

Sicherheitseinstellungen für Smartphones

Android

Inhaltsverzeichnis

Schutz vor unbefugtem Zugriff auf das Gerät	3
System-Updates des Geräteherstellers	8
Synchronisierung & Backups	9
Datenschutzeinstellungen für Apps einrichten	10
Virens Scanner	14
Jailbreak, Root und gesperrte Smartphones	14
Kostenfalle In-App-Käufe	15
Kostenfalle Datentarife	16
WLAN, Bluetooth und mobile Hotspots	18
Datenverschlüsselung	20
Verkaufen, Verschenken & Verborgnen	20
Smartphone-Finder: finden oder sperren	21
Das kindersichere Smartphone	22

Hinweis: Je nach Hersteller Ihres Android-Geräts können die genauen Bezeichnungen für einzelne Einstellungen bzw. deren Positionen im Menü unter Umständen von den Darstellungen in diesem Leitfaden abweichen. Die Funktionen sind allerdings bei den meisten Geräten vorhanden. Konsultieren Sie im Zweifelsfall die Dokumentation des Herstellers.

Impressum:

ISPA – Internet Service Providers Austria, Währinger Straße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft

6. aktualisierte Auflage
Wien, 2020

Redaktion: Birgit Mühl & Jonas Müller

Endgerät: Google Pixel 3 XL

Betriebssystem: Android 9

Android, Google Play und Google Pixel sind eingetragene Marken von Google Inc., USA

Gefördert durch die Europäische Union – Safer Internet Projekt. Alle Angaben erfolgen ohne Gewähr. Eine Haftung der Autorinnen und Autoren, durch die ISPA, das Projekt Saferinternet.at oder die Europäische Union ist ausgeschlossen.

Diese Broschüre wurde in Kooperation mit der Arbeiterkammer Niederösterreich im Rahmen ihrer Digitalisierungsinitiative umgesetzt. Die Arbeiterkammer macht Arbeitnehmerinnen und Arbeitnehmer fit für die digitale Zukunft. Infos unter noe.arbeiterkammer.at/zukunftsprogramm. Eine Haftung durch die Arbeiterkammer Niederösterreich ist ausgeschlossen.

Ein Smartphone ist ein praktischer Begleiter und aus dem Alltag nicht mehr wegzudenken. Knapp 90 Prozent der Bevölkerung in Österreich verwenden bereits ein Smartphone und konsumieren darüber Medien und Informationen, nutzen soziale Netzwerke, recherchieren zu Produkten und Dienstleistungen, machen Preisvergleiche oder erledigen ihre Einkäufe. Doch nicht alle Nutzerinnen und Nutzer sind Profis, weshalb sie Unterstützung benötigen. Damit Sie Ihr Smartphone sicher einsetzen können, sollten Sie einige Dinge beachten. Dieser Ratgeber hilft Ihnen mit Tipps und Schritt-für-Schritt-Anleitungen grundlegende Sicherheitseinstellungen an Ihrem Smartphone vorzunehmen.

Schutz vor unbefugtem Zugriff auf das Gerät

Es gibt verschiedene Möglichkeiten sein Smartphone vor unbefugtem Zugriff z. B. bei Verlust oder Diebstahl zu schützen. Die meisten Smartphones bieten zwei Sicherheitsfunktionen an: einmal die PIN-Abfrage beim Einschalten des Gerätes (SIM-Kartensperre oder PIN-Eingabe) und als zusätzliche Option die Passwortabfrage bei der Aufhebung des Ruhezustandes (Bildschirmsperre).

SIM-Karte schützen

Die SIM-PIN-Abfrage schützt aktiv vor missbräuchlicher Verwendung der SIM-Karte und sollte keinesfalls aus Bequemlichkeit ausgeschaltet werden. Im Falle von Verlust oder Diebstahl kann diese Bequemlichkeit unangenehme und teure Konsequenzen haben. Denn die SIM-Karten verbleiben im Normalfall im Eigentum der Netzbetreiber und werden den Kundinnen und Kunden nur zur Verfügung gestellt. Diese verpflichten sich, die SIM-Karte vor schädlichen Einflüssen und Missbrauch durch Dritte zu schützen. Die Endnutzerinnen und -nutzer haften deshalb auch bis zur Sperrmeldung an den Netzbetreiber für fast alle Entgeltforderungen, die sich auf Missbrauch der SIM-Karte und das Verschulden der Teilnehmerin oder des Teilnehmers zurückführen lassen, z. B. eben auch durch das Deaktivieren des SIM-PINs. Nähere Informationen finden Sie dazu in den allgemeinen Geschäftsbedingungen Ihres Netzbetreibers.

Bildschirmsperre einrichten

Es ist ratsam, zusätzlich zur SIM-Kartensperre auch eine Bildschirmsperre zu verwenden. Es erscheint zwar zeitaufwendig, jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz des Smartphones bzw. der Daten bei. Je nach Nutzungsgewohnheiten kann die Sperrzeit individuell festgelegt werden – von einer automatischen Bildschirmsperre nach wenigen Sekunden bis hin zu mehreren Minuten.

Jedoch sollte darauf Acht gegeben werden, dass die Eingabe des Entsperrmusters oder – codes unauffällig erfolgt. Viele Sicherheitsangriffe sind überraschend trivial, eine weit verbreitete Methode des Hackings ist das Abschauen oder Abfotografieren von Zugangsdaten und Passwörtern bei deren Eingabe (»Visual Hacking«). Besonders auf öffentlichen Plätzen, in dicht gedrängten Verkehrsmitteln oder bei neugierigen Sitznachbarinnen und Sitznachbarn im Flugzeug sollten Nutzerinnen und Nutzer vorsorglich achtsam sein.

Bei der Bildschirmsperre von Android-Smartphones gibt es für gewöhnlich mehrere Möglichkeiten:

- **PIN-Eingabe**
- **Musterentsperrung**
- **Passwort-Eingabe**
- **Optional: Fingerabdruckscanner**
- **Optional: Smart Lock**

Schutz vor unbefugtem Zugriff auf das Gerät

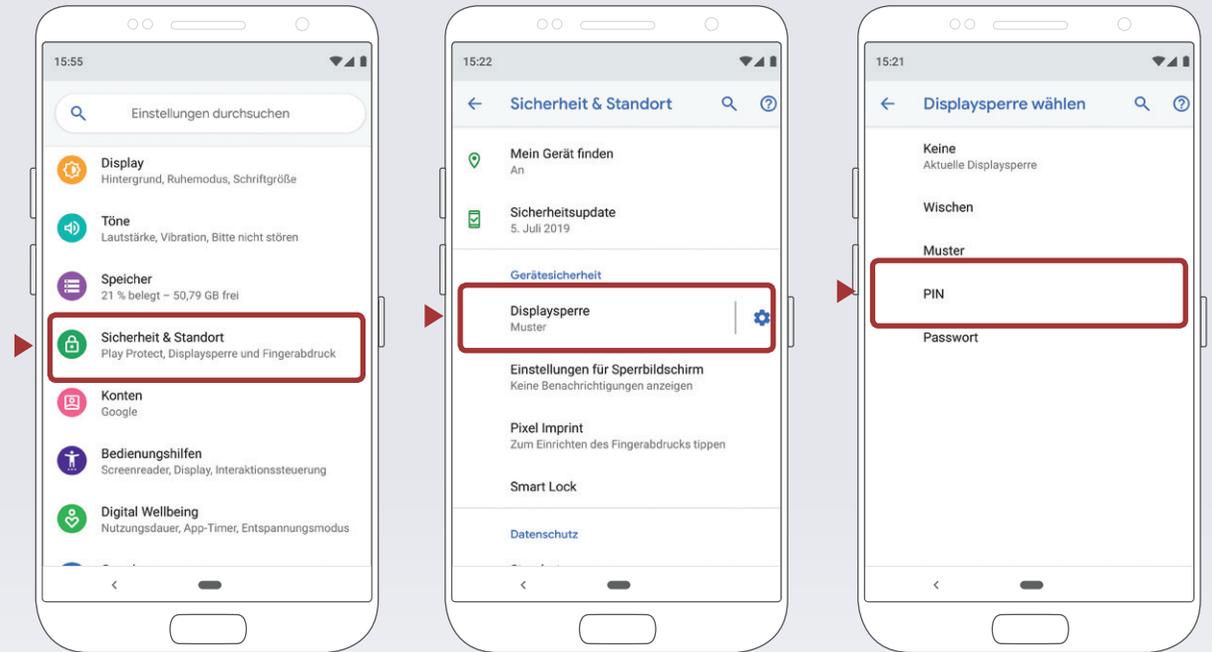
Bildschirm-Sperre bei Android-Smartphones einrichten

Einstellungen ▶ **Sicherheit & Standort** ▶ **Displaysperre**

Die PIN-Eingabe ist der Klassiker beim Passwortschutz. Je nach Schwierigkeitsgrad der Zahlenkombination bietet sie mittlere bis hohe Sicherheit. Die Pin sollte aus mindestens 4 Stellen und nicht mehr als 17 Stellen bestehen. Geburtstage oder 1234 als Zahlenkombination sollten vermieden werden, da diese leicht zu erraten sind. Die Passwordeingabe weist die höchste Sicherheitsstufe auf, besonders wenn eine Zahlen-, Buchstaben- und Sonderzeichenkombination verwendet wird. Um »komplizierte« Passwörter nicht zu vergessen, bieten sich die Anfangsbuchstaben eines einprägsamen Merksatzes an. Beispielsweise ergäbe sich das Passwort »ImÄ&b197og« aus dem Merksatz »Ich mag Äpfel & bin 1970 geboren«.

WICHTIG

Das gleiche Passwort sollte bei anderen Diensten nicht nochmals verwendet werden, da man es so potenziellen Angreifern einfach macht, mit nur einem Passwort auf mehrere Konten zuzugreifen.



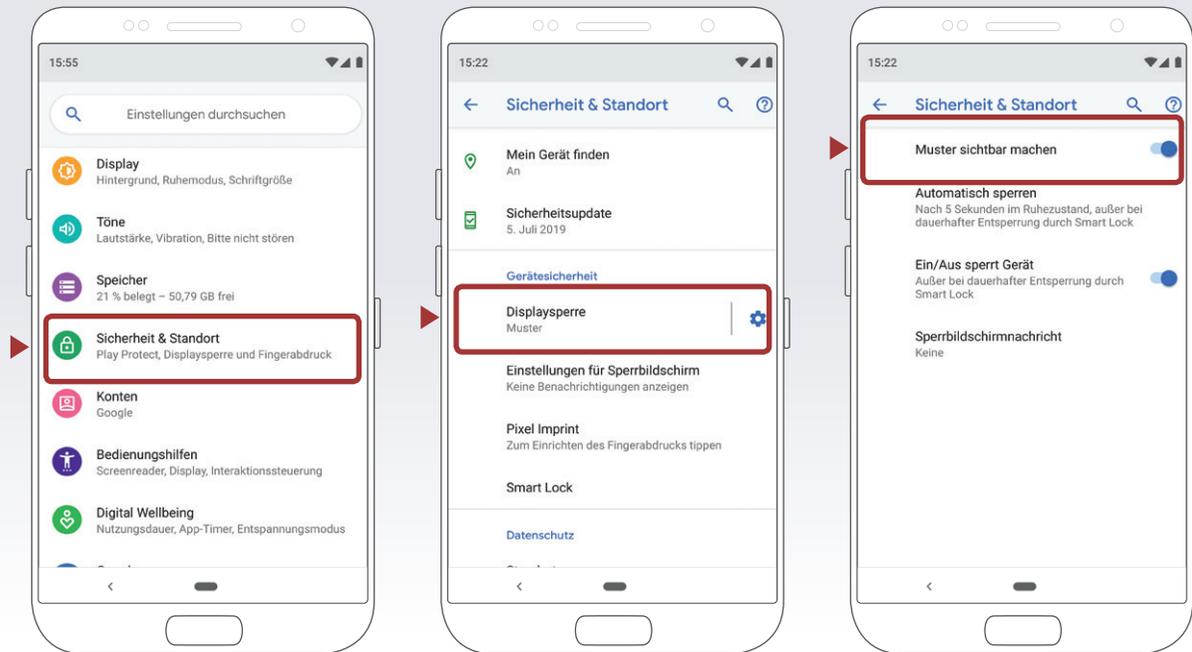
Schutz vor unbefugtem Zugriff auf das Gerät

