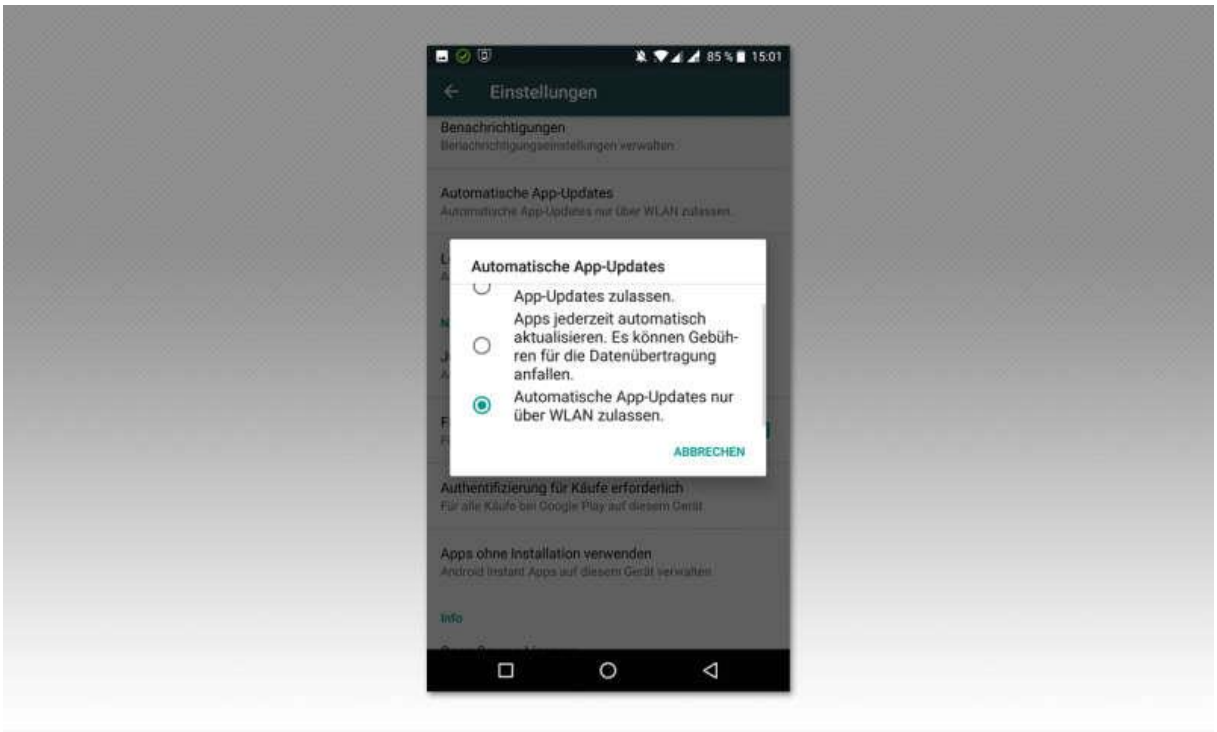
So schützen Sie Ihr Android-Smartphone vor Angriffen und schotten Ihre Daten ab: Mit diesen zehn Tipps machen Sie Ihr Smartphone sicher.

© Production Perig - fotolia.com

Wir geben Tipps für mehr Sicherheit für Ihr Android-Smartphone.

Tipp 1: Displaysperre einrichten

Ohne Sperre öffnen Sie Angreifern die Tür zu all Ihren Daten. Die SIM-Karte ist standardmäßig mit einer PIN geschützt. Wenn nicht, aktivieren Sie diese unter *Einstellungen/ Sicherheit* und *SIM-Sperre*. Außerdem sollten Sie eine Display-Sperre einrichten. Dann kann nur auf das Handy zugreifen, wer Code, Passwort oder das passende Muster kennt. Neuere Smartphones haben oft einen Fingerabdruck-Sensor an Bord, den Sie ebenfalls zur Absicherung verwenden können. Sie stellen die Sperre in den Einstellungen unter Sicherheit und Displaysperre ein.



