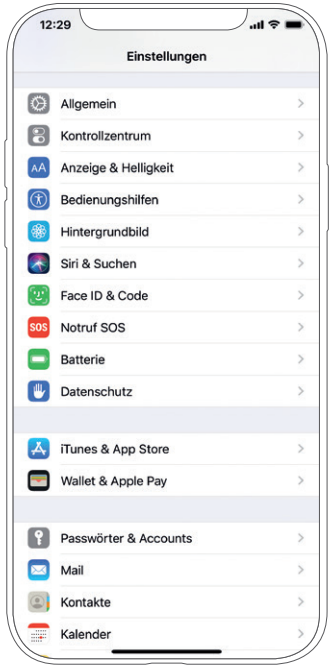
ispa
Internet Service Providers Austria



Sicherheitseinstellungen für Smartphones

iPhone

AK NIEDER ÖSTERREICH

Saferinternet.at
Das Internet sicher nutzen!

Co-financed by the European Union
Connecting Europe Facility

Inhaltsverzeichnis

Hinweis: Je nach Gerätetyp und Betriebssystem-Version 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: iPhone Xs Max
Betriebssystem: : iOS 13

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 Digitalisierungsoffensive 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.

Schutz vor unbefugtem Zugriff auf das Gerät

Ein Smartphone ist ein praktischer Begleiter und aus dem Alltag nicht mehr wegzudenken. Knapp 90 Prozent der Bevölkerung in Österreicher wenden 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. Die meisten Smartphones bieten zwei Sicherheitsfunktionen an, unbefugten Zugriff auf das Telefon und die darauf gespeicherten Informationen zu unterbinden:

SIM-PIN

Die SIM-PIN-Abfrage beim Einschalten des Gerätes (SIM-Kartensperre oder PIN-Eingabe) schützt aktiv vor missbräuchlicher Verwendung und sollte keinesfalls aus Bequemlichkeit abgeschaltet werden. Im Falle von Verlust oder Diebstahl des Smartphones 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 eigene Verschulden, z. B. Deaktivieren des SIM-PINs, zurückführen lassen. Nähere Informationen finden Sie dazu in den allgemeinen Geschäftsbedingungen Ihres Netzbetreibers.

Bildschirmsperre

Die Sperre, um den Ruhezustand aufzuheben, wird bei der ersten Inbetriebnahme des iPhone standardmäßig eingerichtet. Für die Bildschirmsperre bietet das iPhone-Betriebssystem iOS die Wahl zwischen drei verschiedenen Arten von Kennwörtern: einem ›vierstelligen numerischen Code‹ (vierstellige Ziffernkombination), einem ›eigenen numerischen Code‹ (Ziffernkombination beliebiger Länge) sowie einem ›eigenen alphanumerischen Code‹ (Passwort aus beliebigen Zeichen). Geräte ab dem iPhone 5S verfügen zudem über einen Fingerabdrucksensor (›Touch ID‹), mit dem sich das Telefon auf einfache Weise freischalten lässt, ohne jedes Mal aufs Neue einen Code eingeben zu müssen. Ab Geräten der iPhone-X-Generation gibt es die Face ID Funktion, bei der durch einen Blick die Bildschirmsperre aufgehoben werden kann.

Die höchste Sicherheit bietet ein längeres Passwort (›eigener alphanumerischer Code‹), besonders wenn dabei eine Kombination aus Zahlen, Groß- und Kleinbuchstaben und Sonderzeichen verwendet wird. Um ›komplizierte‹ Passwörter nicht zu vergessen, bieten sich die Anfangsbuchstaben eines einprägsamen Merksatzes an. Beispielsweise ergäbe sich aus dem Merksatz ›Ich mag Äpfel und bin 1980 geboren‹ das Passwort ›ImÄ&b1980g‹. Bei der Verwendung eines Ziffern-Pins sollten leicht zu erratende Kombinationen wie etwa der eigene Geburtstag, ›1234‹ oder gar ›0000‹ vermieden werden. Auch hier gilt natürlich: je länger der Zifferncode, desto sicherer.

Auf jeden Fall sollte darauf Acht gegeben werden, dass die Eingabe des Entsperr-Codes unauffällig erfolgt. Viele Sicherheitsangriffe sind überraschend trivial. Eine weit verbreitete Methode ist etwa das Abschauen oder Abfotografieren von Zugangsdaten und Passwörtern bei deren Eingabe. Besonders auf öffentlichen Plätzen, in dicht gedrängten Verkehrsmitteln oder bei neugierigen Sitznachbarinnen und -nachbarn im Flugzeug sollten Nutzerinnen und Nutzer vorsorglich achtsam sein.

Das Entsperren mittels Fingerabdrucksensor bietet diesbezüglich guten Schutz, allerdings sollte man sich bewusst sein, dass auch diese Form der Sicherung keine absolute Sicherheit bietet und von Angreifern umgangen werden kann. So genannte biometrische Merkmale (Fingerabdruck, Gesichtsgeometrie etc.) haben gegenüber Passwörtern zudem einen entscheidenden Nachteil: Sie können, sollten sie einmal in falsche Hände geraten, nicht einfach ›gewechselt‹ werden.

Die Art der Code-Sperre stellt letztendlich immer einen Kompromiss zwischen Sicherheit und bequemer Anwendung im Alltag dar. Ein für die meisten Nutzerinnen und Nutzer sinnvoller Mittelweg besteht in der Kombination eines starken Passwortes und der Verwendung des Fingerabdrucksensors.

Schutz vor unbefugtem Zugriff auf das Gerät

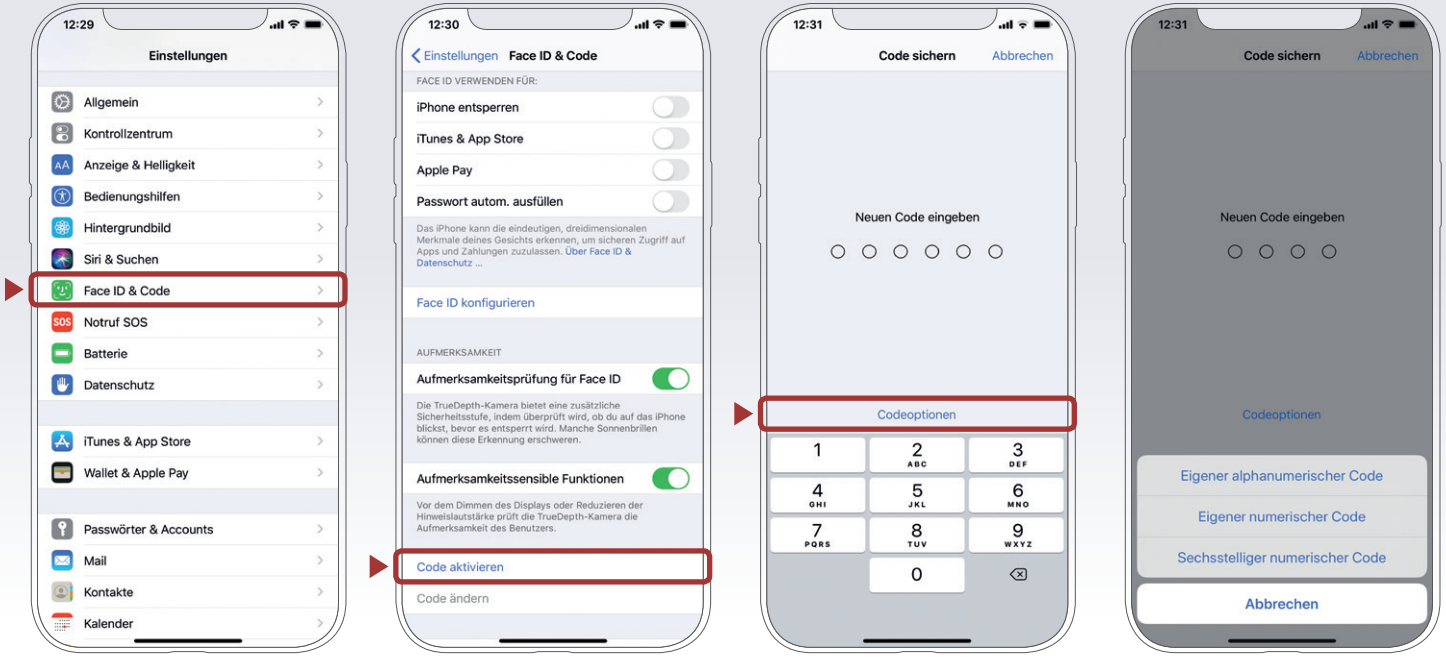
Die Code-Sperre aktivieren oder ändern

Einstellungen ▸

Face ID & Code (auf älteren Geräten auch Touch ID oder Code) ▸

Code aktivieren bzw. Code ändern

Mittels der Schaltfläche ›Codeoptionen‹ kann die Art der Code-Sperre (vierstelliger Zifferncode, mehrstelliger Zifferncode, alphanumerisches Passwort) eingestellt werden.