Muster bei Mustersperre unsichtbar machen

Einstellungen > Sicherheit & Standort > Displaysperre Einstellungen >

Muster sichtbar machen deaktivieren

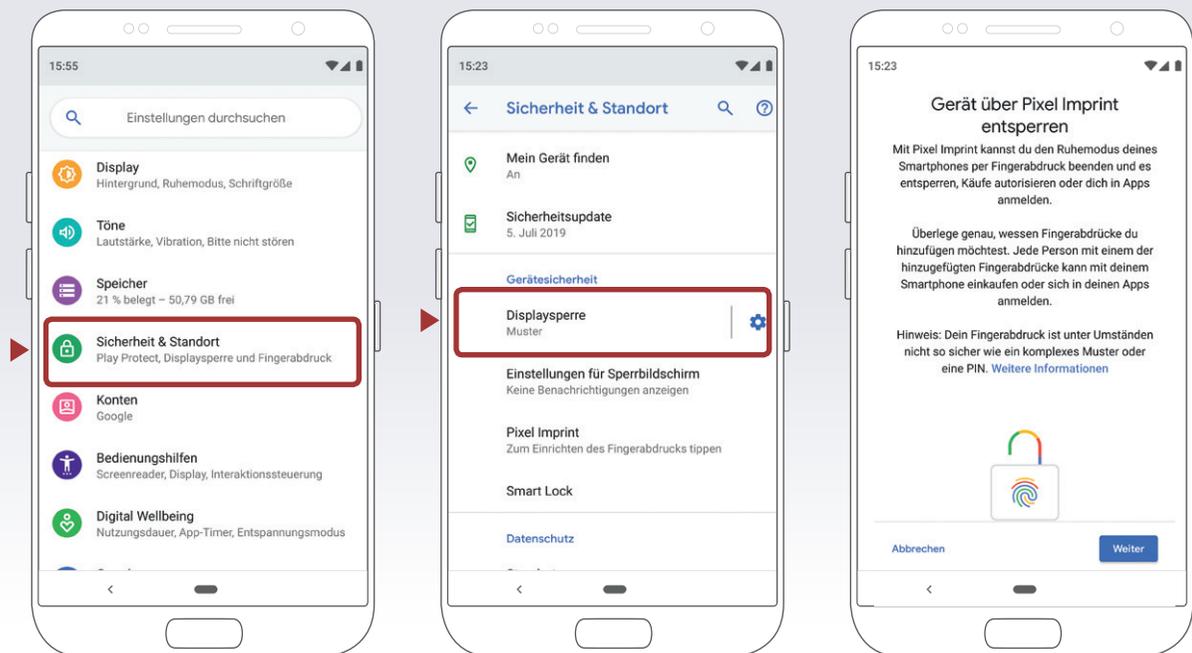
Die Mustersperre ist eine sehr beliebte Methode zum Schutz des Endgerätes, jedoch mit mittlerer Sicherheit, da diese leicht beobachtet oder nachvollzogen werden kann. Das Muster wird meistens auf einer 3 x 3-Punkte-Matrix als Verbindungslinie von mindestens vier Punkten festgelegt. Zum Entsperren muss auf dem Touch-Display die vorher festgelegte Linie nachgefahren werden. Einige Smartphones bieten zusätzlich die Möglichkeit, das Muster beim Entsperren des Smartphones nicht sichtbar zu machen (die Verbindungslinien nicht anzuzeigen). Diese Einstellung sollte unbedingt gewählt werden, da sie es für Fremde erschwert, das Muster zu erkennen.



Fingerabdruckscanner einrichten

Einstellungen > Sicherheit & Standort > Pixel Imprint

Viele Smartphones bieten auch einen Fingerabdruck-Scanner an, der allerdings auch keinen absoluten Schutz bietet. Um diese Art der Entsperung nutzen zu können, muss vorab eine andere Displaysperre eingerichtet werden. Dies ist notwendig, sollte der Fingerabdruck einmal nicht erkannt werden.



Schutz vor unbefugtem Zugriff auf das Gerät

Gesichtserkennung oder Smart Lock einrichten

Einstellungen ▶ **Sicherheit & Standort** ▶ **Smart Lock**

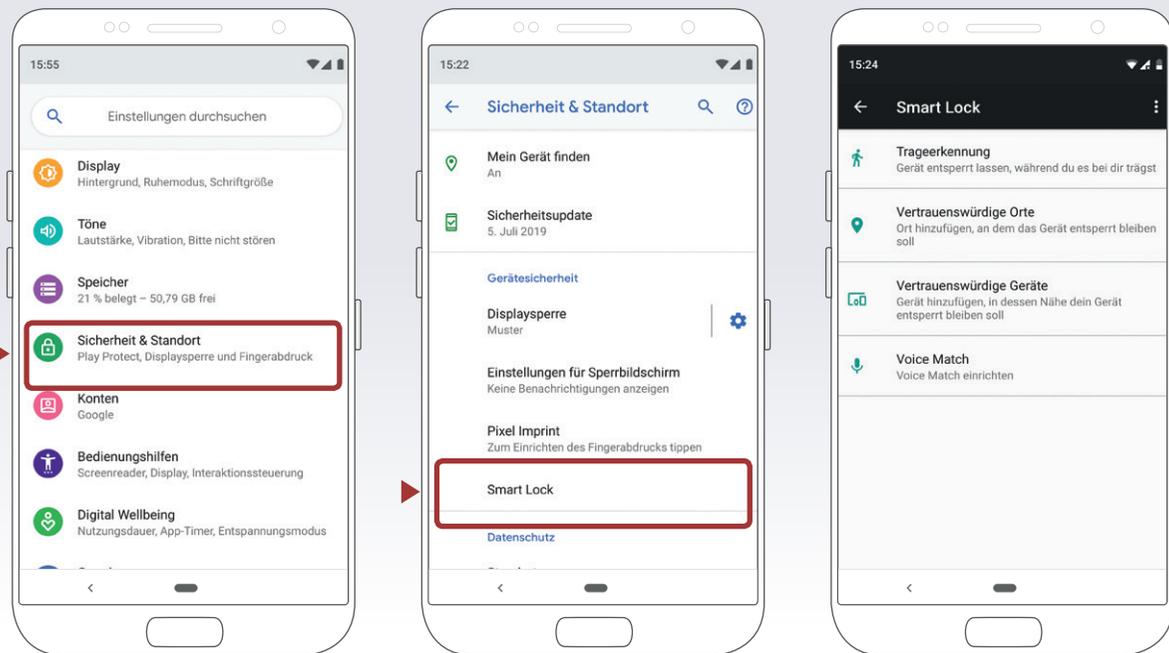
Die Gesichtserkennung (Face Unlock) hat die niedrigste Sicherheitsstufe, denn jemand der einem ähnlich schaut, könnte das Smartphone entsperren. Hierbei scannt das Smartphone das Gesicht, ein Blick in die (eingeschaltete) Kamera reicht aus. In der Praxis können aber beispielsweise schlechte Lichtverhältnisse rasch zu einer Nicht-Erkennung und somit zu keiner Entsperrung führen. Bei dieser Art der Bildschirmsperre wird daher zusätzlich auch ein PIN-Code verwendet, damit bei Nicht-Erkennung das Gerät zumindest per PIN entsperrt werden kann. Mittlerweile gibt es bei Face Unlock erweiterte Einstellungen, mit denen zusätzliche Aufnahmen getätigt werden können, um diese Funktion zuverlässiger zu machen. Vorsicht ist bei älteren Versionen der Gesichtserkennung, bei denen das Gerät mit einem Foto der berechtigten Person entsperrt werden könnte, geboten. Neuere Systeme verwenden deshalb zusätzliche Sicherheitsmaßnahmen wie z. B. Iris-Scanner, bzw. analysieren minimale Bewegungen.

Auf dem für diese Broschüre verwendeten Testgerät steht diese Funktion nicht zur Verfügung.

Unter dem Stichwort ›Smart Lock‹ stehen auch noch andere Entsperrfunktionen zur Verfügung:

- **Trageerkennung**
- **Vertrauenswürdige Orte**
- **Vertrauenswürdige Geräte**
- **Voice Match**

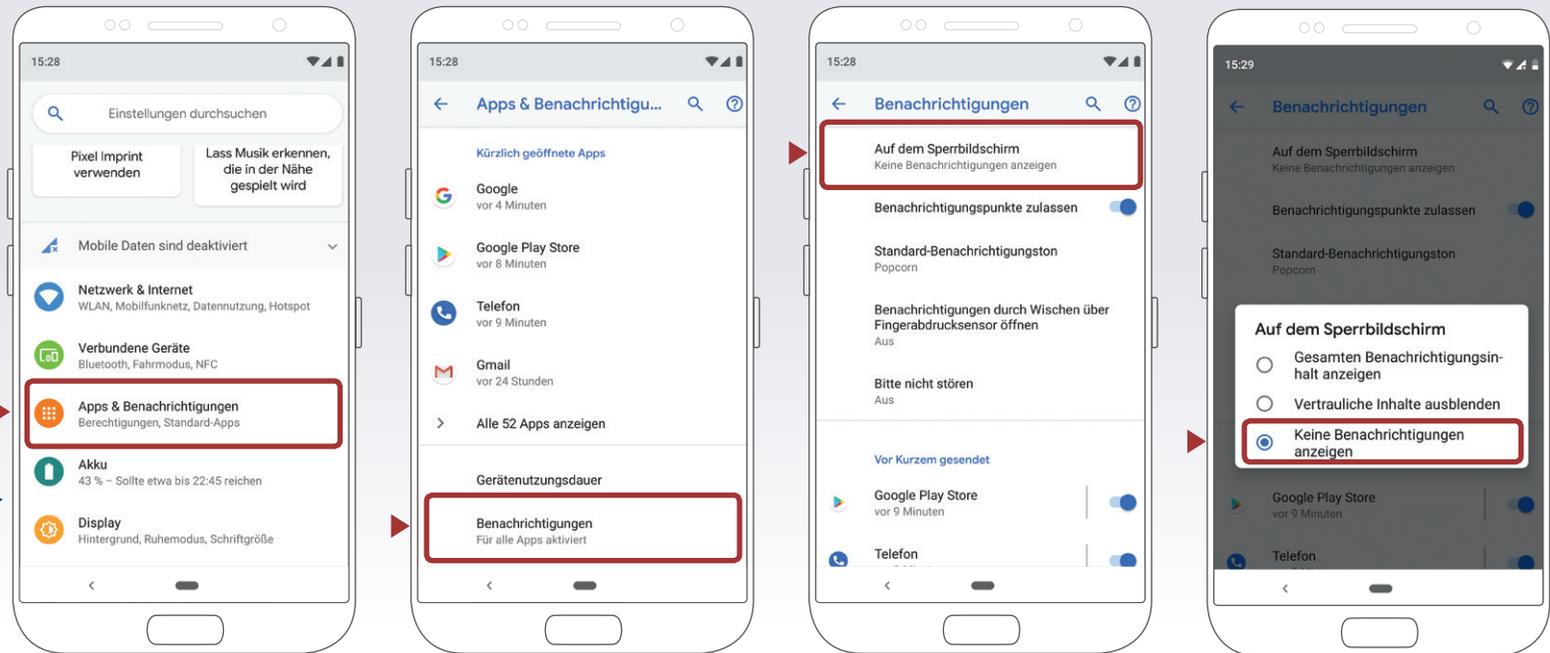
Diese Entsperrfunktionen sind zwar durchaus praktisch, man sollte jedoch auch die Sicherheitsrisiken dabei nicht vergessen. Nur weil sich das Gerät an einem vertrauenswürdigen Ort befindet, heißt das nicht, dass alle Personen, die sich dort aufhalten, vertrauenswürdig sind und Zugriff auf mein Gerät bekommen sollen.



Benachrichtigungen auf dem Sperrbildschirm

Es gibt die Möglichkeit, dass Benachrichtigungen z. B. von Messenger-Services direkt am Sperrbildschirm angezeigt werden. Wer sensible Inhalte von Nachrichten lieber erst nach Eingabe der gewählten Entsperrmöglichkeit angezeigt bekommt, kann dies in den Einstellungen bearbeiten.