© Screenshot WEKA / connect

Android sicher machen: Tipp 2 Updates sofort installieren

Tipp 2: Updates sofort installieren

Achten Sie darauf, dass sowohl Betriebssystem als auch alle Programme immer aktuell sind, und installieren Sie Updates umgehend. Die Entwickler liefern mit Aktualisierungen nicht nur neue Funktionen, sondern schließen auch Sicherheitslücken. Wenn es eine neue Android-Version gibt, bekommen Sie eine Benachrichtigung. Bei Apps sollten Sie automatische Updates erlauben. Rufen Sie dazu den Play Store auf und tippen auf die drei Striche oben links. Wählen Sie dann *Einstellungen* und aktivieren *Automatische Updates* – am besten aber nur über WLAN, sonst müssen Sie womöglich für die Datenübertragung zahlen.

Mehr lesen

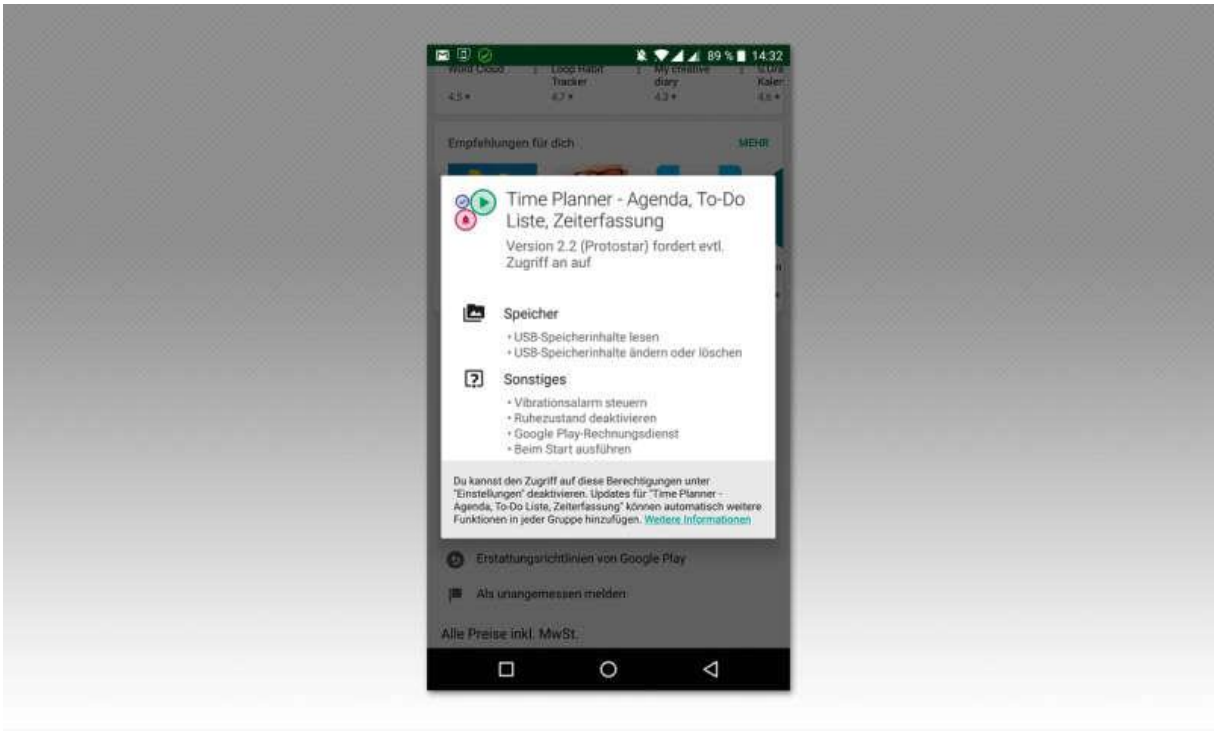
Android-Tipps

Android 8: Oreo clever nutzen mit diesen 9 Tipps

Benachrichtigungen abschalten & aufschieben und Nachtlicht-Modus sind nur einige Neuerungen von Oreo. So können Sie das neue Android clever nutzen.