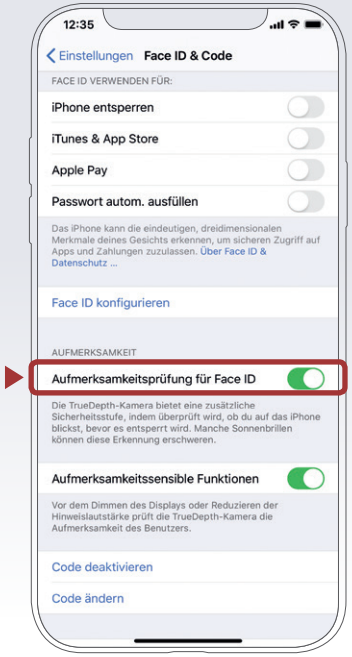


Aufmerksamkeitsprüfung für Face ID

Einstellungen ▸ Face ID & Code ▸

Aufmerksamkeisprüfung für Face ID

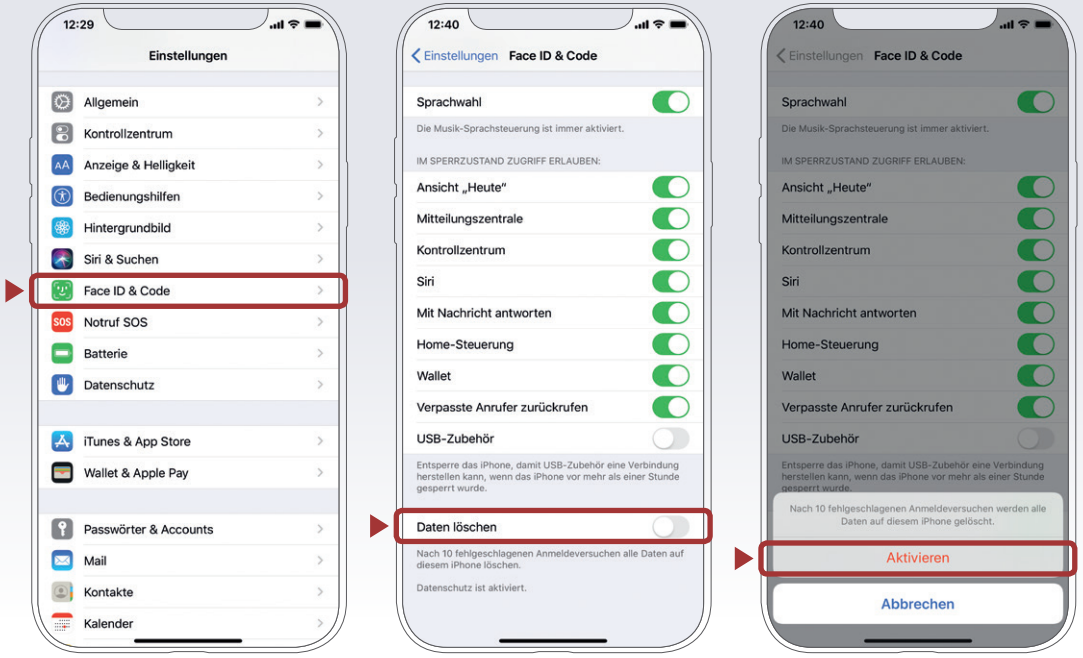
Ab Geräten der iPhone-X-Generation gibt es die Face ID Funktion, bei der durch einen Blick die Bildschirmsperre aufgehoben werden kann. Als zusätzliche Sicherheit für die Face ID kann eingestellt werden, dass beim Entsperrversuch mit geöffneten Augen direkt auf das Handy geblickt wird.



Automatische Datenlöschung

Einstellungen ▸ **Face ID & Code (auf älteren Geräten auch Touch ID oder Code)** ▸ **Daten löschen**

Ein weiteres unter iOS verfügbares Sicherheitsfeature ist die automatische Datenlöschung. Ist diese Option aktiviert, werden nach zehn fehlgeschlagenen Versuchen, das iPhone zu entsperren, alle darauf gespeicherten Daten gelöscht. Auch diese Einstellung findet sich unter ›Touch ID & Code‹ in der ›Einstellungen‹-App.



Den Sperrbildschirm sicher konfigurieren

Einstellungen ▸ **Kontrollzentrum** ▸ **Zugriff im Sperrbildschirm deaktivieren**

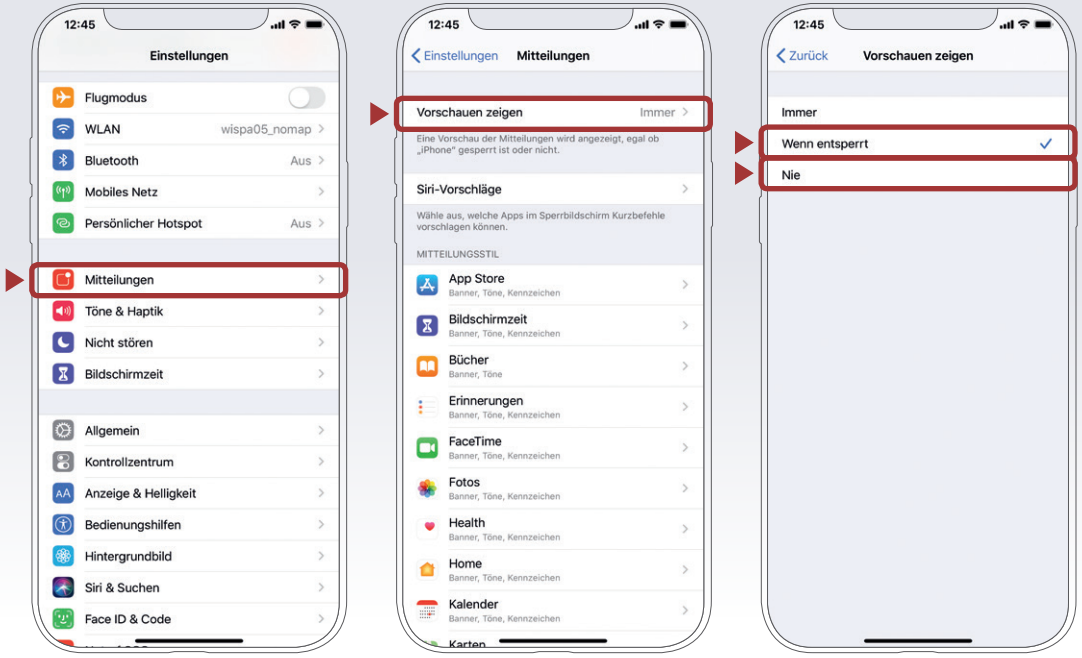
iOS bietet einige Funktionen, auf die auch im gesperrten Zustand des iPhone zugegriffen werden kann. So lassen sich etwa die Kamera, das Kontrollzentrum oder der Sprachassistent Siri benutzen und Apps können Widgets und Benachrichtigungen am Sperrbildschirm anzeigen.
Nicht verwendete Funktionen sollten deaktiviert werden, da sie unter Umständen den Zugriff auf persönliche Daten auch ohne Eingabe des Codes ermöglichen. So zeigt etwa die ›Heute‹-Ansicht je nach Konfiguration Kalendereinträge, Erinnerungen etc. an.
Auch das Kontrollzentrum sollte deaktiviert werden, da es einem Angreifer ermöglicht, durch Deaktivierung der Internetverbindung die Funktion von ›Mein iPhone suchen‹ zu umgehen.

Schutz vor unbefugtem Zugriff auf das Gerät

Vorschau deaktivieren

Einstellungen ▸ Mitteilungen ▸ Nachrichten bzw. Mail ▸ Vorschauen zeigen – ›wenn entsperrt‹ oder ›nie‹