- Einstellungen** → **Apps & Benachrichtigungen** →
- Benachrichtigungen** → **Auf dem Sperrbildschirm** →
- Keine Benachrichtigungen anzeigen bzw.**
- Vertrauliche Inhalte ausblenden**



System-Updates des Geräteherstellers

Die vom Hersteller empfohlenen System-Updates sollten unbedingt durchgeführt werden, denn Updates enthalten kleine Systemverbesserungen: Sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-) Problem bei einem ihrer Produkte erlangen, großes Interesse, umgehend zu reagieren, und versuchen schnell eine Lösung des Problems zu erarbeiten. Die meisten Smartphones haben eine Funktion, die automatisch auf System-Aktualisierungen überprüft. Es ist empfehlenswert, Software-Updates möglichst zeitnah nach deren Veröffentlichung

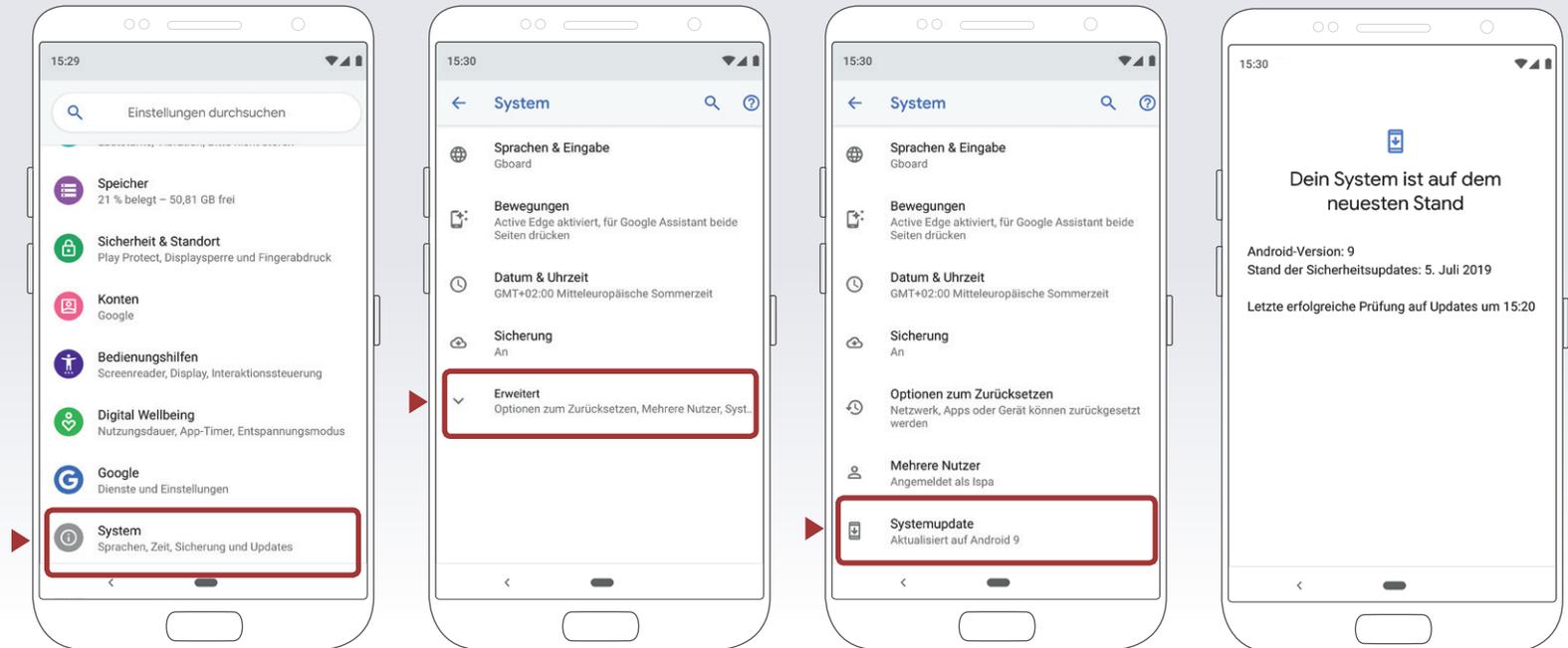
durchzuführen. Sicherheitslücken sind sehr gut dokumentiert und können von unbefugten Personen für eigene Angriffe schnell ausgenutzt werden.

TIPP

Achten Sie schon beim Kauf auf etwaige Update-Garantien des Anbieters

Software-Updates

Einstellungen → System → Erweitert
Systemupdates

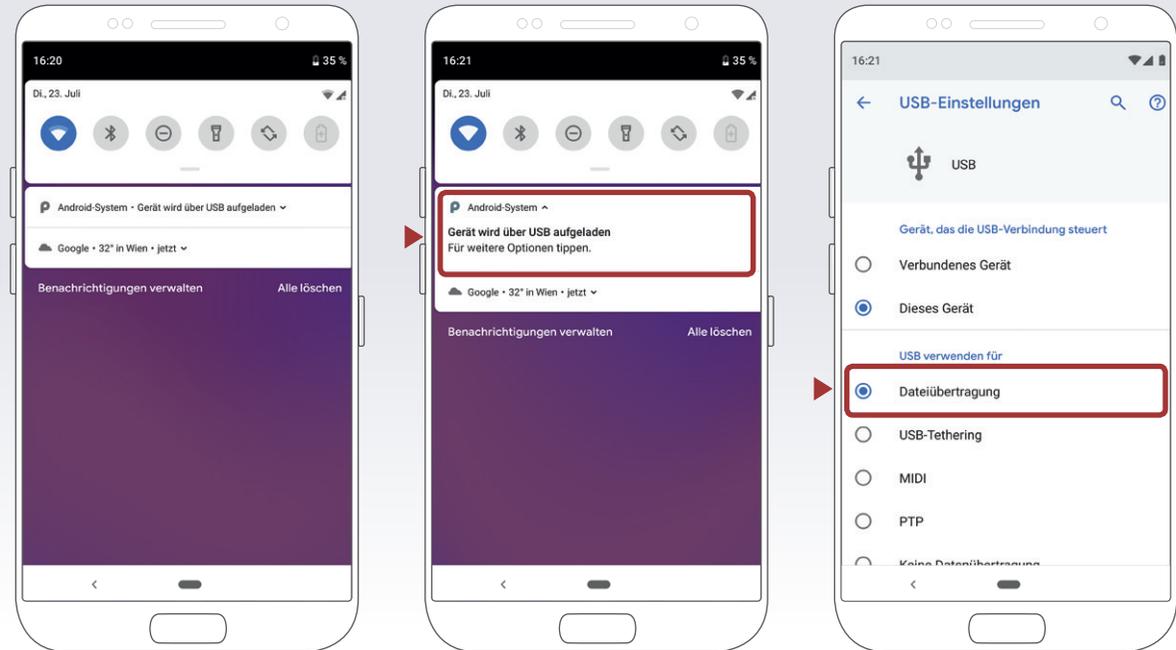


Daten von Smartphone auf PC übertragen

(Verbinden Sie vorher das Smartphone per USB-Kabel mit dem PC.)

Benachrichtigungen ► Gerät wird über USB aufgeladen (Für weitere Optionen tippen) ►
Dateien übertragen

Genau wie bei einem Laptop oder PC ist es bei einem Smartphone sinnvoll, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Verlusts kann so auf das Backup zurückgegriffen werden. Somit ist zumindest der letzte Stand der gesicherten Daten verfügbar.



Datensicherung über die Google-Cloud

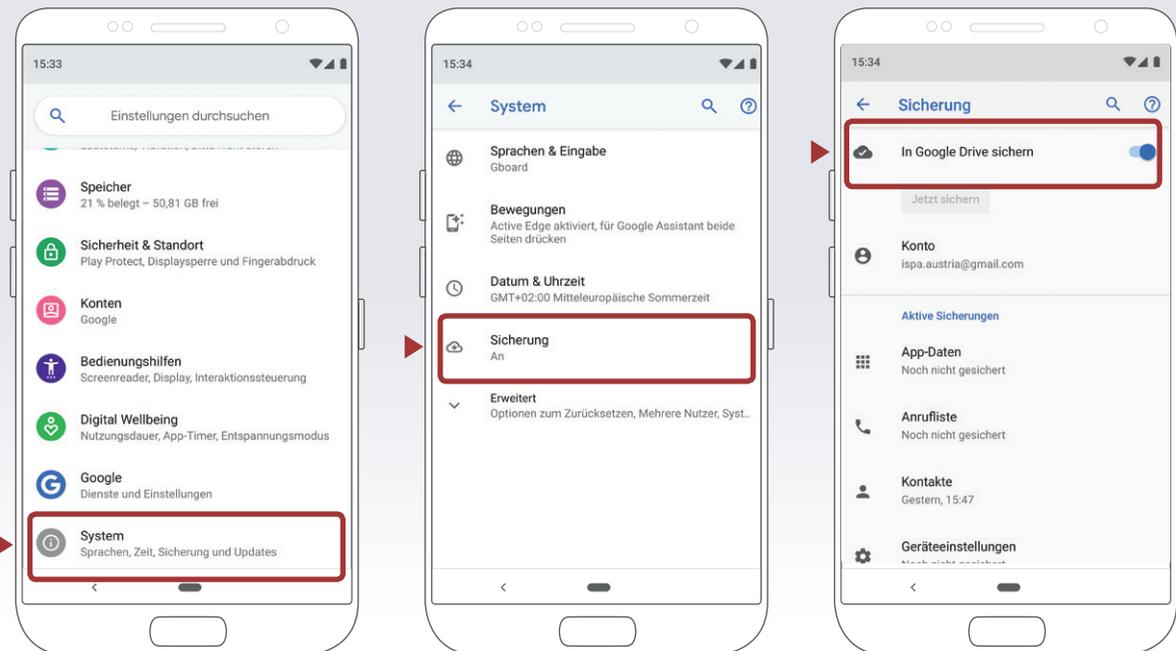
Einstellungen ► System ► Sicherung ► In Google Drive sichern (EIN)

2 Faktor Authentifizierung

Um die Daten möglichst sicher abzuspeichern, ist es sinnvoll für Konten wie das Google-Konto eine 2 Faktor Authentifizierung zu verwenden, auch Bestätigung in zwei Schritten genannt. Sie ist eine weitere Sicherheitsmaßnahme, die missbräuchlichen Zugriff auf das Konto verhindert. Nach erfolgter Einrichtung sind zwei Schritte nötig, um sich beim Konto anzumelden. Für ein erfolgreiches Login, braucht man ...

1. ... etwas, das man weiß ► Passwort
2. ... etwas, das man hat ► Smartphone bzw. PIN, Token, Fingerprint etc.

Durch die zusätzliche Sicherheitsebene wird das jeweilige Konto, auf welchem Kontaktdaten, Emails, Fotos und viele weitere persönliche Daten gespeichert sind, besser abgesichert.



Datenschutzeinstellungen für Apps einrichten

Ein Smartphone ohne Apps ist wie Winter ohne Schnee. Jedoch können die kleinen Anwendungen genutzt werden, um in Smartphones und somit auch an sensible Daten zu gelangen: Solche schädlichen Apps heißen »Malware«. Ebenso gibt es aber auch Apps, die über Hintertüren oder (zu) viele Zugriffsberechtigungen Schindluder treiben können. Wenn beim Kauf und Download von Apps ein paar Punkte beachtet werden, kann das Sicherheitsrisiko jedoch minimiert werden.