Tipp 3: Nur im Play Store downloaden

Laden Sie Apps nur aus dem offiziellen Play Store von Google herunter, nicht von möglicherweise dubiosen Webseiten. Denn dort fangen Sie sich mit größerer Wahrscheinlichkeit Viren und Schad-Software ein. Um ganz sicher zu gehen, sollten Sie auf Ihrem Handy die Installation von Apps unbekannter Herkunft unterbinden. Das geht bei älteren Android-Versionen unter *Einstellungen* und *Sicherheit*. Ab Android 8.0 finden Sie den Menüpunkt in den Einstellungen unter *Apps/Spezieller Zugriff*. Ganz unten steht *Unbekannte Apps installieren*. Tippen Sie darauf, sehen Sie alle bereits installierten Apps. Prüfen Sie, ob bei allen steht: Nicht zulässig. Ansonsten tippen Sie darauf und verschieben den Regler.



© Screenshot WEKA / connect

Android sicher machen: Tipp 4 - Auf Berechtigungen achten

Tipp 4: Auf Berechtigungen achten

Überprüfen Sie bei jeder App, die Sie installieren, welche Berechtigungen sie sich einräumen will. Das steht auf der App-Seite im Play Store unter Berechtigungsdetails. Eine Taschenlampen-Funktion benötigt zum Beispiel keinen Internet-Zugriff. Bei schon installierten Apps entziehen Sie einzelne Berechtigungen unter *Einstellungen/ Apps/App-Berechtigungen*.

Tipp 5: Das Smartphone verschlüsseln

Falls ein Fremder trotz aller Sicherheitsaktionen Ihr Handy in die Hand bekommt, sollte er sensible Daten nicht auslesen können – so wie E-Mails, Kontakte oder Zugangsdaten. Davor schützt die Verschlüsselung des Geräts. Bei den meisten Mobiltelefonen müssen Sie diese einmalig selbst anstoßen. Tippen Sie dazu auf *Sicherheit/Verschlüsselung* und wählen dort die Option *Smartphone verschlüsseln*.

Mehr lesen

Sicherheits-Tipps

Smartphone-Sicherheit: Schutz vor Hackern und Malware

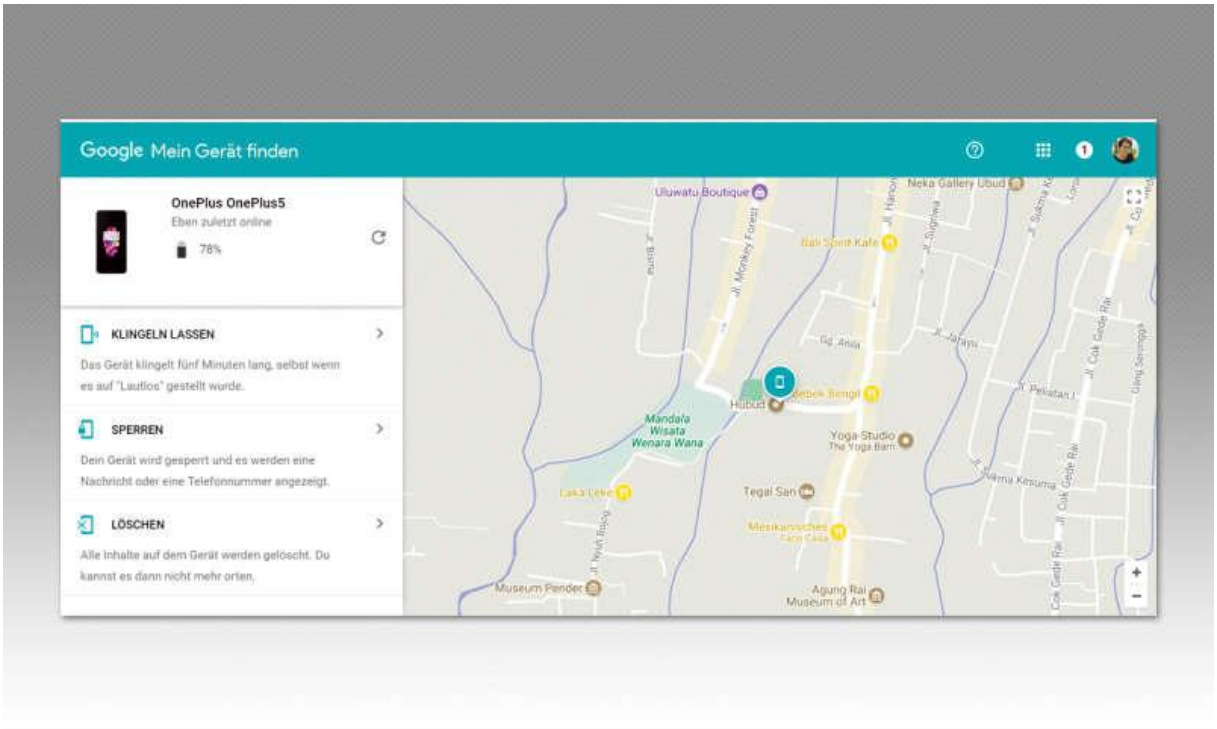
Auch Smartphones können Ziele von Hackerangriffen und Malware werden. Dabei kann man schon mit einfachen Maßnahmen die mobile Sicherheit erhöhen.