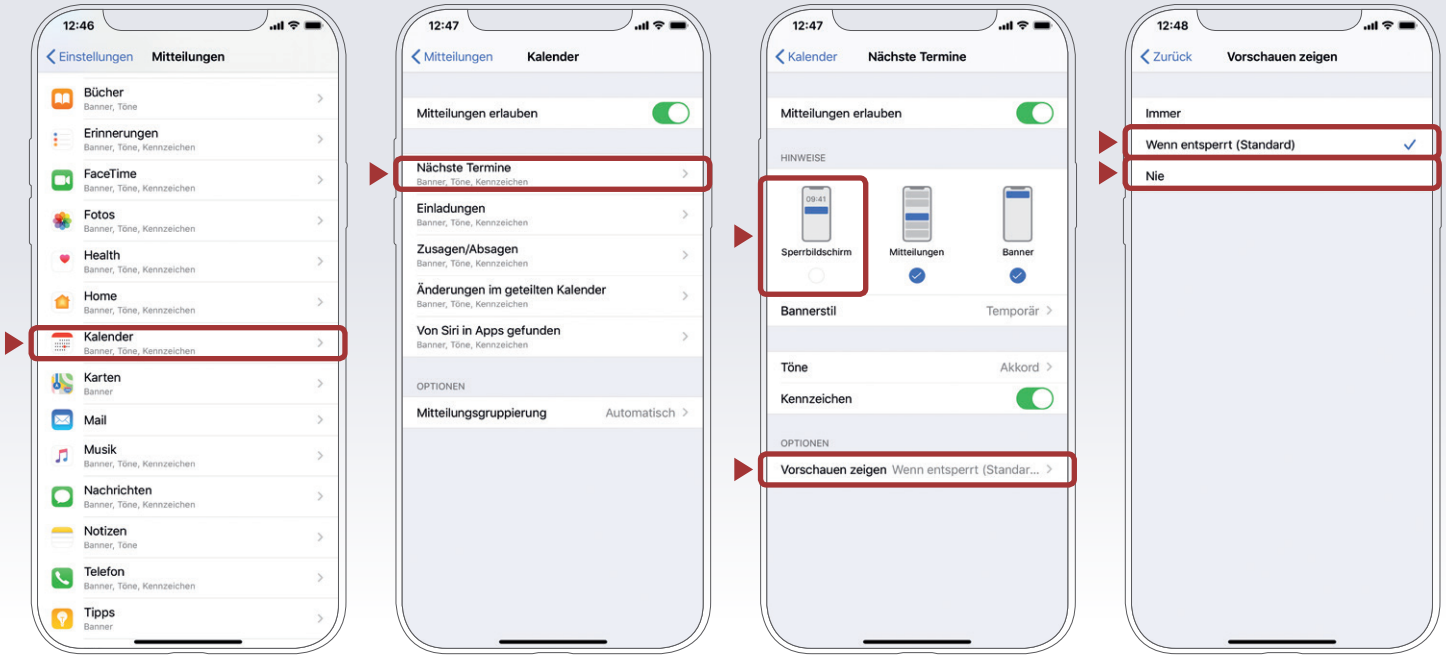
Kommunikations-Apps wie ›Nachrichten‹ und ›Mail‹ können so eingestellt werden, dass der Inhalt von SMS und E-Mails im gesperrten Zustand nicht angezeigt wird. So lässt sich zwar auf einen Blick sehen, von wem eine Nachricht empfangen wurde, deren Inhalt bleibt aber verborgen, bis das iPhone entsperrt wird.



Benachrichtigungen am Sperrbildschirm deaktivieren

Einstellungen ▸ Mitteilungen ▸
App auswählen z. B. Kalender ▸ ›Im Sperrbildschirm‹ deaktivieren

Die Anzeige von Benachrichtigungen am Sperrbildschirm lässt sich für einzelne Apps auch vollständig deaktivieren.



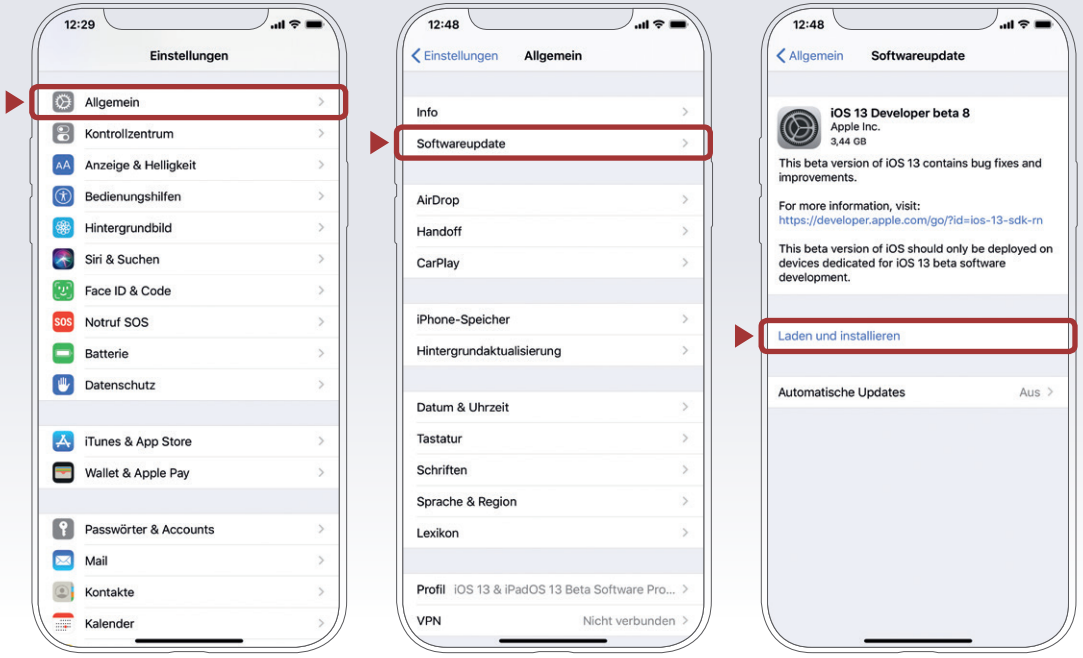
Software-Updates

Die vom Hersteller bereitgestellten Software-Updates für das iPhone sollten regelmäßig durchgeführt werden. Sie enthalten kleine Systemverbesserungen, reparieren Fehler und schließen eventuelle Sicherheitslücken. Üblicherweise sucht das iPhone bei bestehender Internetverbindung automatisiert nach Updates und macht gegebenenfalls darauf aufmerksam. Es ist empfehlenswert, Software-Updates möglichst zeitnah nach deren Veröffentlichung durchzuführen.

Manuelle Suche nach Software-Updates

Einstellungen ▸ Allgemein ▸ Softwareupdate

Unter der Rubrik ›Softwareupdate‹ in den allgemeinen Einstellungen können verfügbare Aktualisierungen gesucht und installiert werden.



App-Updates

Auch die am iPhone installierten Apps sollten regelmäßig aktualisiert werden. Dazu in der ›App Store‹-App das eigene Profil aufrufen. Über die Schaltfläche ›Alle aktualisieren‹ lassen sich sämtliche auf dem iPhone installierten Apps auf den neuesten Stand bringen. Alternativ können auch einzelne Apps aktualisiert werden.

Software-Updates

Automatische App-Updates

Einstellungen ▸ iTunes & App Store ▸ App-Updates

App-Updates lassen sich auch völlig automatisch durchführen, wobei eingestellt werden kann, ob aktualisierte Versionen nur bei bestehender WLAN-Verbindung oder auch über das Mobilfunknetz heruntergeladen werden.

App-Rückgabe

Bei einem App-Kauf wird man derzeit nicht über den Wegfall des Rücktrittsrechts gem. Fern- und Auswärtsgeschäfte-Gesetz (FAGG) informiert, daher besteht volle 14 Kalendertage die Möglichkeit, einen Kauf rückgängig zu machen. Auf der Seite reportaproblem.apple.com den jeweiligen Kauf und ›Ich möchte diesen Kauf stornieren‹ wählen, danach wird innerhalb weniger Geschäftstage der Kaufbetrag refundiert. (Diese Vorgehensweise kann sich erfahrungsgemäß bei exzessiver Nutzung des Rücktrittsrechts ändern, indem Apple bei einem weiteren Kauf den Rücktritt dann im Einzelnen ausschließt.)

Datenschutzeinstellungen

Moderne Smartphones verfügen über zahlreiche Sensoren (z. B. Mikrofon, Kamera, GPS-Empfänger), sind ständig mit dem Internet verbunden und speichern jede Menge persönliche Daten – diese Informationen können nicht nur mittels gezielter Angriffe bzw. durch physischen Zugriff auf das iPhone, sondern auch durch auf dem Gerät installierte Software in unbefugte Hände gelangen.

Prinzipiell bietet iOS hier einen vergleichsweise guten Schutz, da alle Apps von Drittanbietern ein Testverfahren durchlaufen müssen, bevor sie im App-Store zum Download verfügbar sind und auf dem Gerät installiert werden können. Auch dieses Verfahren kann naturgemäß keinen absoluten Schutz vor Schadsoftware garantieren, solange aber die Integrität des Betriebssystems nicht von den Nutzerinnen und Nutzern bewusst ausgehebelt wird (siehe Kapitel ›Jailbreak‹) und nur Apps aus dem offiziellen Store geladen werden, ist das iPhone vor der unbeabsichtigten Installation von Schadsoftware relativ sicher. Zudem können Apps nur dann auf die Sensoren des iPhone bzw. persönliche Daten wie das Adressbuch oder die gespeicherten Fotos zugreifen, wenn dies von den Nutzerinnen und Nutzern zuvor ausdrücklich erlaubt wurde.