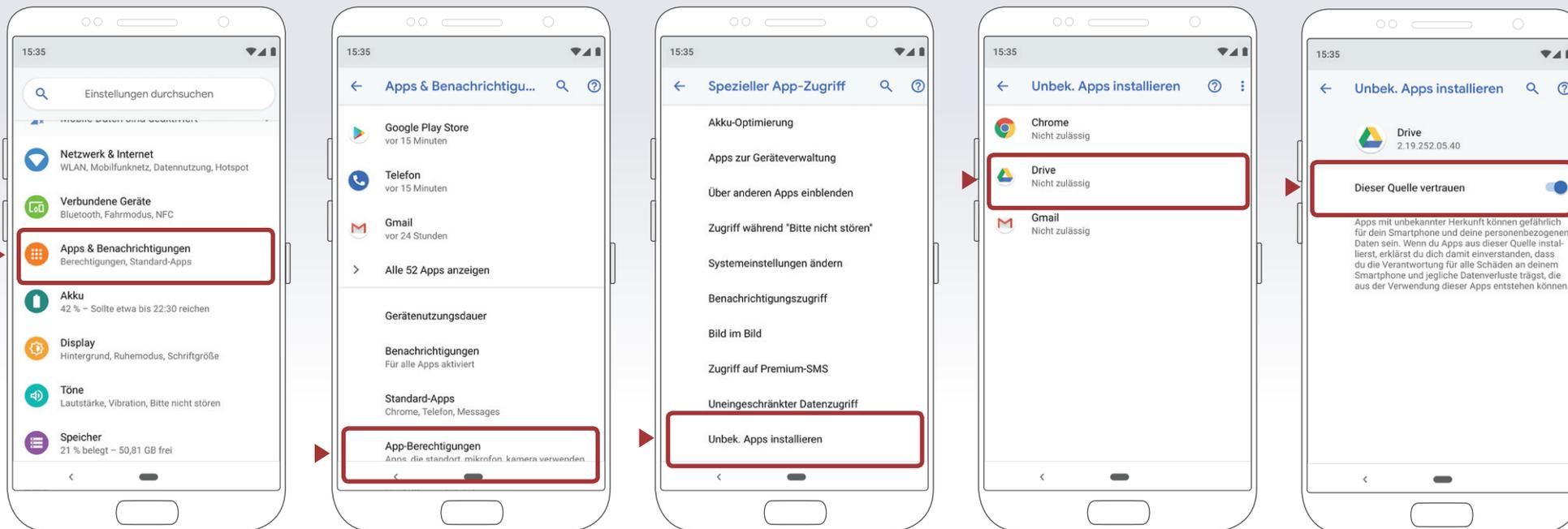
Apps nur aus den offiziellen App-Stores beziehen

Natürlich kann es auch hier keine endgültige Garantie geben, aber der offizielle Store von Android, der Play Store (play.google.com), ist definitiv vertrauenswürdiger als andere Quellen. Um im Play Store aufgenommen zu werden, müssen Apps gewisse Anforderungen erfüllen. Sie werden auch regelmäßig durch Google Play Protect überprüft und auf Schadsoftware gescannt.

Bei Android können Apps auch aus anderen und somit fremden Quellen bezogen werden. Diese Möglichkeit der Installation von fremden, also Nicht-Play-Store-Anwendungen, ist per Standardeinstellung deaktiviert und muss erst erlaubt werden.

Sperre fremder Apps aus anderen Quellen als dem Play Store aufheben

Einstellungen → Apps & Benachrichtigungen → Erweitert → Spezieller App-Zugriff → Unbek. Apps installieren → auf Quelle klicken → Dieser Quelle vertrauen aktivieren



Datenschutzeinstellungen für Apps einrichten

Rückgaberecht für Apps

Beim Google Play Store kann eine App derzeit innerhalb von zwei Stunden ab dem Erwerb problemlos und unbürokratisch zurückgegeben werden. Hierfür müssen Nutzerinnen und Nutzer im Google Play Store unter dem Menüpunkt ›Konto‹ und ›Bestellverlauf‹ die entsprechende App auswählen und anschließend auf ›Erstattung‹ klicken.

Bis 48 Stunden nach erfolgter Installation kann aktuell im Play Store via Browser auf play.google.com unter Bestellverlauf eine Erstattung des App-Kaufs beantragt werden, dies gilt auch für In-App-Käufe. Danach ist nur noch eine De-Installation der App möglich.

Datenschutz bei Google

Auf myactivity.google.com und myaccount.google.com können Standortverläufe, Spracheingaben, Suchmaschinenabfragen oder Youtube-Historie des jeweiligen Kontos, das mit dem Endgeräts verbunden ist, abgefragt werden, da Google dies standardmäßig protokolliert. Die Speichereinstellungen können hier geändert werden.

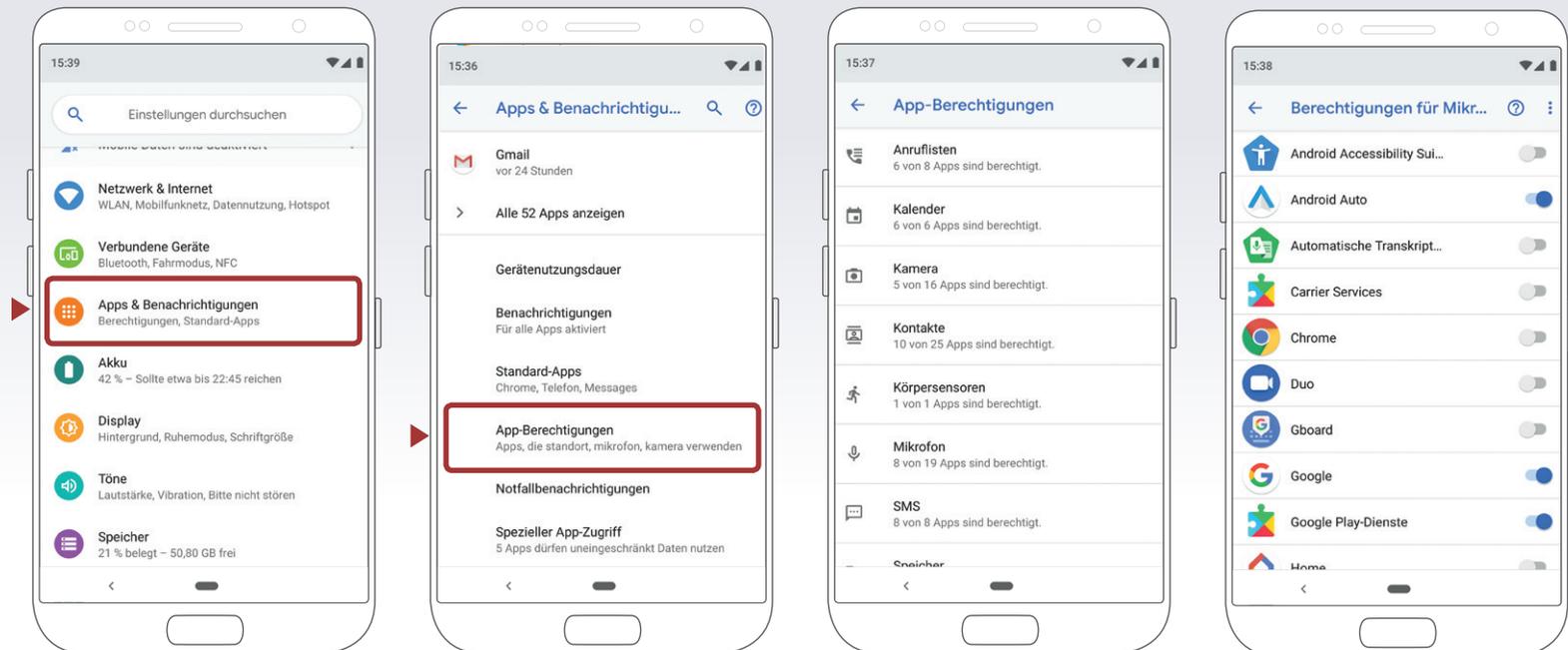
App-Berechtigungen

Vor der endgültigen Installation einer App oder bei erstmaligem Zugriff auf bestimmte Funktionen wie Standort oder Kontakte muss deren Zugriffsberechtigungen zugestimmt werden. Hier sollten Nutzerinnen und Nutzer vorsichtig sein und nur dann zustimmen, wenn diese Zugriffsrechte notwendig erscheinen. Bösartige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen, die einerseits nicht notwendig sind und andererseits das Smartphone und die Daten angreifbar machen.

Nutzerinnen und Nutzer sollten bewusst auswählen, welche Daten sie welcher App zur Verfügung stellen wollen. Handelt es sich zum Beispiel um eine Spiele-App, braucht diese eher keinen Zugriff auf das Telefonbuch; dass eine Navigations-App Zugriff auf die GPS-Daten benötigt, macht wiederum Sinn. Nutzerinnen und Nutzer sollten sich hier die Frage stellen, warum sie einer App Zugriff zu Daten gestatten sollten, für deren Beauskunftung staatliche Einrichtungen in der Regel eine richterliche Anordnung benötigen.

App-Berechtigungen verwalten

Einstellungen → App-Berechtigungen → Berechtigungsart auswählen (z. B. Mikrophon) → nicht benötigte Berechtigung abwählen



Datenschutzeinstellungen für Apps einrichten

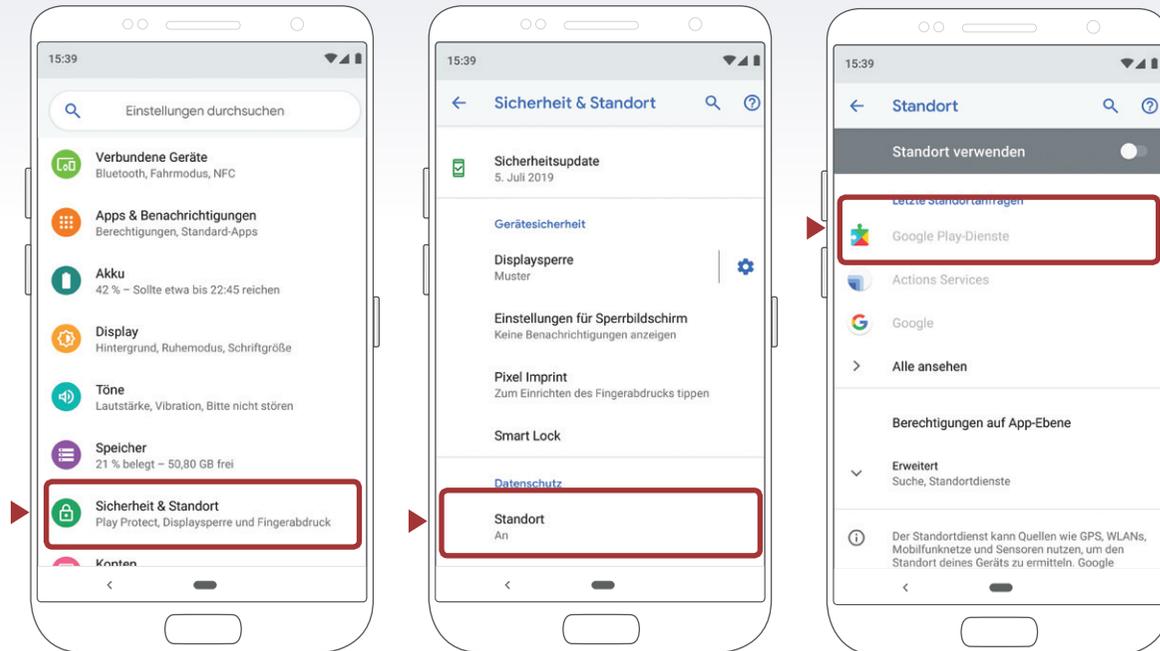
Berechtigungen bei Updates

Nicht nur bei der Neu-Installation sollte auf die Berechtigungen geachtet werden, auch ungeprüfte App-Updates können Überraschungen beinhalten. Für das Berechtigungsmanagement wurden bei Android Berechtigungsgruppen wie Kamera, Kontakte, Standort

usw. mit jeweilig untergeordneten Funktionen wie z. B. genauer Standort, ungefährer Standort, usw. angelegt. Bei einem Update einer App können in jenen Gruppen, die bei der Installation bereits akzeptiert wurden, zusätzliche Funktionen hinzugefügt werden. Daher sollten App-Updates nicht ungeprüft installiert werden.

