10 TIPPS FÜR MEHR SICHERHEIT EINES ANDROID-HANDYS

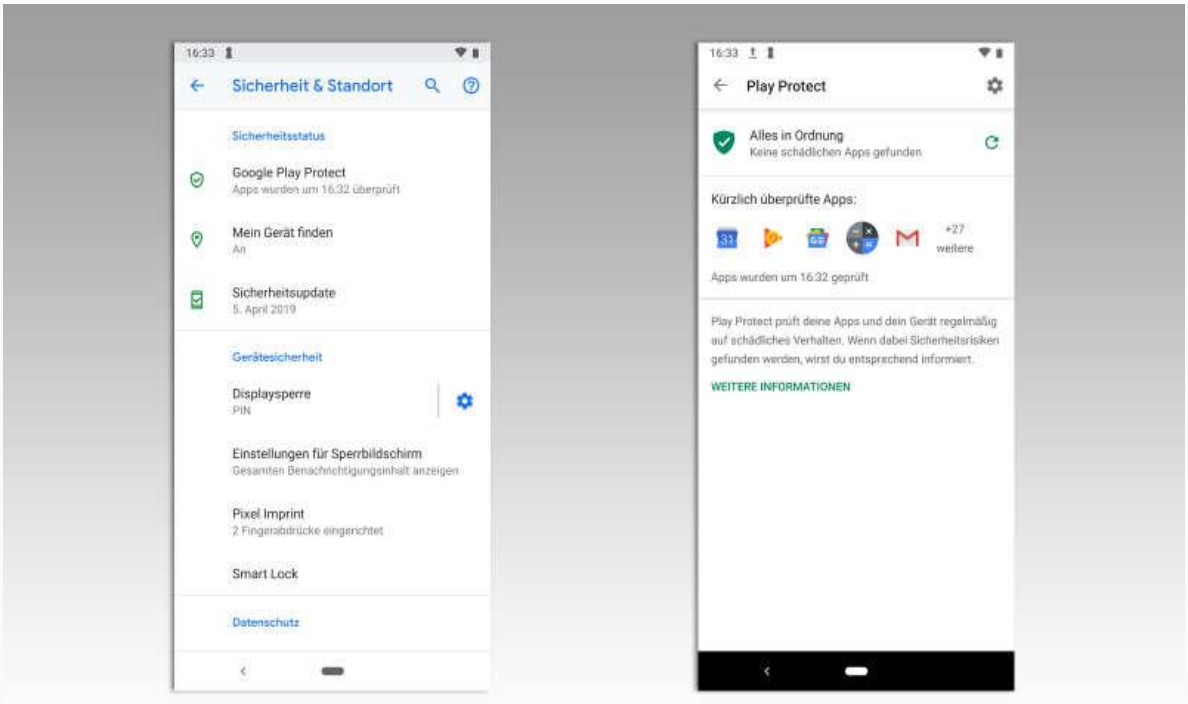
Android ist nicht nur ein weit verbreitetes Betriebssystem, seine Nutzer kämpfen auch immer wieder mit Sicherheitsproblemen. Immer wieder muss Google gleich mehrere Dutzend oder sogar hunderte gefährliche Apps aus dem Play Store löschen. Um Ihr Handy vor Angriffen zu schützen, müssen Sie aber nicht zwangsläufig in einen Virenscanner investieren. Schon in den Android-Einstellungen finden Sie einige Optionen, die für mehr Sicherheit sorgen.

Den Beitrag haben wir unter Android 11 auf einem Google Pixel 3 erstellt. Ältere Android-Versionen bieten vergleichbare Einstellungen, die Bezeichnung kann aber - auch abhängig vom Handy-Hersteller - abweichen.

ANZEIGE

Tipp 1: Google Play Protect

Google Play Protect ist eine Sammlung von Funktionen, die Ihr Handy vor gefährlichen Apps und gefährlichen Websites schützen sollen und dank denen Sie Ihr Handy aus der Ferne orten, sperren und löschen können. Google hat diese Funktionen unter dem Namen Google Play Protect zusammengefasst. Das hat den Vorteil, dass Sie ganz leicht kontrollieren können, ob Google Play Protect auf Ihrem Handy aktiv ist. Genau das sollten Sie jetzt tun.