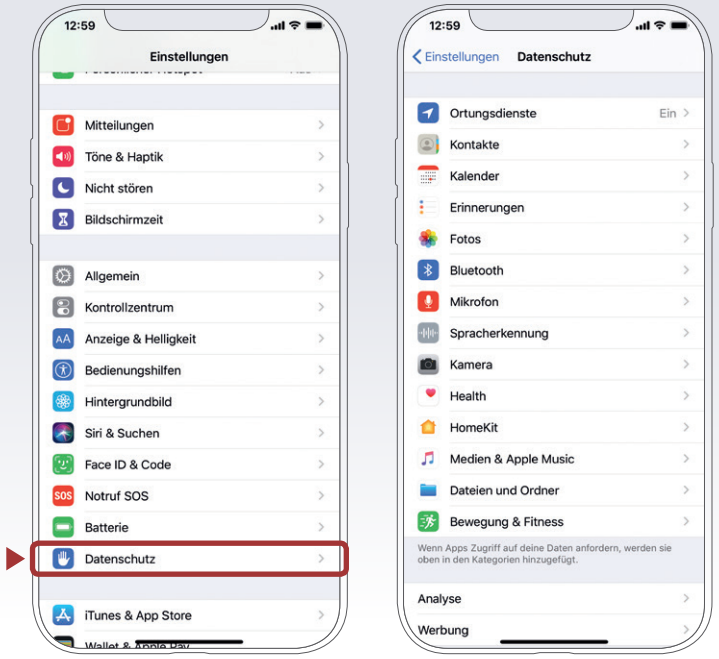
Nicht bedenkenlos allen App-Zugriffsberechtigungen zustimmen

Oftmals ist es aber gar nicht unbedingt eine Sicherheitslücke im engeren Sinne, die von ›bösartigen‹ Apps ausgenutzt wird, um an Daten zu kommen. Vielmehr macht man sich die Unachtsamkeit der Userinnen und User zunutze und fordert Berechtigungen, etwa für den Zugriff auf das Adressbuch, obwohl diese für die Funktionalität der App gar nicht nötig sind. Hier sollte man vorsichtig sein und nur dann zustimmen, wenn diese Zugriffsrechte plausibel und notwendig erscheinen. Handelt es sich zum Beispiel um eine Spiele-App, braucht diese eher keinen Zugriff auf das Adressbuch; dass hingegen eine Navigations-App Zugriff auf die Standort-Daten benötigt, macht wiederum Sinn. Es empfiehlt sich, bewusst auszuwählen, welche Daten welcher App zur Verfügung gestellt werden. Die Zugriffsrechte einer App können zudem auch jederzeit wieder deaktiviert werden.

Einzelne Zugriffsberechtigungen anzeigen und deaktivieren

Einstellungen ▸ Datenschutz

Der Menüpunkt ›Datenschutz‹ in der ›Einstellungen‹-App ermöglicht es, genau festzulegen, welche Apps auf den eigenen Standort, die Kontakte, Kalender, aber auch Sensoren wie Kamera oder Mikrofon zugreifen können.



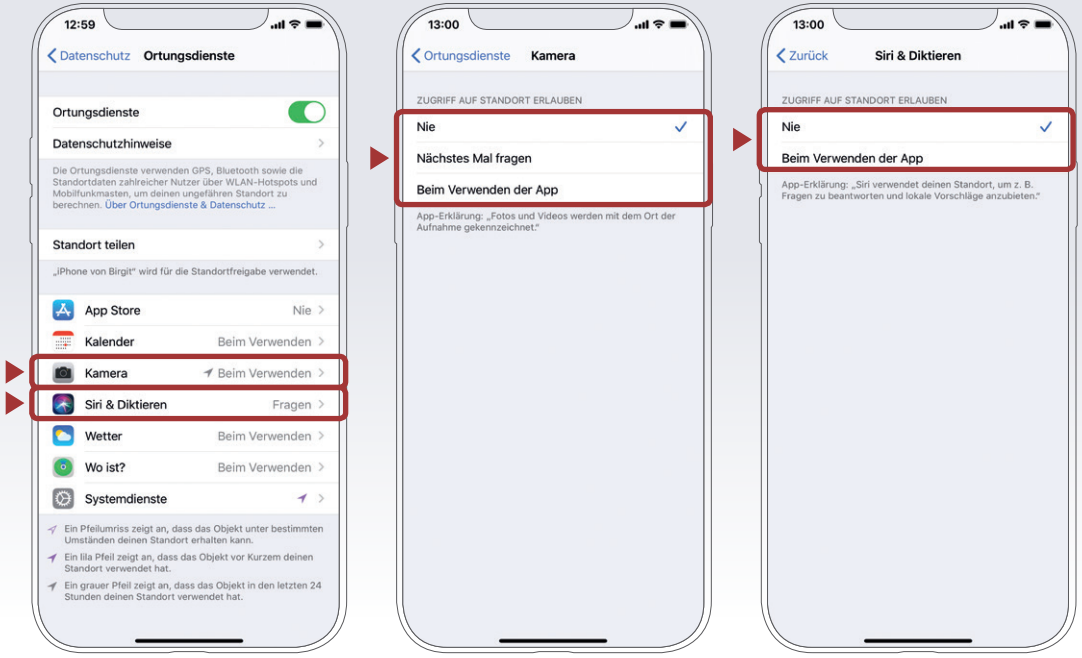
Datenschutzeinstellungen

Beispiel: Zugriff auf den eigenen Standort einschränken

Einstellungen ▸ Datenschutz ▸ Ortungsdienste

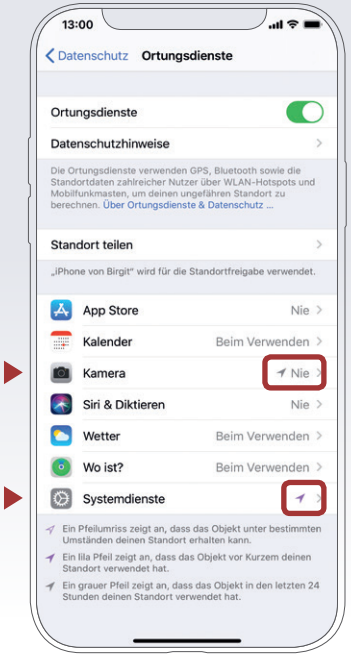
Die sogenannten ›Ortungsdienste‹ ermöglichen dem iPhone den eigenen Standort aus GPS-Daten, Bluetooth- und WLAN-Informationen und der Position von Mobilfunkmasten zu errechnen. Der Standort kann sowohl vom System selbst als auch von installierten Apps verwendet werden. Der Zugriff auf die Ortungsdienste sollte nur jenen Apps gewährt werden, die diesen auch wirklich benötigen. Sollte nicht schlüssig ersichtlich sein, warum eine App den Standort benötigt, ist es sicherer, diesen zu deaktivieren. Ein positiver Nebeneffekt besteht in einer verlängerten Akkulaufzeit, da insbesondere eine häufige Aktivierung des GPS-Sensors den Stromverbrauch deutlich erhöht.

In den Einstellungen für Ortungsdienste lässt sich für jede App einzeln einstellen, ob diese auf den eigenen Standort ›nie‹, ›beim Verwenden‹ der App oder ›immer‹ zugreifen kann. Manche Apps fordern Zugriff auf die Ortungsdienste, auch wenn sie nicht aktiv verwendet werden. So benötigt etwa die Wetter-App den Standort auch dann, wenn sie nicht geöffnet ist, um im Sperrbildschirm das Wetter für den jeweils aktuellen Standort als Widget anzeigen zu können. Auf Wunsch kann auch die Einstellung getroffen werden, dass eine App bei jedem Ausführen nachfragen muss, ob der Standort freigegeben wird.