Deaktivierung von GPS-Daten-Übermittlung

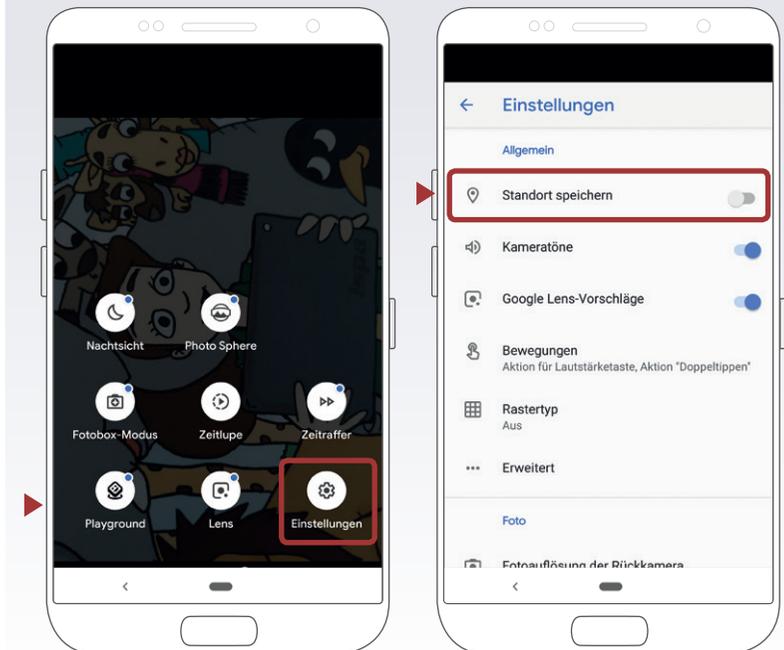
Einstellungen > Sicherheit & Standort > Standort verwenden



Deaktivierung des Geo-Taggings bei Fotos

Kamera > Einstellungen > Standort speichern abwählen

Achtung: Bei einigen Smartphones reicht es aber nicht, lediglich die allgemeine Positions-Daten-Übermittlung zu deaktivieren. Auch wenn die allgemeine Positions-Daten-Übermittlung abgedreht ist, kann es dennoch sein, dass weiterhin der eigene Aufenthaltsort bekannt gegeben wird: und zwar beim Aufnehmen und Versenden von Fotos (>Geo-Tagging<). Ein Geo-Tag ist das automatische Einbetten des Standorts zum Zeitpunkt der Aufnahme in die Fotodatei.

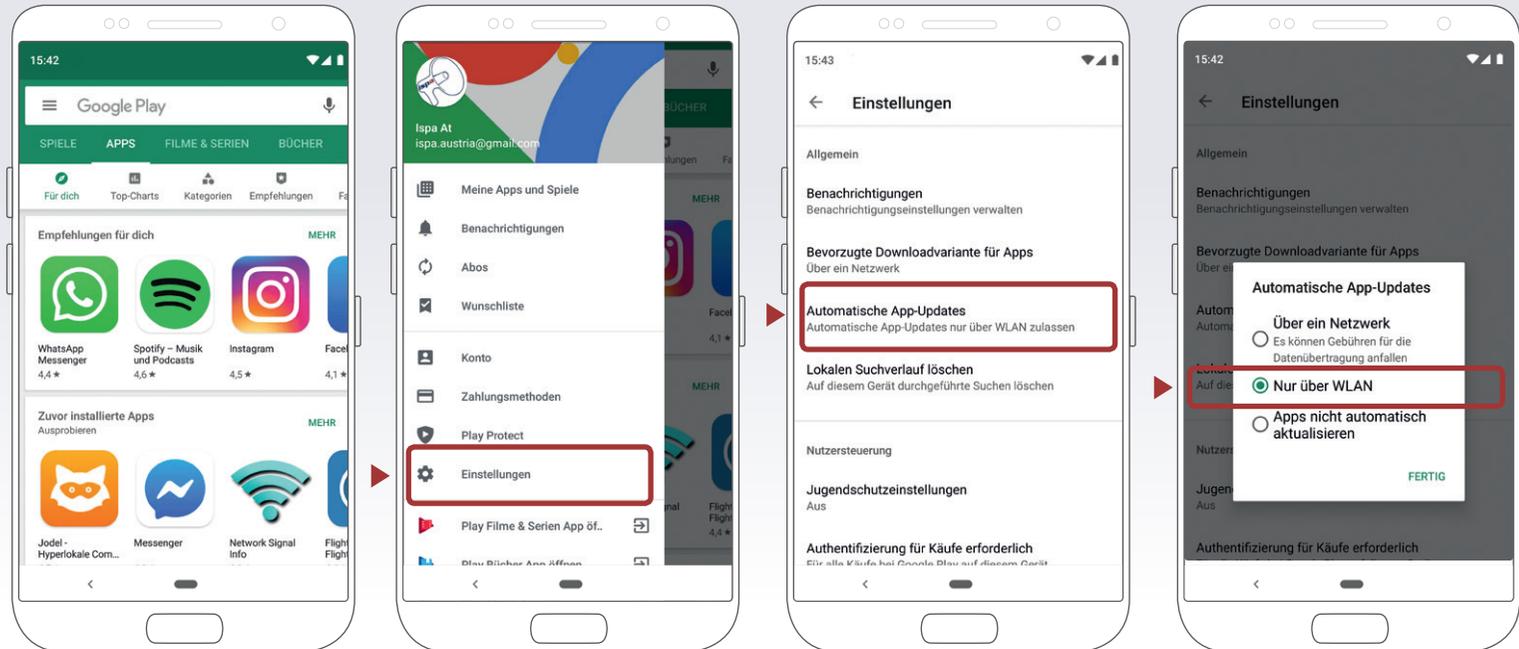


Datenschutzeinstellungen für Apps einrichten

Sichere App Aktualisierung

Google Playstore → nach rechts swipen → Einstellungen → Automatische App-Updates → Nur über WLAN auswählen

Werden App- Updates angeboten, kann es durchaus sein, dass weitere oder neue Nutzungsrechte von der App verlangt werden. Es empfiehlt sich daher auch bei Updates auf neue Zugriffsrechte zu achten und diese wiederum nach deren Sinnhaftigkeit oder Notwendigkeit zu hinterfragen. Möchten Nutzerinnen und Nutzer nicht manuell nach neuen App-Updates suchen müssen, kann die »Benachrichtigungsfunktion« aktiviert werden. Diese informiert, wenn ein neues Update bereitsteht. Entscheiden sich Nutzerinnen und Nutzer für die automatische Aktualisierung, sollte die Funktion »nur über WLAN« aktiviert werden; ansonsten können solche Hintergrundaktualisierungen das eigene Datenvolumen strapazieren und im schlimmsten Fall Zusatzkosten verursachen.



Virens Scanner

Wenn das Smartphone intensiv genutzt wird, viele Apps heruntergeladen oder auch Online-Banking verwendet werden, sollten Nutzerinnen und Nutzer die Anschaffung einer Sicherheits-App andenken.

Virenschutzprogramme durchsuchen das Smartphone nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren und beseitigen diese wenn möglich. Bei Android kann aus dem großen Pool der angebotenen Virenschutzprogramme gewählt werden (z. B. die

kostenlose Sophos Mobile Security App oder die Sophos Security & Antivirus Guard App). Speziell beim Kauf eines Virens scanners empfiehlt es sich natürlich, besonders aufmerksam und auf die persönlichen Bedürfnisse abgestimmt auszuwählen. Eine Virenschutz-App ist ein guter Ansatz für mehr Sicherheit, aber auch kein Patentrezept.

WEB-TIPP

Auf av-test.org finden Sie Testberichte zu vielen gängigen Virenschutzprogrammen.

Jailbreak, Root und gesperrte Smartphones

»Jailbreaking« ist das inoffizielle Entsperrn von Software und Hardware, meint in den meisten Fällen aber das Entsperrn von Smartphones. Das Gegenstück zum Jailbreak bei Apple ist das »Rooten« bei Android: Ein »Root« ist vergleichbar mit einem Administrator-Konto, welches volle Zugriffs- und Schreibrechte hat und über welches somit das gesamte System verändert werden kann.

ACHTUNG

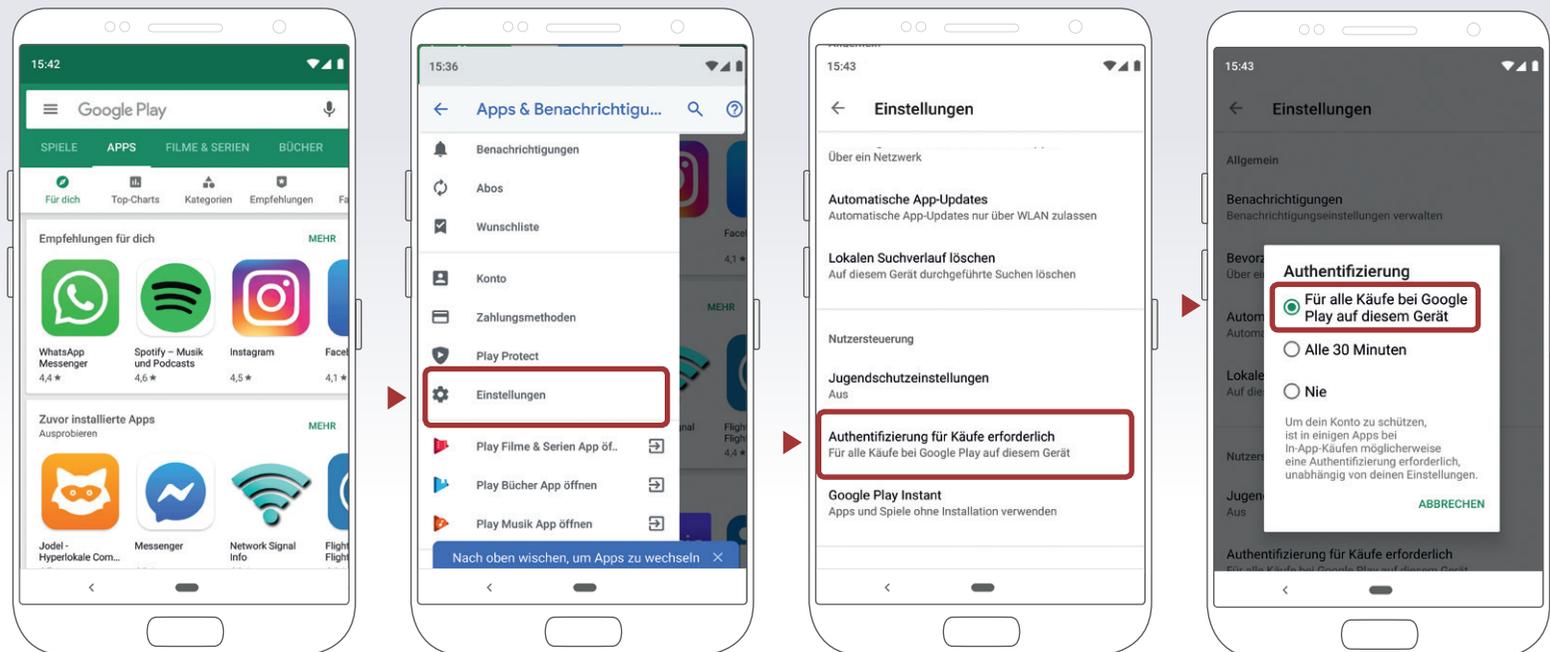
Durch den Jailbreak und das Rooten können die Betriebssysteme der Smartphones beeinträchtigt oder sogar beschädigt werden. Ebenso können nach dem Jailbreak und dem Rooten Software-Updates des Geräteherstellers nicht mehr so einfach eingespielt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Jailbreak-Programmen oder von Schadsoftware werden. Zudem fällt das Jailbreaking und Rooten in eine rechtliche Grauzone und kann unter Umständen die Garantie beeinträchtigen!

Bei manchen Apps (z. B. Spielen) besteht die Möglichkeit, in den Anwendungen Guthaben oder Punkte zu kaufen, ohne den klassischen Bestellvorgang zu durchlaufen (»In-App-Käufe«), wodurch die Gefahr, unbeabsichtigt Geld auszugeben, steigt. In-App-Käufe können zu einer unvorhergesehenen Kostenfalle werden: Besonders Kindern und Jugendlichen ist es oft nicht bewusst, dass sie auf ein kostenpflichtiges Angebot klicken, wenn sie zum Beispiel zusätzliches Spielguthaben erwerben, um in einem Spiel schneller voranzukommen.

Bei Android gibt es hier die Funktion der »Authentifizierung für Käufe«. Ist diese aktiviert, müssen Nutzerinnen und Nutzer bei jedem Kaufvorgang den entsprechenden Code zur Bestätigung eingeben.