Öffnen Sie die Einstellungen und gehen Sie auf „Sicherheit“. Unter „Google Play Protect“ sollten Sie auf ein aktives Google Play Protect treffen. Eventuelle Warnhinweise, die sich aus einer Systemprüfung durch Google Play Protect ergeben haben könnten, erscheinen hier ebenfalls.

Tippen Sie auf das Zahnradsymbol rechts oben. Anschließend stellen Sie sicher, dass die Optionen „Gerät auf Sicherheitsbedrohungen prüfen“ und „Erkennung schädlicher Apps verbessern“ aktiv sind.

Tipp 2: Mein Gerät finden

Ob Sie Ihr Handy nun verlegt oder verloren haben, mit der Funktion „Mein Gerät finden“ lässt es sich in vielen Fällen rasch aufstöbern. Ist das Handy abhanden gekommen, dann besuchen Sie einfach die Website android.com/find, loggen sich dort mit Ihrem Google-Konto ein und lassen sich das Handy auf einer Karte anzeigen. Sie können es klingeln lassen, es sperren und Ihre Daten vom Gerät löschen - alles aus der Ferne.

Eine der Voraussetzungen für „Mein Geräte finden“ ist eine Online-Verbindung für Ihr Handy. Kein WLAN? Kein Mobilfunk? Dann lässt sich das Gerät auch nicht aufstöbern.

Eine andere Voraussetzung ist, dass Sie sich auf dem Handy mit Ihrem Google-Konto angemeldet haben. Unter „Einstellungen > Konten“ sollte ein entsprechender Eintrag zu finden sein. Anderenfalls fügen Sie Ihr Konto hier hinzu. Anschließend überprüfen Sie, dass „Mein Gerät finden“ in den Einstellungen unter "Sicherheit" aktiv ist.

Tipp 3: Sperrbildschirmnachricht

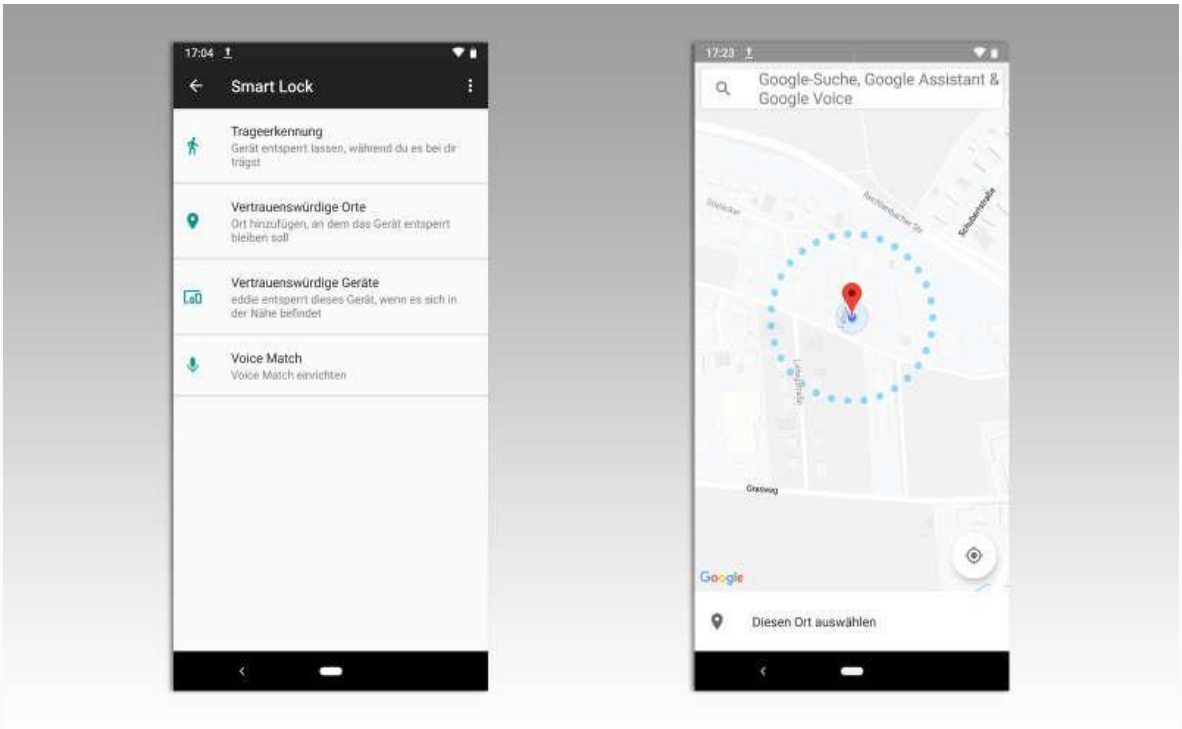
Wenn „Mein Gerät finden“ nicht funktioniert, dann kommt die Sperrbildschirmnachricht ins Spiel. Mit ihrer Hilfe können Sie dem Finder einen Hinweis darauf geben, wie er das Handy zurückbringen kann. Die Nachricht erscheint nämlich auf dem Sperrbildschirm (das war Ihnen jetzt bestimmt schon klar) und zwar auch dann, wenn das Gerät nicht entsperrt ist.