Zeitpunkt des Zugriffs

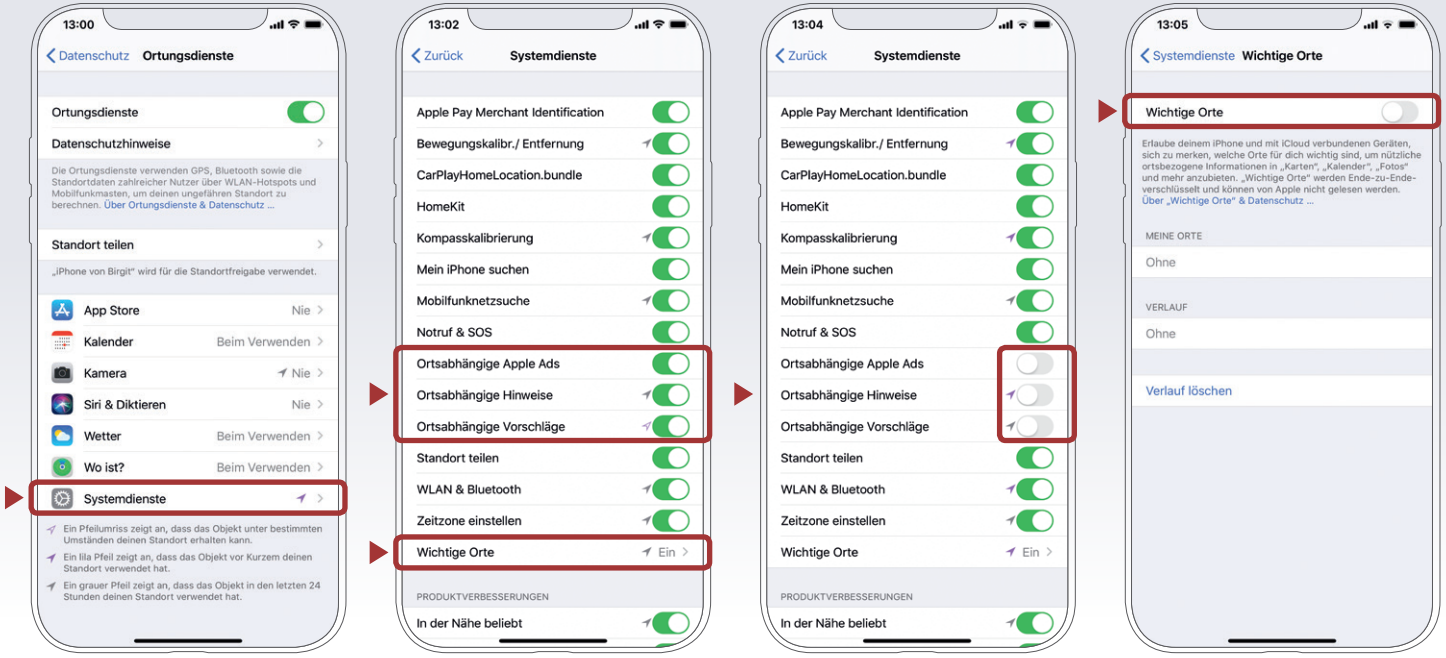
Zur vereinfachten Überprüfung wird in dieser Liste jeweils ein Symbol angezeigt, wann die entsprechende App die Ortungsdienste verwendet hat. Ist das Symbol lila, wurde der Standort kürzlich abgefragt. Ein nicht ausgefüllter lila Pfeil bedeutet, dass eine Anwendung unter bestimmten Bedingungen den Standort erhält. Ein grauer Pfeil bedeutet, dass die App innerhalb der letzten 24 Stunden auf den Standort zugegriffen hat.



Standort-Tracking deaktivieren

Einstellungen ▸ Datenschutz ▸ Ortungsdienste ▸ Systemdienste

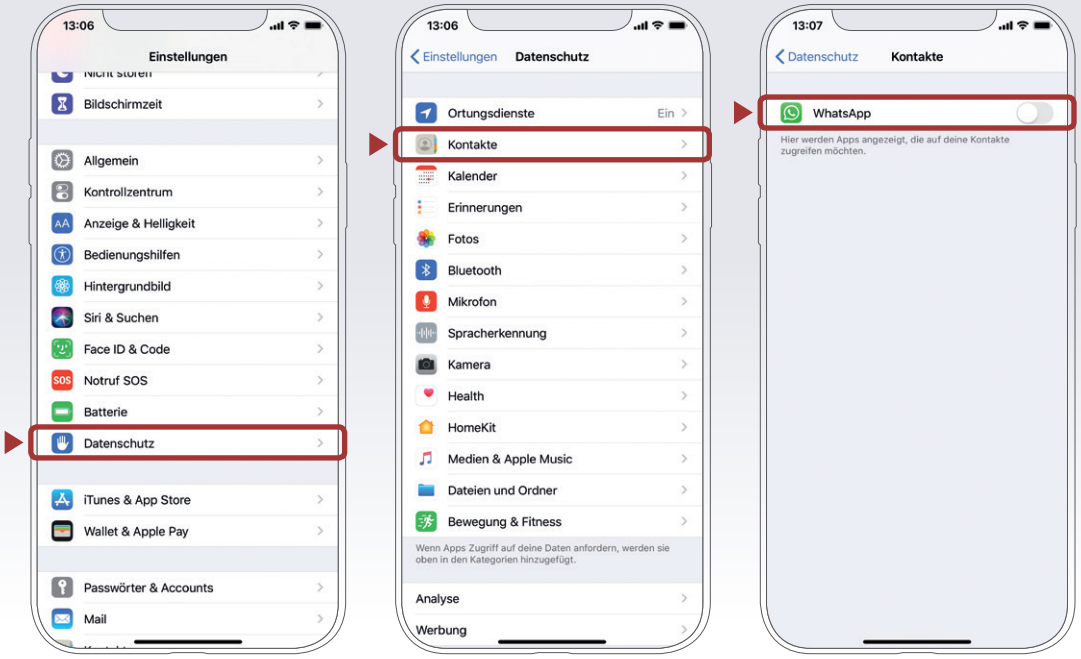
Einige Systemdienste, die zum Beispiel die Anzeige ortsabhängiger Werbung oder Hinweise ermöglichen, können bei Bedarf ebenfalls deaktiviert werden.



Einzelne Datenzugriffspunkte für einzelne Apps deaktivieren

Einstellungen ▸ Datenschutz ▸ Kontakte (o. ä.)

Damit Apps nur Zugriff auf jene Daten haben, die sie brauchen, und nicht zusätzliche sammeln, kann der Zugriff eingeschränkt werden.



Datenschutzeinstellungen

Ad-Tracking Beschränken

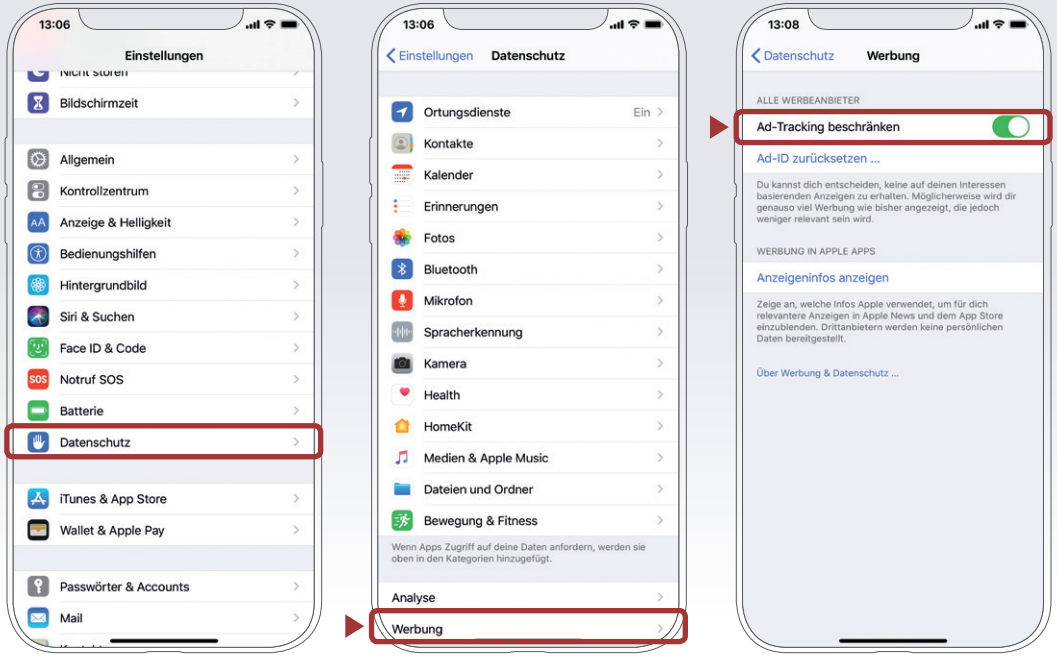
Einstellungen ▸ Datenschutz ▸ Werbung ▸ Ad-Tracking beschränken

Werbung wird durch das Sammeln von Daten möglichst personalisiert an Nutzerinnen und Nutzer ausgespielt. Durch Aktivieren des Ad-Tracking-Limits wird die Werbung nicht personalisiert.

Ortsabhängige Apple-Ads

Einstellungen ▸ Datenschutz ▸ Ortungsdienste ▸ Systemdienste ▸ Ortsabhängige Apple Ads deaktivieren

Das iPhone sendet den Standort an Apple, damit den Nutzerinnen und Nutzern geografisch relevante Anzeigen in Apple News sowie im App Store gezeigt werden. Diese Option kann deaktiviert werden.



Siri auf Sperrbildschirm ausschalten

Einstellungen ▸ Face ID & Code ▸ Im Sperrzustand Zugriff erlauben ▸ Siri aus

Bei aktivierter Siri im Sperrbildschirm können auch Unberechtigte Zugang zu persönlichen Daten, Nachrichten oder vertraulichen Terminen (z. B. Arztterminen) erhalten. Daher empfiehlt es sich, diese Funktion auszuschalten.