Authentifizierung für App-Käufe

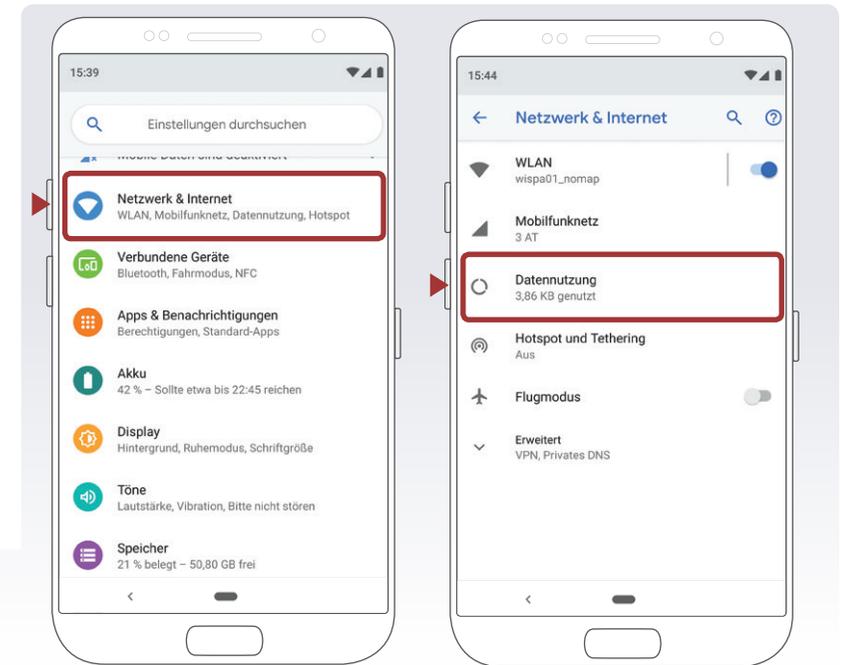
Google Playstore → nach rechts swipen → Einstellungen → Authentifizierung → Für alle Käufe bei Google Play auf diesem Gerät



Kostenfalle Datentarife

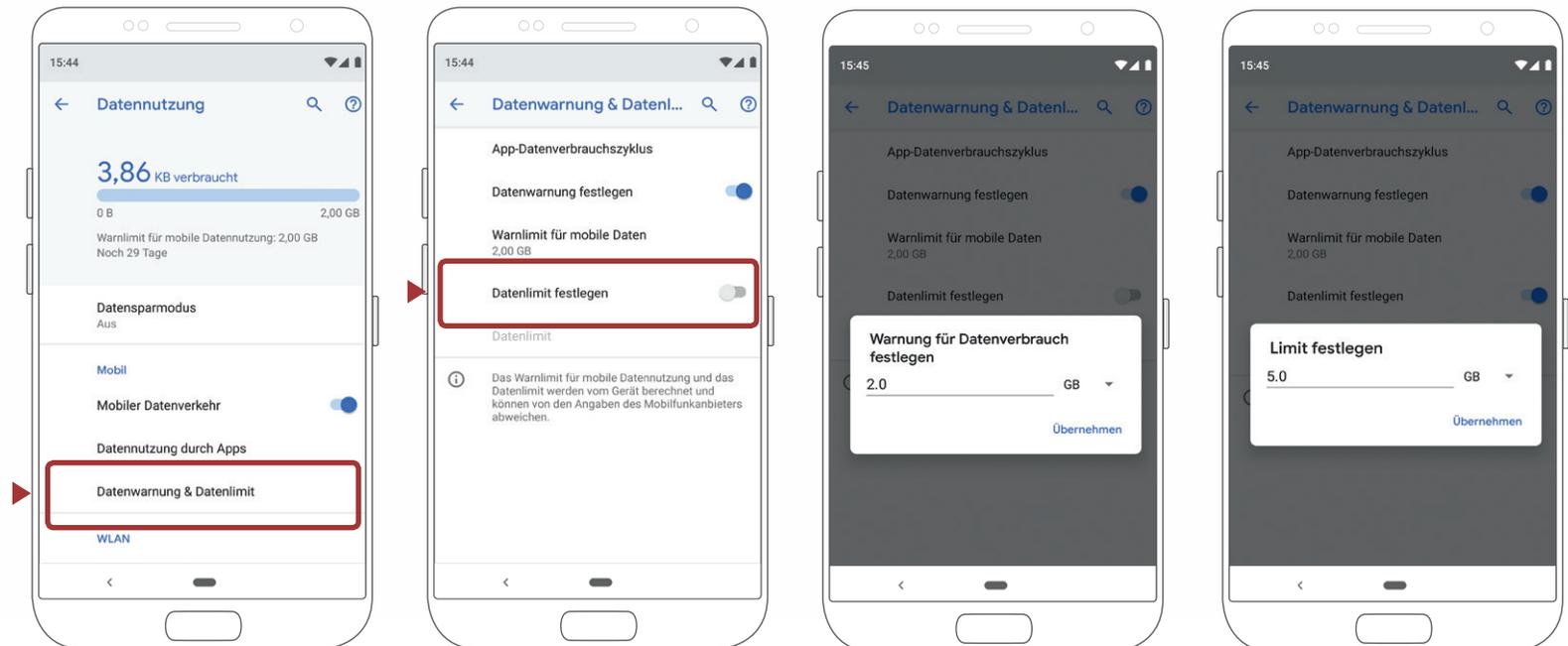
Viele Smartphone-Nutzerinnen und -Nutzer haben Handyverträge mit einem limitierten Internet-Paket, pro Monat können sie somit nur ein bestimmtes Datenvolumen verbrauchen. In vielen Fällen wird nach dem Überschreiten dieses Limits die Internetverbindung gedrosselt, in einigen wird jedes weitere Megabyte extra abgerechnet – und das kann teuer werden. Es empfiehlt sich daher, den eigenen Verbrauch im Auge zu behalten.

Viele Smartphones haben integrierte Funktionen, um den Datenverbrauch zu messen und auch Limits einzustellen. Alternativ kann eine App zur Kontrolle des Datenvolumens heruntergeladen werden; die meisten Mobilfunkanbieter bieten solche Apps zur Volumen- und Kostenkontrolle an. Jedoch sollte bei allen Lösungen beachtet werden, dass diese Programme keine endgültige Genauigkeit haben. Ist das Datenlimit beinahe erreicht, sollten Nutzerinnen und Nutzer im Zweifelsfall lieber auf weiteren Datenverbrauch verzichten, um so Extrakosten zu vermeiden. Zur Reduktion des Datenverbrauchs empfiehlt es sich auch, die Hintergrundsynchrosynchronisationen abzuschalten.



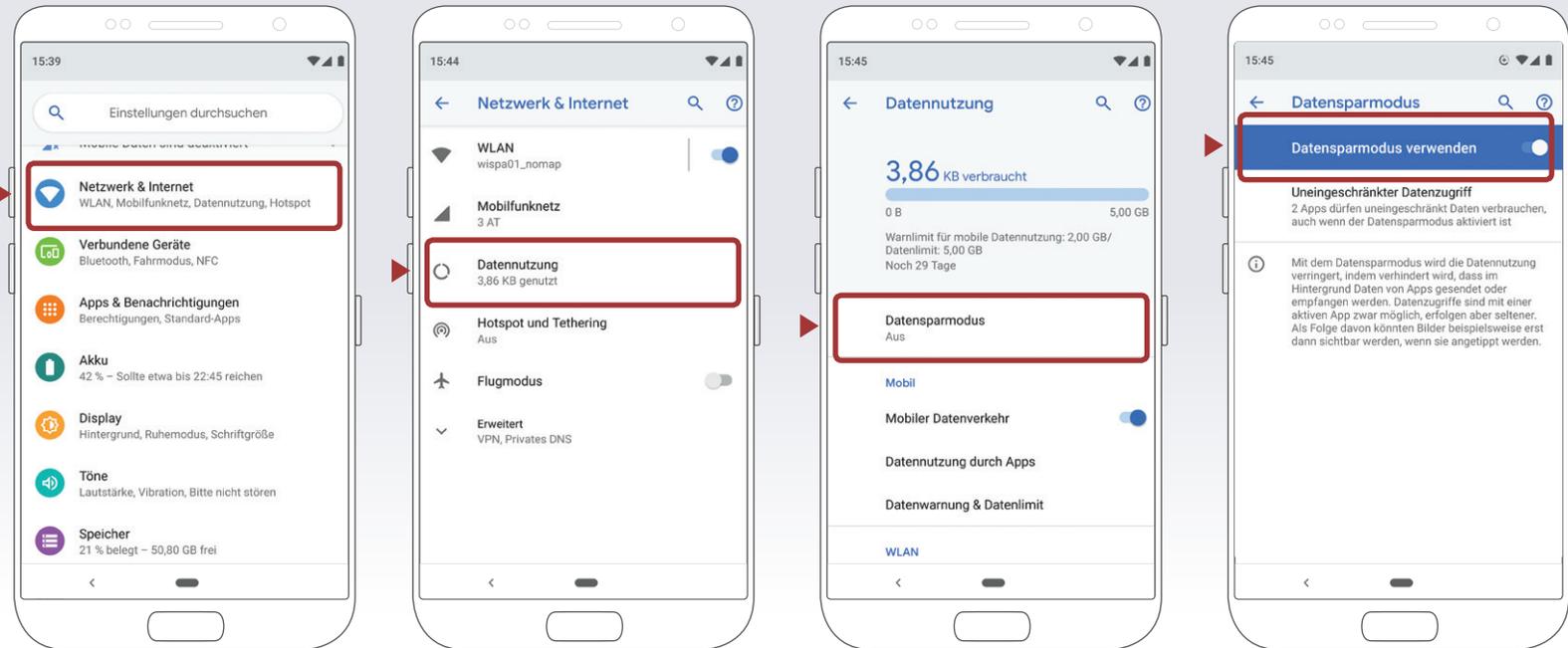
Datenlimit festlegen

Einstellungen → Netzwerk & Internet → Datennutzung → Datenwarnung & Datenlimit → Datenlimit festlegen → Datenlimit eintragen



Hintergrundsynchronisation deaktivieren

- Einstellungen
- Netzwerk & Internet
- Datennutzung
- Datensparmodus
- Datensparmodus verwenden



Roaming

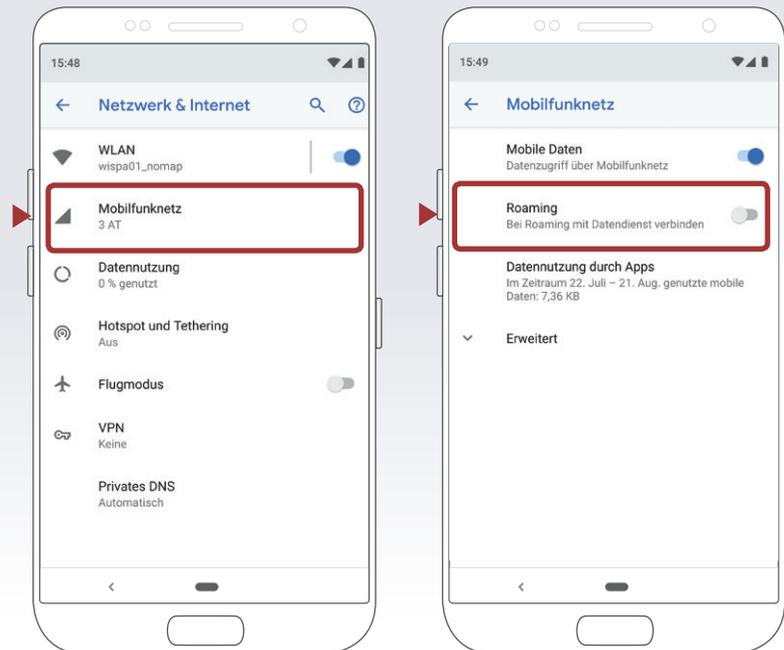
- Einstellungen
- Netzwerk & Internet
- Mobilfunknetz
- Roaming abwählen

Um zusätzliche Kosten im Ausland zu vermeiden, kann das Roaming deaktiviert werden. Im Juni 2017 wurden Roaminggebühren innerhalb der EU mit Ausnahmen abgeschafft. Konkret bedeutet das, dass Anrufe, die aus dem EU-Ausland getätigt werden, nicht mehr kosten dürfen als jene, die im Inland erfolgen. Freieinheiten (Freiminuten und -SMS), die durch das Bezahlen einer Grundgebühr zur Verfügung stehen, können auch im EU-Ausland genutzt werden. Das gilt ebenso für Datenpakete, hier kann der Betreiber aber eine eingeschränkte Nutzung vorgeben. Von inkludierten fünf GB dürften dann z. B. nur zwei GB auch im EU-Ausland genutzt werden. Außerhalb der EU kann es aber zu erhöhten Kosten kommen: Preise für Datendienste sind zum Teil extrem hoch: EUR 15,- bis EUR 20,- pro MB. Laut Roaming-VO muss eine Schutzgrenze bei EUR 60,- (auch in Drittstaaten) eingehalten sein. Dieser Grenzwert kann jedoch geändert werden.