Öffnen Sie die Einstellungen, gehen Sie auf „Sicherheit und Standort“ und tippen Sie dann auf das Zahnrad-Symbol hinter „Displaysperre“ und auf „Sperrbildschirmnachricht“. Geben Sie nun eine Nachricht wie „Handy von Max Mustermann, 01234 - 123456789“ ein. Verwenden Sie eine andere Nummer als die Ihres eigenen Handys - schließlich können Sie darauf nicht zugreifen, wenn das Handy weg ist.

Tipp 4: Smart Lock eingrenzen

Mehr Sicherheit ist gut, aber häufig geht sie auch mit einem gewissen Komfortverlust einher. Dem soll die Android-Funktion „Smart Lock“ entgegenwirken. Sie erleichtert das Entsperren des Smartphones beziehungsweise macht es in einigen Situationen sogar ganz überflüssig. Allerdings sind die einzelnen Optionen nach unserer Einschätzung nicht sicher genug:

Bei aktivierter **Trageerkennung** bleibt Ihr Handy entsperrt, so lange es bewegt wird, also zum Beispiel beim Marsch durch die Stadt und beim Workout.



Allerdings kann die Funktion nicht erkennen, ob Sie es sind, mit dem sich das Smartphone bewegt, oder ein Dieb. Legen Sie es auf einen Tisch, dann dauert es ein paar Minuten, bis Smart Lock das Handy verriegelt. Zu viel Zeit für einen neugierigen Kollegen!

Unter **Vertrauenswürdige Orte** können Sie Standorte hinterlegen, an denen sich Ihr Handy automatisch entriegelt, zum Beispiel zu Hause. Ganz ähnlich funktioniert **Vertrauenswürdige Geräte**, dank dem Bluetooth-fähige Geräte wie Laptops und Smartwatches das Android-Handy entsperren.

Das Problem: Legen Sie zum Beispiel Ihr Zuhause als vertrauenswürdigen Ort fest, dann gilt die Einstellung auch in der unmittelbaren Nachbarschaft. Auch die Funkreichweite von Bluetooth schafft häufig unerwünscht große Spielräume. Prüfen Sie deshalb in den Sicherheitseinstellungen von Android, ob eine der Funktionen aktiv ist und schalten Sie sie gegebenenfalls ab.