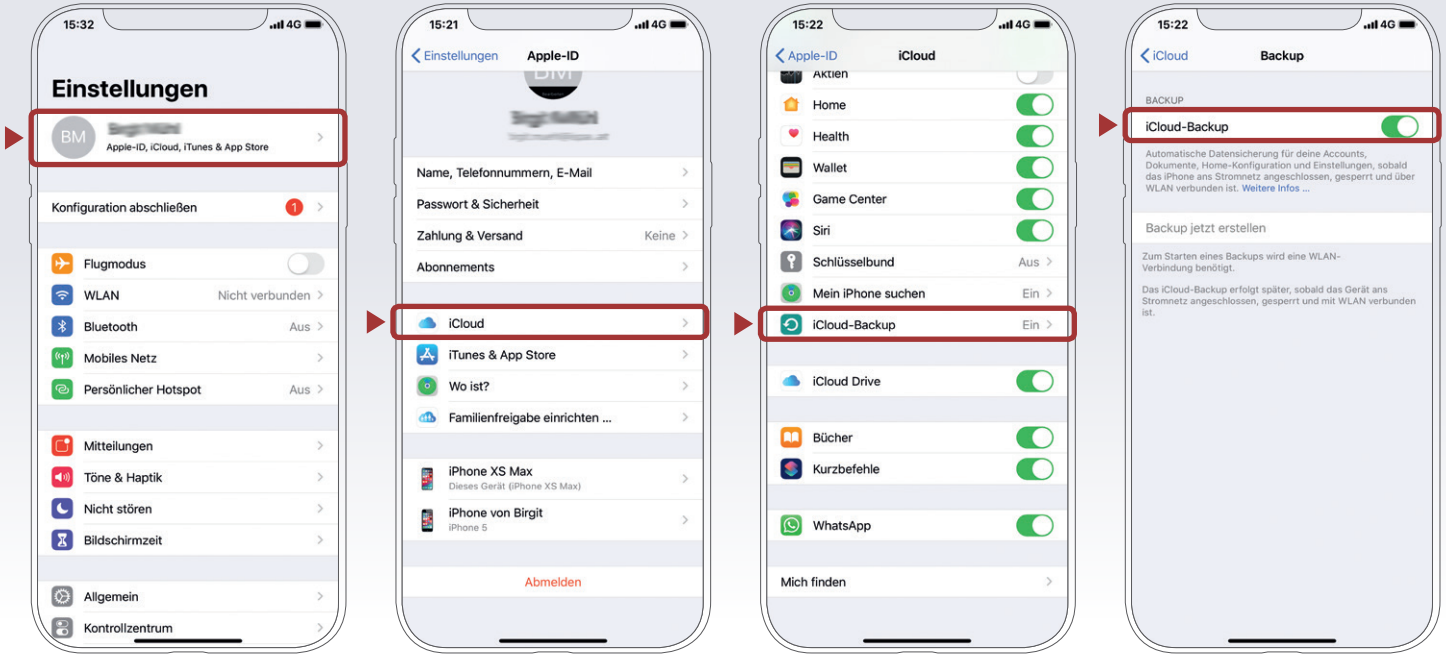
Synchronisierung & Backups

Genau wie bei einem Mac/PC ist es auch bei einem Smartphone sinnvoll, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Daten- oder Handyverlusts kann so auf das Backup zugegriffen werden. Somit ist zumindest der letzte Stand der gesicherten Daten verfügbar.

Eine Möglichkeit beim iPhone ist der iTunes-WLAN-Sync, hierfür kann das iPhone per USB-Kabel mit dem Mac/PC verbunden oder die Daten kabellos via WLAN übertragen werden. Eine andere Möglichkeit bietet die Funktion iCloud-Backup. Hier werden Daten und Einstellungen über WLAN im Cloud-Service von Apple gespeichert. Dabei kann festgelegt werden, welche Daten in der iCloud abgelegt werden sollen (z. B. nur Fotos, nicht aber Kontakte). Hierfür wird die Apple-ID benötigt. Zusätzlich können mit iCloud Daten automatisch zwischen mehreren Geräten synchronisiert werden. Wer sich bei iCloud registriert, erhält automatisch kostenlos 5 GB Onlinespeicherplatz. Wenn mehr iCloud-Speicherplatz benötigt wird, kann ein kostenpflichtiges Upgrade auf einen Speicherplan mit mehr Speicherplatz durchgeführt werden.

Aktivierung von iCloud-Backup

Einstellungen ▸ Apple-ID ▸ iCloud ▸ iCloud-Backup an

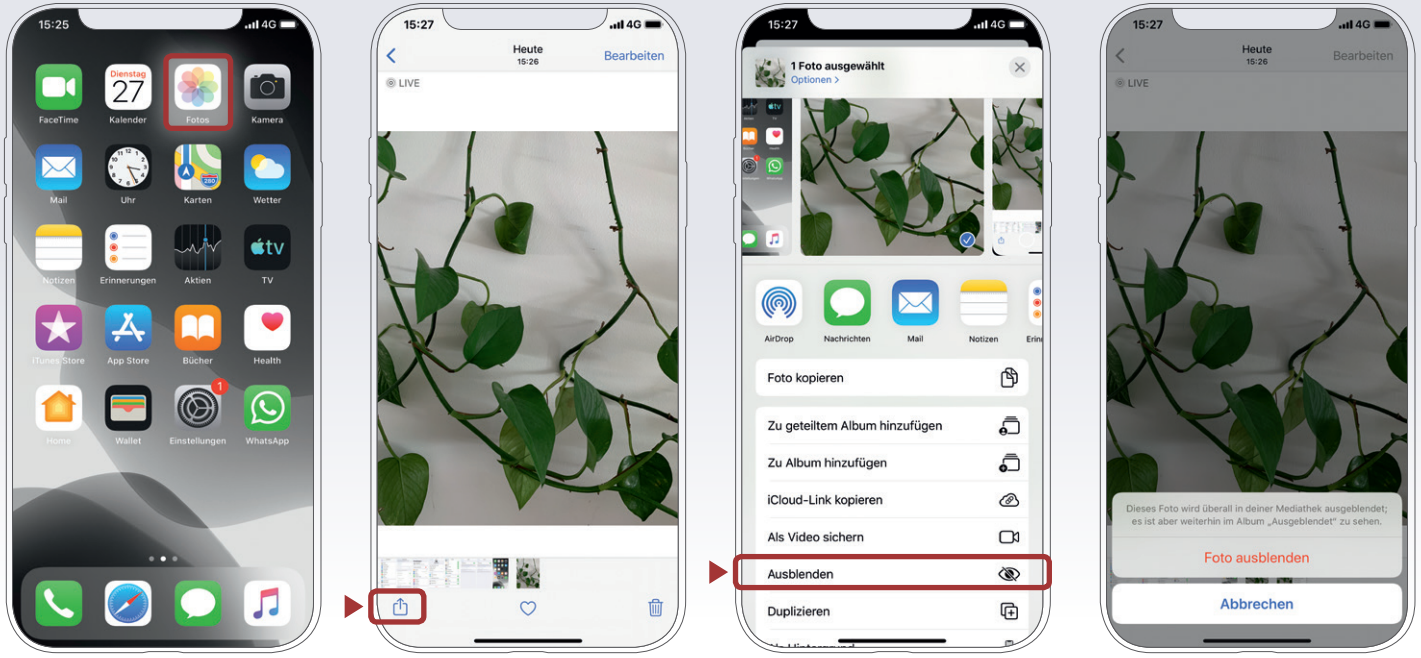


Synchronisierung & Backups

Fotos verstecken

Fotos ▸ Foto auswählen ▸ Teilen-Button ▸ Ausblenden

Viele Nutzerinnen und Nutzer besitzen Fotos auf dem Smartphone, die privat sind und nicht mit anderen geteilt werden möchten. Es gibt z. B. die Möglichkeit, zu verhindern, dass Fotos automatisch in die Cloud hochgeladen werden. Die versteckten Fotos werden in den Ordner ›Versteckt‹ (bei anderen Versionen auch ›Ausgeblendet‹) verschoben und erscheinen dann auch nicht in den automatisch erstellten Moments, Years und Collections.



Zwei-Faktor-Authentifizierung

Um die Daten möglichst sicher abzuspeichern, ist es sinnvoll, für Konten wie die Apple-ID eine Zwei-Faktor-Authentifizierung (auch Bestätigung in zwei Schritten genannt) zu verwenden. Sie ist eine weitere Sicherheitsmaßnahme, die missbräuchlichen Zugriff auf das Konto verhindert.
Nach erfolgter Einrichtung sind zwei Schritte nötig, um sich beim Konto anzumelden. Um sich erfolgreich einzuloggen, 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, E-Mails, Fotos und viele weitere persönliche Daten gespeichert sind, besser abgesichert. Viele Anwendungen bieten aus Sicherheitsgründen bereits eine Zwei-Faktor-Authentifizierung an, die nur noch aktiviert werden muss. Geräte, die man häufig verwendet, können als vertrauenswürdig eingestuft werden, wodurch die Bestätigung des zweiten Faktors beim nächsten Einloggen über diese Geräte nicht mehr notwendig ist.