ACHTUNG

Der Schutz durch die Roaming-VO gilt nicht auf Schiffen oder in Flugzeugen, die zum Teil eigene Mobilfunknetze (technisch gesehen via Satellit realisiert) anbieten.

Am besten schaltet man vor Aufenthalte außerhalb der EU zumindest die Daten-Roamingdienste und die Mobilbox für das Hinterlassen von Nachrichten direkt beim Netzbetreiber via App oder Telefonhotline aus. Roamingdienste können zwar auch am Endgerät selbst deaktiviert werden, direkt beim Betreiber ist aber die sicherere Variante. Beachten Sie, dass nicht bei allen Tarifen Roaming möglich ist.



WLAN, Bluetooth und mobile Hotspots

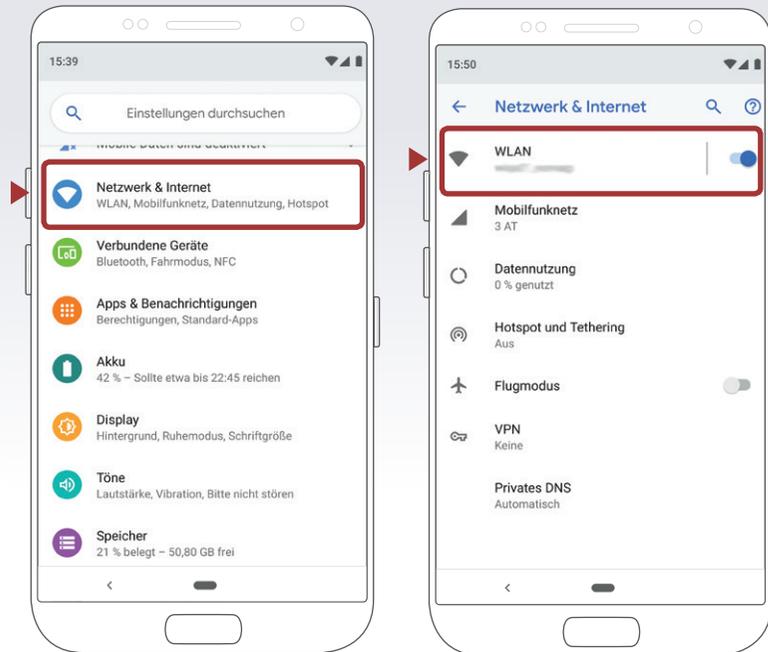
»Home is where your wifi connects automatically.«

Wenn sich das Smartphone selbstständig im Büro oder daheim mit dem WLAN verbindet, ist das praktisch und bequem, aber auf Dauer ein Sicherheitsrisiko. Der Datenaustausch über WLAN oder Bluetooth ist oft nur mangelhaft gesichert und kann relativ leicht

ausspioniert werden. Die WLAN-, Bluetooth- und NFC-Funktionen sollten nur dann eingeschaltet werden, wenn beispielsweise auf ein lokales WLAN-Netzwerk zugegriffen werden soll oder die Bluetooth-Funktion beziehungsweise NFC-Funktion unmittelbar benötigt wird. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist außerdem ein stark reduzierter Stromverbrauch.

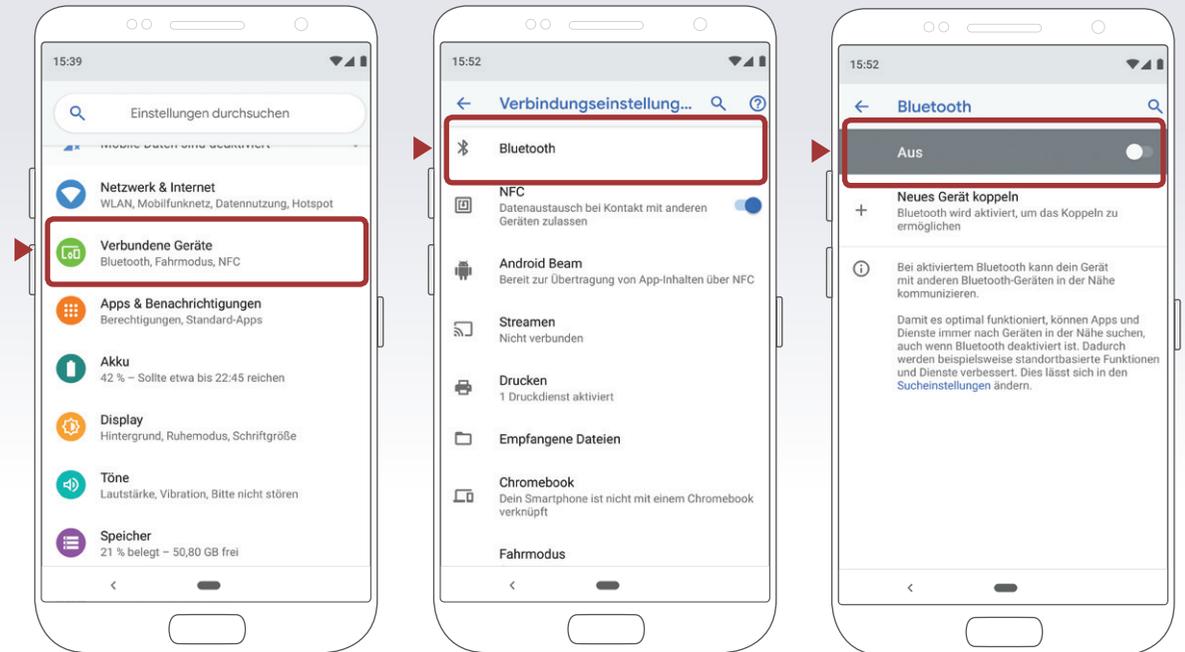
WLAN deaktivieren

Einstellungen → Netzwerk & Internet → WLAN abwählen



Bluetooth deaktivieren

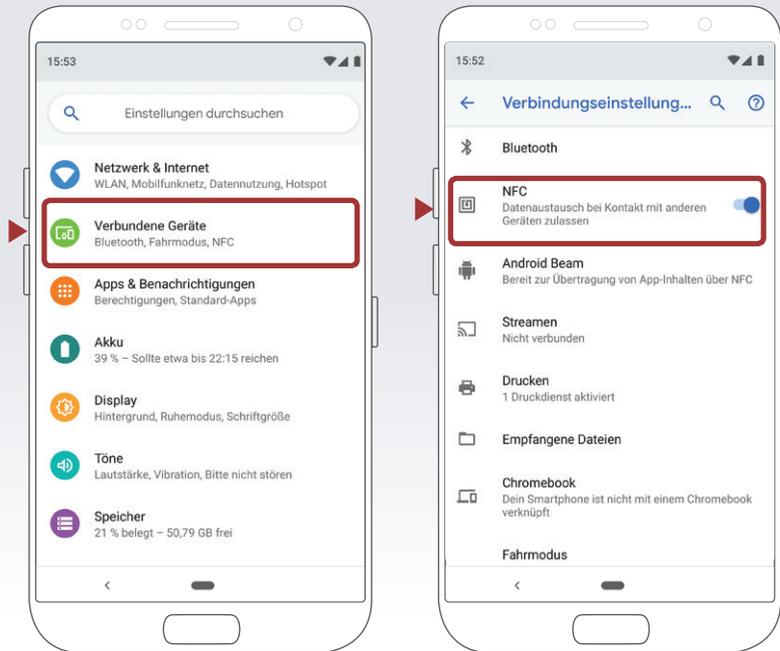
Einstellungen → Verbundene Geräte → Verbindungseinstellung → Bluetooth abwählen



NFC

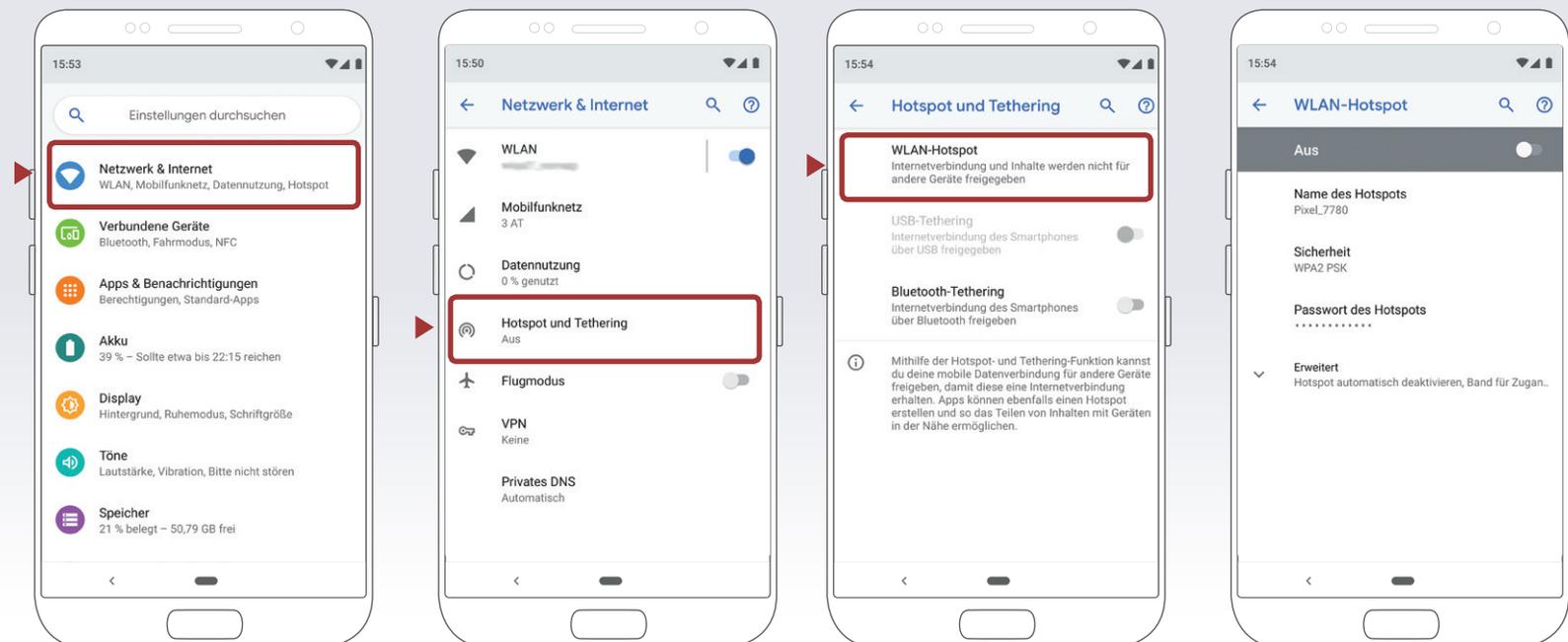
Einstellungen → Verbundene Geräte → Verbindungseinstellung → NFC abwählen

Near Field Communication (NFC) ermöglicht eine drahtlose Verbindung und den Transfer von Daten über eine kurze Distanz, dazu müssen sich zwei Geräte berühren oder sehr nah beieinander sein.



Sicherheitseinstellungen für WLAN-Hotspot

Einstellungen → Netzwerk & Internet → Hotspot & Tethering → WLAN-Hotspot



Datenverschlüsselung

Viele Android-Smartphones bieten die Funktion der Datenverschlüsselung für die Micro-SD-Karte – wenn eine im Smartphone eingesetzt und in Verwendung ist. Damit können Daten, welche extern – also auf der Micro-SD-Karte – gespeichert sind, zusätzlich geschützt werden. Hier gibt es oftmals die Möglichkeit, die gesamte Speicherkarte oder auch nur einzelne Inhalte zu verschlüsseln.

Sollen die Daten noch besser vor Missbrauch geschützt werden, kann eine Datenverschlüsselung für alle Smartphone-Inhalte angedacht werden. Diese Option wird jedoch nicht von allen Smartphones unterstützt. Wird das Smartphone gestohlen oder geht es verloren, sind

Konten, Einstellungen, Apps, Musik und Videos nur mit einem vorher festgelegten PIN-Code einsehbar. Die Passwortabfrage zur Entschlüsselung erfolgt bei jedem Einschalten des Gerätes zusätzlich zur SIM-Codesperre.

ACHTUNG

Die Verschlüsselung kann nicht rückgängig gemacht werden. Die Verschlüsselung kann nur aufgehoben werden, wenn das Gerät auf den Werkzustand zurückgesetzt wird, wodurch die Daten gelöscht werden.