Tipp 5: Zwei-Faktor-Authentifizierung

Viele Android-Funktionen sind an Ihr Google-Konto gekoppelt. Deshalb trägt es zur Sicherheit Ihres Smartphones bei, wenn Sie das Google-Konto bestmöglich absichern. Dazu gehört die Zwei-Faktor-Authentifizierung. Ist sie aktiv, dann sendet Google bei jedem Anmeldeversuch einen Sicherheitscode an eines Ihrer bereits eingeloggten Geräte. Diesen müssen Sie zusätzlich zu Ihrem Passwort eingeben. So kann sich nicht mehr jeder bei Google anmelden, der Ihre Zugangsdaten erspäht.

Ist kein Gerät mehr eingeloggt, dann erhalten Sie den Code per Anruf auf Ihre bei Google hinterlegte Telefonnummer. Wie Sie die Zwei-Faktor-Authentifizierung einrichten, hat Google für verschiedene Geräte in seiner Online-Hilfe beschrieben.

Tipp 6: Sicheres Surfen

Chrome ist der Standard-Browser von Android. Wenn Sie ihn verwenden, dann sollten Sie überprüfen, ob die Funktion „Safe Browsing“ aktiv ist, die Sie vor gefährlichen Websites schützt.

Öffnen Sie dazu die Einstellungen in Chrome und tippen Sie auf „Synchronisierung und Google-Dienste“. Dann kontrollieren Sie, ob das Häkchen bei „Safe Browsing“ gesetzt ist. Dank „Safe Browsing“ blendet Chrome einen unübersehbaren Warnhinweis ein, wenn Sie eine nach Einschätzung von Google gefährliche Website besuchen oder eine Datei mit einem Schadprogramm herunterladen wollen.

Tipp 7: App-Berechtigungen

Erteilen Sie Apps Zugriffsberechtigungen für den Standort, die Kamera, Fotos und andere Daten auch „einfach so“? Viele Android-Nutzer gucken nicht so genau hin, wenn eine App Berechtigungen anfordert. Dabei sollten sie eigentlich zumindest überprüfen, ob der Zusammenhang zu den App-Funktionen gegeben ist. Warum sollte zum Beispiel die Facebook-App Zugriff auf die Telefonanrufe haben? Glücklicherweise können Sie bereits erteilte App-Berechtigungen in Android sehr leicht korrigieren.

Öffnen Sie dazu die Einstellungen, gehen Sie auf „Datenschutz“ und öffnen Sie den Berechtigungsmanager. Dann gehen Sie die Rubriken wie "Anrufliste", "Dateien und Medien", "Kamera" und "Mikrofon" durch. Werfen Sie jeweils einen Blick auf die Apps und passen Sie die Rechte gegebenenfalls an. Dabei kann es nicht schaden, wenn Sie zu streng sind. Fehlen einer App die notwendigen Rechte, dann wird Sie sie beim nächsten Start schon darauf hinweisen.