Anmelden mit Apple: Kontrolle über Privatsphäre

Ähnlich wie Google und Facebook bietet Apple eine Funktion an, sich bei anderen Diensten und Webseiten mit der Apple-ID anzumelden. Apple limitiert dabei jedoch die Menge an persönlichen Daten, die mit den Diensteanbietern geteilt wird, und verspricht den Schutz der persönlichen Daten. Voraussetzung für die Verwendung dieser Funktion ist, dass die Zwei-Faktor-Authentifizierung der Apple-ID aktiv ist.

WLAN, Bluetooth und mobile Hotspots

»Home is where your wifi connects automatically«: Wenn sich das Smartphone selbstständig mit dem WLAN verbindet, ist das zwar praktisch und bequem, kann aber auf Dauer ein Sicherheitsrisiko darstellen.

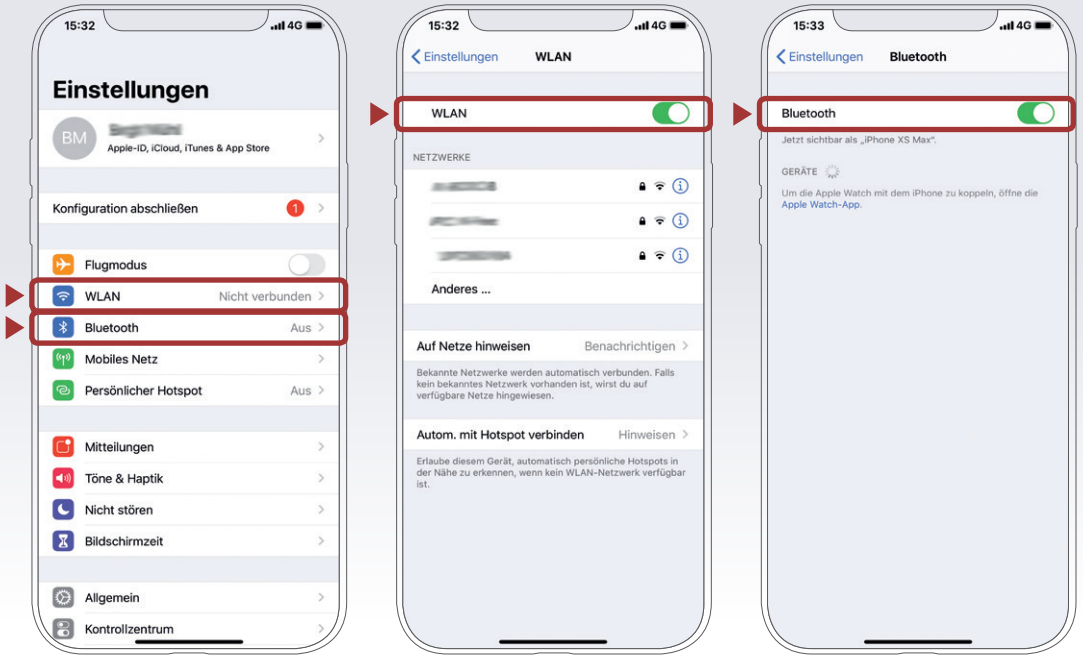
Der Datenaustausch über WLAN oder Bluetooth ist oft nur mangelhaft gesichert und kann relativ leicht ausspioniert werden. Die WLAN- und Bluetooth-Funktion sollte nur dann eingeschaltet werden, wenn auf ein lokales WLAN-Netzwerk zugegriffen werden soll oder die Bluetooth-Funktion unmittelbar benötigt wird. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist ein stark reduzierter Stromverbrauch.

WLAN und Bluetooth deaktivieren

Einstellungen ▸ WLAN deaktivieren

Einstellungen ▸ Bluetooth deaktivieren

Wie viele Smartphones bietet auch das iPhone die Möglichkeit, als WLAN-Router zu fungieren und so beispielsweise als mobiler Hotspot für den eigenen Laptop zu dienen. Die Hotspot-Funktion sollte jedenfalls mit einem starken Passwort, das aus Zahlen und Buchstaben besteht, gesichert und ebenfalls nur bei Bedarf aktiviert werden.

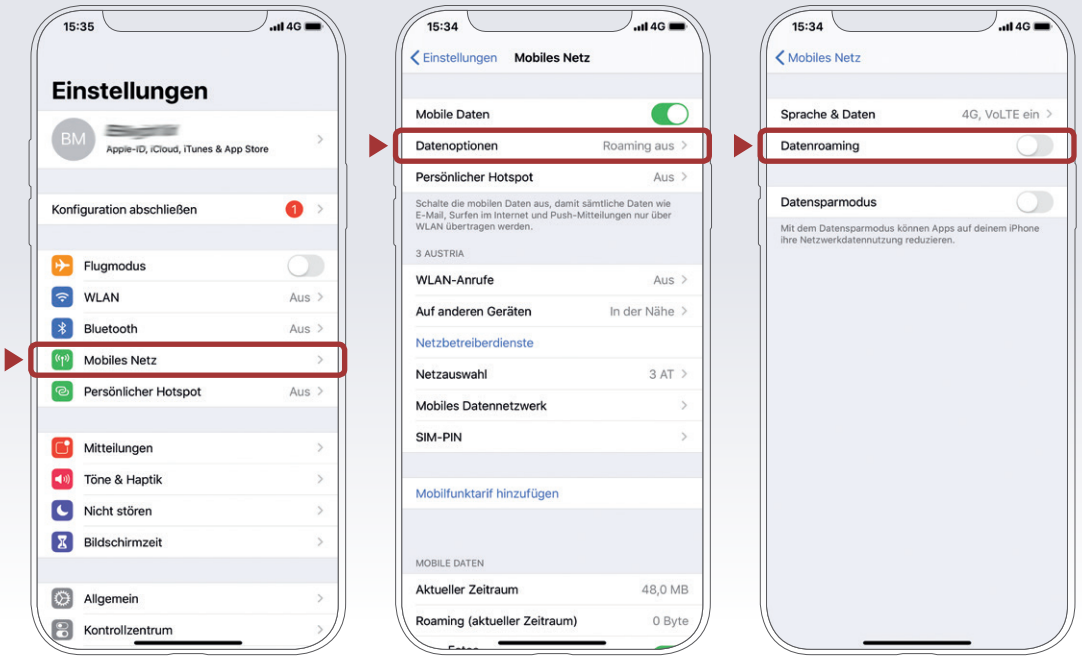


WLAN, Bluetooth und mobile Hotspots

Roaming

Einstellungen ▸ Mobiles Netz ▸ Datenoptionen ▸ Datenroaming

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. Nach dem Aufbrauchen der inkludierten Freieinheiten dürfen Roamingzuschläge verrechnet 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 für mobile Datendienste bei EUR 60,- (auch in Drittstaaten) eingerichtet sein. Dieser Grenzwert kann jedoch geändert oder ganz deaktiviert werden, wovor jedoch aus Kostengründen ausdrücklich gewarnt wird.



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 Aufenthalten 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 Roaming nicht bei allen Tarifen möglich ist.

Jailbreak

›Jailbreaking‹ ist das inoffizielle Entsperren von Software und Hardware. Aus Sicherheitsgründen wird empfohlen, darauf zu verzichten.