Tipp 6: Obacht im offenen WLAN

Im offenen WLAN im Café oder am Flughafen surfen Sie kostenlos. Aber seien Sie vorsichtig: Mit relativ einfachen Mitteln können andere Sie ausspionieren und mitlesen. Sie sollten deshalb dort nie Homebanking machen. Seien Sie zudem zurückhaltend bei allen Seiten, bei denen Sie sich einloggen müssen, so wie E-Mail oder Amazon. Zumindest sollten die Seiten eine SSL-Verschlüsselung beim Login geben, erkennbar am https://. Noch besser: Surfen Sie über eine sichere VPN-Verbindung.

Tipp 7: Verbindungen deaktivieren

Apps können über GPS und WLAN-Netze Ihren Standort ermitteln und Bewegungsprofile erstellen. Sie sollten deshalb alle Netzwerk-Funktionen deaktivieren, wenn Sie sie nicht ständig benutzen. Dazu gehören auch Bluetooth und NFC, denn die Schnittstellen können Angreifern potenzielle Einfallstore bieten. Sie schalten all diese Funktionen in den Einstellungen ab – unter *Drahtlos und Netzwerke* und unter *Standort*. Schieben Sie jeweils den virtuellen Regler auf die Aus-Position.



© Screenshot WEKA / connect

Android sicher machen: Tipp 8 - Diebstahlschutz aktivieren

Tipp 8: Diebstahlschutz aktivieren

Es hat Vorteile, wenn Sie die Standortermittlung einschalten: Sie können dann Ihr Handy orten, falls es verloren geht. Zudem lassen sich dann aus der Ferne alle Daten löschen. Sie müssen die Funktion natürlich vor dem Geräteverlust eingeschaltet haben. Erlauben Sie die Standortermittlung unter *Einstellungen/Nutzer und Standort*. Dann aktivieren Sie *Sicherheit* und *Mein Gerät finden*. Im Notfall rufen Sie im Browser https://accounts.google.com auf und melden sich dort mit Ihrem Google-Konto an.

Tipp 9: Regelmäßige Backups

Wenn das Smartphone den Geist aufgibt, sind alle Daten weg – außer, Sie sichern sie regelmäßig. Ein Backup der Fotos klappt am einfachsten mit Cloud-Diensten wie Google Drive oder OneDrive, die diese automatisch speichern. Die Einstellungen und Daten von Apps, WLAN-Passwörter oder den Anrufverlauf sichert Google. Aktivieren Sie das über *Einstellungen/Sichern & zurücksetzen* und *Meine Daten sichern*.

Tipp 10: Sicherheits-App verwenden

Bereits die kostenlosen Sicherheits-Apps etwa von Kaspersky, Avira oder Bitdefender schützen vor Malware und scannen neue Programme auf Bedrohungen. Manche bringen sogar Funktionen zur Diebstahlsicherung mit. Ab Android 8.0 aktivieren Sie in den Einstellungen zudem als Zusatz-Schutz die Funktion Play Protect, die installierte Apps auf Sicherheitslücken überprüft.