Tipp 8: Bildschirmfixierung

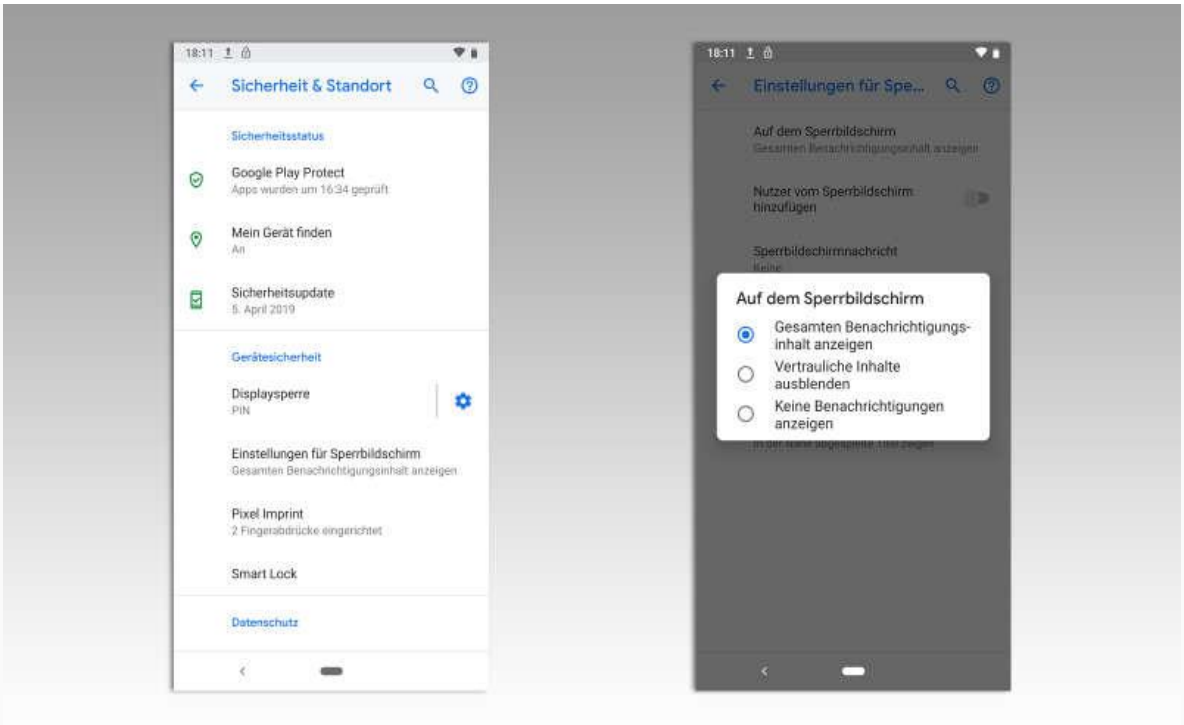
Mit der Bildschirmfixierung können Sie die Nutzung Ihres Handys auf eine einzelne App beschränken. Zum Verlassen ist die Eingabe eines Codes oder Ihres Fingerabdrucks notwendig. Das kann hilfreich sein, wenn Sie Ihr Smartphone einem Freund oder dem Nachwuchs in die Hände geben wollen.

Aktiviert wird die Bildschirmfixierung in den Android-Sicherheitseinstellungen, wo sie sich unter „Erweitert“ versteckt. Anschließend können Sie Apps über die App-Übersicht fixieren. Tippen Sie dazu in der Übersicht auf das App-Icon und gehen anschließend auf „Fixieren“.

In älteren Android-Versionen starten Sie ebenfalls mit der App-Übersicht. Dort erscheint ein Stecknadel-Symbol auf jeder App, das Sie antippen, um die jeweilige App zu fixieren.

Tipp 9: Sperrbildschirm

Ab Werk zeigt Android viele Infos auf dem Sperrbildschirm an, d.h. bei verriegeltem Gerät. Dazu können möglicherweise auch vertrauliche Nachrichten gehören.



Um das zu verhindern öffnen Sie in den Einstellungen "Apps & Benachrichtigungen". Dann tippen Sie unten auf "Benachrichtigungen". Auf der folgenden Seite finden Sie ziemlich weit unten die Rubrik "Benachr. auf Sperrbildschirm". Hier können Sie festlegen in welchem Umfang Ihr Handy Infos anzeigen darf.

Tipp 10: Sperren aktivieren

Die Funktion „Sperren“ verriegelt das Handy so, dass Sie es nur noch per PIN, Passwort oder Muster entsperren können. Entsperren per Fingerabdruck oder „Smart Lock“ ist im Sperren-Modus nicht mehr möglich. So verhindert "Sperren" unter anderem, dass ein möglicherweise unter Gewaltanwendung auf den Sensor gepresster Finger das Handy entsperrt. Zusätzlich erscheinen keine Nachrichten-Inhalte mehr auf dem Sperrbildschirm. Auch per Neustart des Smartphones lässt sich Sperren nicht umgehen.

"Sperren" müssen Sie als Funktion freischalten, bevor Sie es verwenden können. Aktivieren Sie dazu in den Einstellungen unter „Display > Sperrbildschirm“ die Option „Option zum Sperren anzeigen“. Dann können Sie Sperren aktivieren, indem Sie die Ein-Aus-Taste Ihres Handys gedrückt halten. Es erscheint ein kleines Menü, in dem Sie auf „Sperren“ tippen.