Verkaufen, Verschenken & Verborgnen

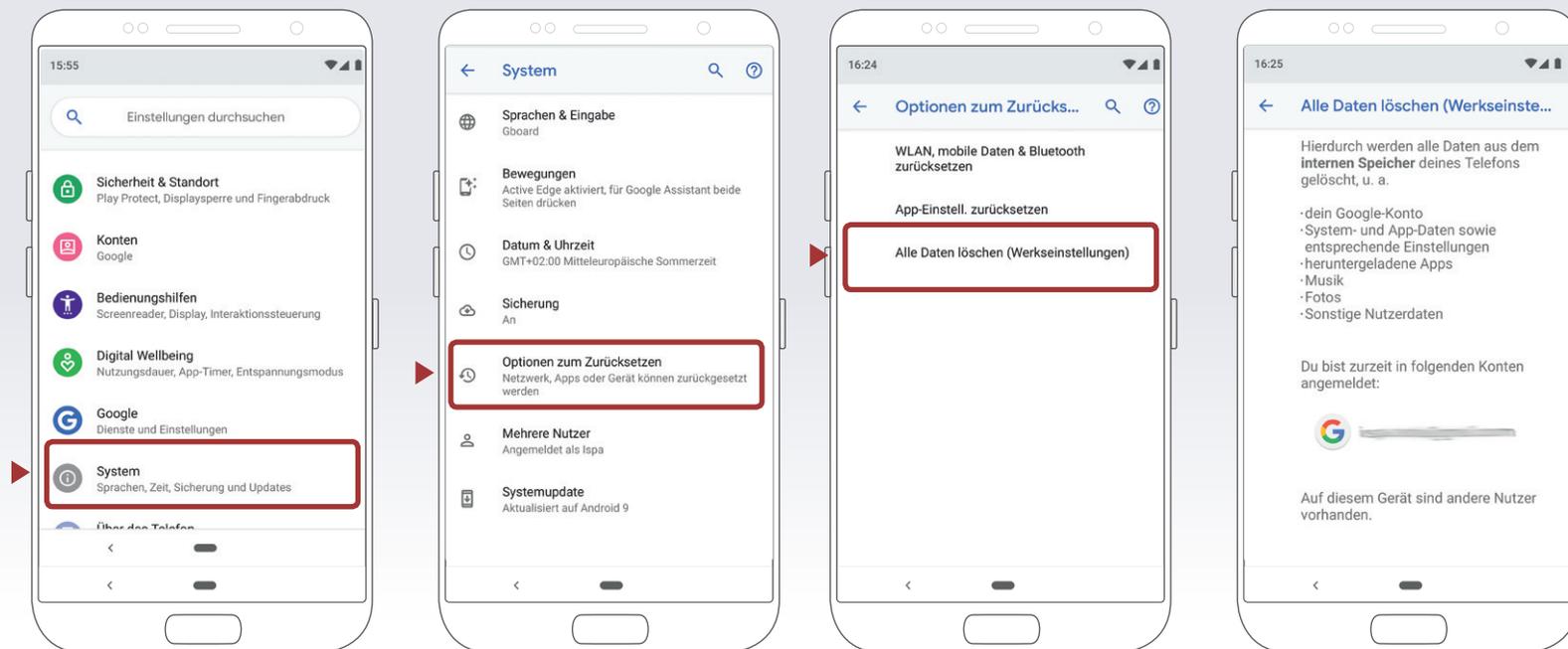
E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem Smartphone sind sehr viele persönliche Daten gesammelt. Soll das Gerät weitergegeben oder verkauft werden, sollte es unbedingt auf den Werkzustand zurückgesetzt und alle Daten gelöscht werden.

Um die Weitergabe der persönlichen Daten zu verhindern, sollten alle vorhandenen Speicher

gelöscht werden, also nicht nur der interne Speicher, sondern auch der externe (die Micro-SD-Karte). Hierfür reicht es nicht, diese einfach nur zu löschen oder das Smartphone auf die Werkseinstellungen zurückzusetzen, da mittels einiger Programme gelöschte Daten wiederhergestellt werden können. Erst spezielle Löschrprogramme machen durch mehrfaches Überschreiben des Speichers eine Wiederherstellung der Daten unmöglich.

Auf Werkzustand zurücksetzen

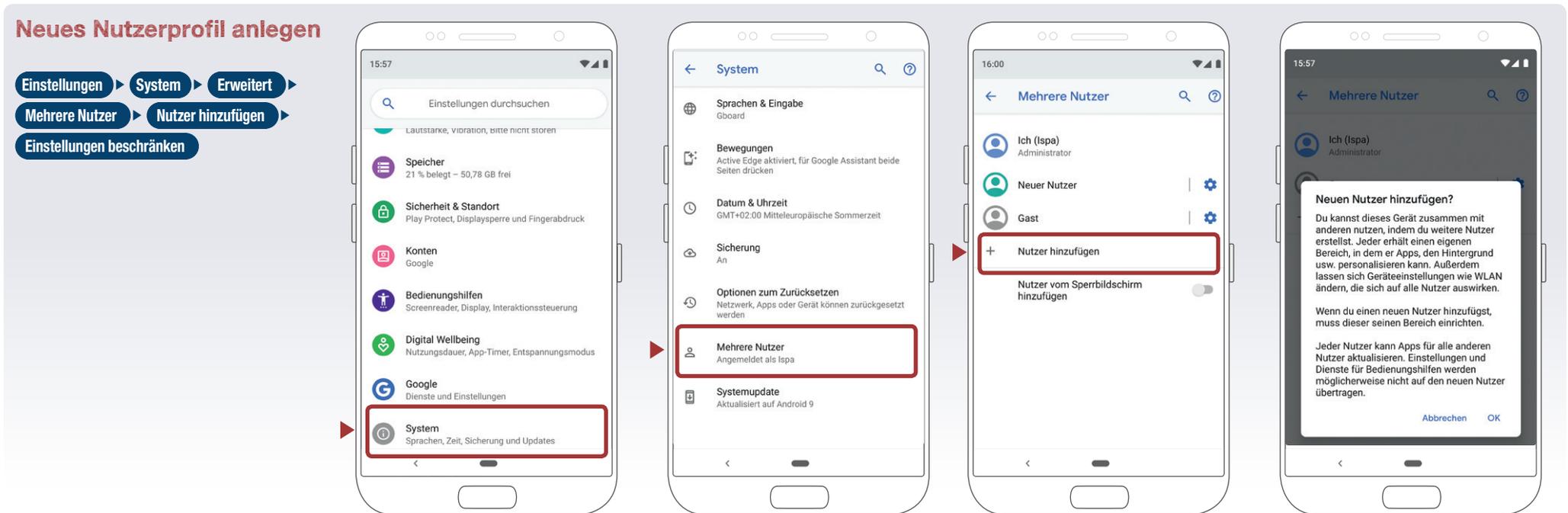
- Einstellungen ▶ System ▶ Erweitert ▶
- Optionen zum Zurücksetzen ▶
- Alle Daten löschen (Werkseinstellungen) ▶
- Telefon zurücksetzen



Das kindersichere Smartphone

Um ein Smartphone bei Bedarf kindersicher zu machen, sollten Roamingdienste außerhalb der EU deaktiviert, Jugendschutzeinstellungen im Playstore aktiviert, die Authentifizierung für App-Käufe eingeschaltet, der App-Filter auf jugendfrei gestellt und ebenso Mehrwertdienste und Drittanbieter gesperrt werden. Falls diese Funktion vom Smartphone unterstützt wird, kann ein Limit für den mobilen Datenverbrauch gesetzt werden. Für eine Nutzung durch jüngere Kinder kann überhaupt das Internet deaktiviert werden (in den Flugmodus wechseln).

Eine weitere Möglichkeit ist es ein eigenes – kindgerechtes - Nutzerprofil auf dem Smartphone anzulegen. Hier ist die Hauptnutzerin oder der Hauptnutzer gleichzeitig Administratorin oder Administrator und kann für jedes weitere angelegte Profil individuelle Einstellungen vornehmen, beispielsweise festlegen, auf welche Apps zugegriffen werden kann oder nicht.



Mittlerweile gibt es zahlreiche Apps, die sich dem Thema Kindersicherheit widmen. Diese sind aber Endgerät-basiert und funktionieren primär über Sperren und Filter. Zusätzlich sollten Erziehungsberechtigte bedenken, dass Medienerziehung nicht an Programme delegiert werden kann. Wichtig ist es, mit Kindern über das Internet, ungeeignete Inhalte und Online-Gefahren zu sprechen; ganz generell die Medienkompetenz der jüngsten Userinnen und User zu fördern. Ebenso sollten Eltern – und ältere Geschwister – bedenken, dass sie eine Vorbildfunktion haben, Kinder ahmen gerne das Verhalten von Älteren nach.

App fixieren

Möchte man dem Kind das Eltern-Smartphone kurz geben, um z. B. ein Spiel zu spielen, kann man die gerade verwendete App fixieren, damit das Kind keinen Zugriff auf die anderen Funktionen des Geräts erhält.

Einstellungen ▶ **Sicherheit & Standort** ▶ **Erweitert** ▶ **Bildschirmfixierung** ▶ **An aktivieren** ▶ **Gerät beim Beenden sperren aktivieren** ▶ **App öffnen – auf Übersichts-Modus wechseln – länger auf App-Symbol oben drücken** ▶ **Fixieren**

Zum Aufheben der Fixierung:

Zurück-Taste und Startbildschirm gleichzeitig gedrückt halten und **Entsperrungsmuster/PIN/Fingerabdruck**

Jugendschutzeinstellungen im Playstore

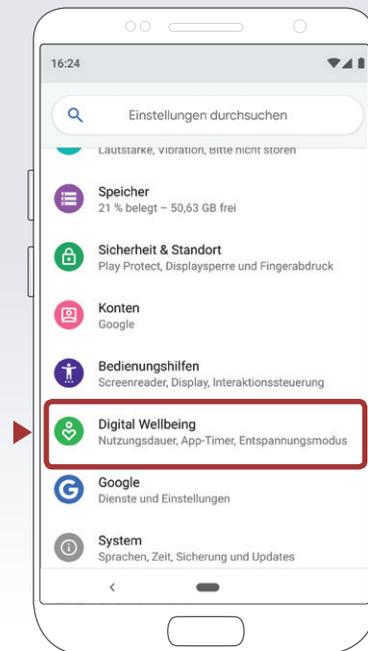
Damit Kinder keine Käufe im Playstore ohne die Zustimmung der Eltern tätigen könne, kann in den Playstore Einstellungen z. B. festgelegt werden, dass bei jedem Kauf eine Authentifizizierung erforderlich ist. Außerdem können Jugendschutzeinstellungen für Inhalte (Apps, Filme und Musik) getroffen werden.

Playstore ▶ **Einstellungen** ▶ **Nutzersteuerung**

Digital Wellbeing

Einstellungen ▶ **Netzwerk & Internet** ▶ **WLAN abwählen**

Immer mehr Menschen wird bewusst, dass sie sehr viel Zeit mit digitalen Geräten verbringen. Damit das Nutzungserlebnis besser wird, gibt es für Android unterschiedliche Digital Wellbeing Funktionen, z. B. Zeitlimits für bestimmte Apps.



TIPP

In unserer Broschüre »Technischer Kinderschutz im Internet« stellen wir weitere Möglichkeiten vor und geben Informationen, wie Kinder bei ihren ersten Erfahrungen im Internet unterstützt werden können.

Tipps, Hilfestellungen und Info-Materialien für Eltern und Erziehungsberechtigte gibt es unter www.saferinternet.at/fuer-eltern. Pädagoginnen und Pädagogen finden unter www.saferinternet.at/fuer-lehrende auch Materialien und Übungen für den Einsatz im Unterricht.

Die Arbeiterkammer Niederösterreich bietet Ihnen Beratung rund um die Themen Smartphone, Internet und Digitalisierung an. Mit dem Handy- und Internettarifrechner der AK (handy.arbeiterkammer.at) finden Sie sich leichter im Tarifdschungel zurecht. Weitere Leistungen und Kontakt zur Konsumentenberatung der Arbeiterkammer Niederösterreich finden Sie unter noe.arbeiterkammer.at/konsument



Währinger Straße 3/18, 1090 Wien
Tel.: +43 (0)1 409 55 76 | office@ispa.at
www.ispa.at | twitter.com/ispa_at
facebook.com/ISPA.InternetserviceProvidersAustria