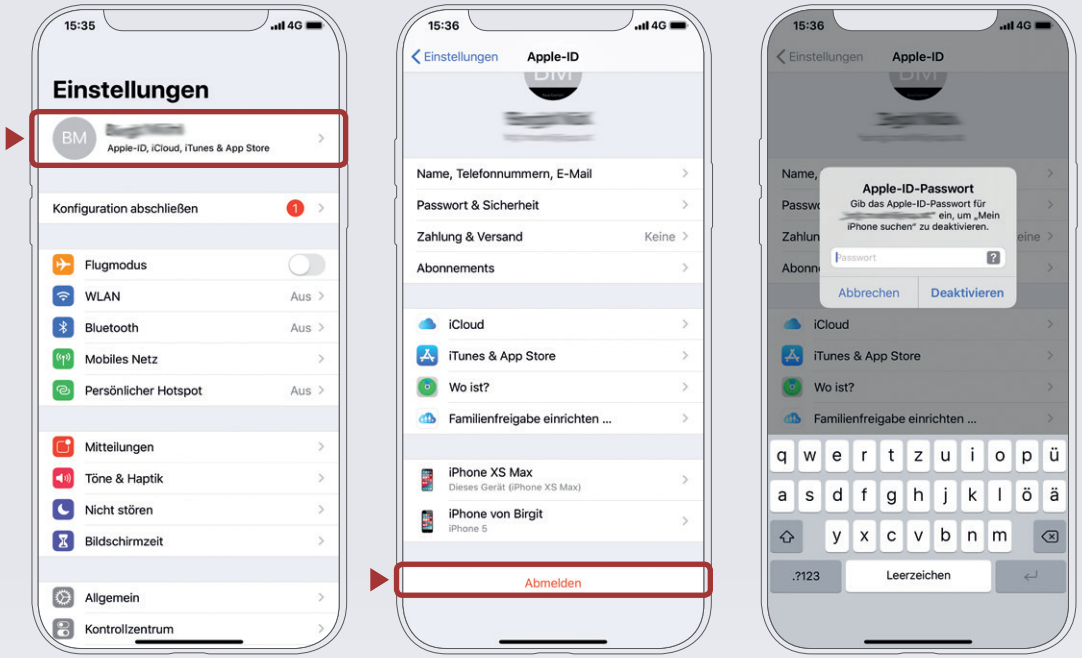
Das iPhone gerät mit seinem geschlossenen Betriebssystem immer wieder in die Kritik, da zum Beispiel keine Apps installiert werden können, die nicht im offiziellen App-Store erhältlich sind. Mit dem sogenannten ›Jailbreak‹ können diese und ähnliche Einschränkungen zwar umgangen werden, allerdings sollte man sich bewusst sein, dass dies mit erheblichen Nachteilen und potenziellen Gefahren verbunden ist.
Durch den Jailbreak kann das Betriebssystem beeinträchtigt oder sogar beschädigt werden und bei der Nutzung des Gerätes kann es zu Problemen, z. B. mit der Akkulaufzeit, kommen. Ebenso können nach dem Jailbreak unter Umständen Software-Updates des Geräteherstellers nicht mehr so einfach eingespielt werden. Dies stellt ein erhebliches Sicherheitsrisiko dar und erhöht die Gefahr potenzieller Angriffe durch Schadsoftware. Ungeübte Nutzerinnen und Nutzer können auch Opfer von ›falschen‹ Jailbreak-Programmen werden. Zudem fällt Jailbreaking in eine rechtliche Grauzone und kann die Garantie beeinträchtigen. Aus diesen Gründen empfiehlt es sich für die meisten Nutzerinnen und Nutzer, darauf zu verzichten.

Verkaufen, Verschenken & Verborgen

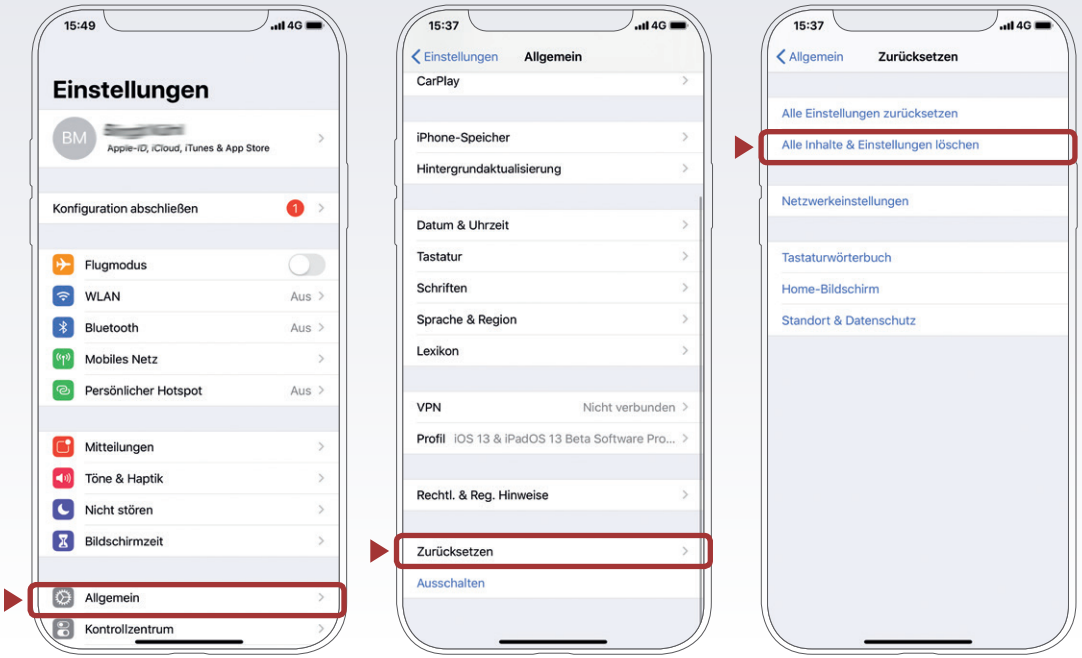
E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem iPhone sind sehr viele persönliche Daten gesammelt. Soll das iPhone weitergegeben oder verkauft werden, sollte das Gerät unbedingt auf den Werkzustand zurückgesetzt werden, um alle Daten zu löschen. Außerdem muss das iCloud-Konto vom iPhone abgemeldet werden.

Auf Werkzustand zurücksetzen/Daten löschen

Vor dem Zurücksetzen sollte auf jeden Fall eine Abmeldung vom iCloud-Konto vorgenommen werden. Dazu in der ›Einstellungen‹-App oben auf den eigenen Namen tippen. Ganz am Ende findet sich die Schaltfläche ›Abmelden‹. Es empfiehlt sich zudem, ein Backup anzulegen, bevor die Daten vom Gerät gelöscht werden.



Einstellungen ▸ Allgemein ▸ Zurücksetzen ▸ Alle Inhalte & Einstellungen löschen



›Mein iPhone suchen‹: Das iPhone finden, sperren und löschen

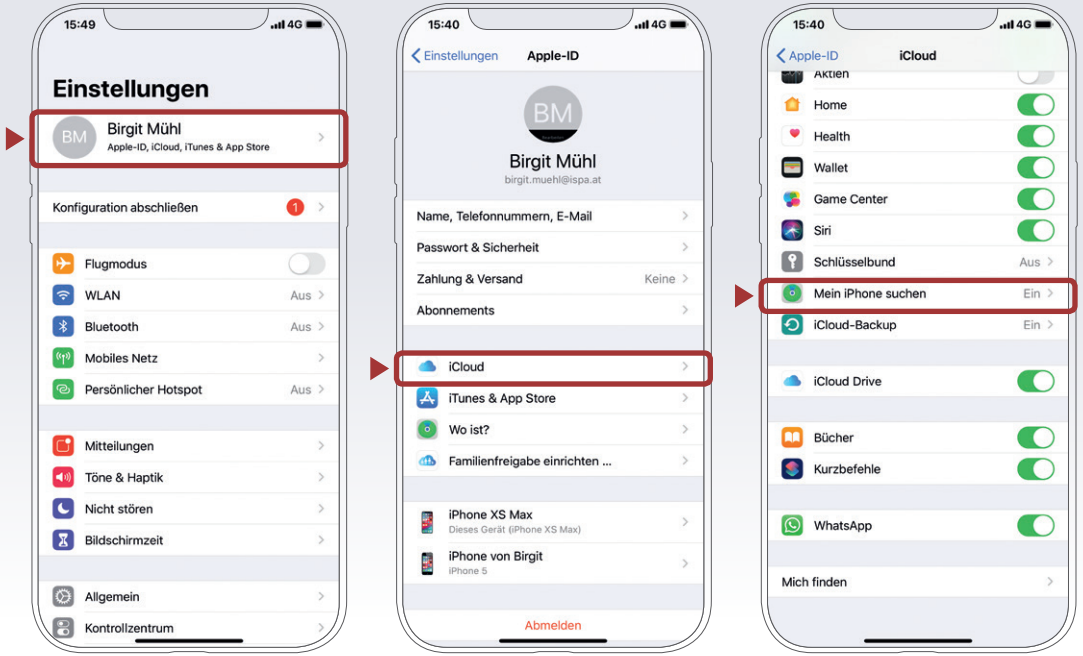
Die meisten Smartphones bieten mittlerweile die Möglichkeit, es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen.

Apple hat hierzu die ›Mein iPhone suchen‹-Funktion integriert. Ist die Funktion auf dem iPhone aktiviert, ist die (ungefähre) Position des Smartphones über die iCloud einsehbar. Außerdem kann eine Nachricht an das Telefon gesendet oder eine Löschung aller Daten vorgenommen werden. Hierfür müssen sich Nutzerinnen und Nutzer bei icloud.com mit ihrer Apple-ID anmelden.

Es gilt aber bei dieser Funktion zwischen Privatsphäre und Sicherheit abzuwägen: Soll diese Funktionen aktiviert sein, muss auch das GPS-Tracking des Ortungsdienstes aktiviert sein.

Aktivierung von ›Mein iPhone suchen‹

Einstellungen ▸ Apple-ID ▸ iCloud ▸ Mein iPhone suchen ▸ aktivieren



Diebstahl

Bei Diebstahl und Verlust sollte auch sofort der Netzbetreiber informiert werden, damit die SIM-Karte gesperrt wird. In den meisten Fällen haften die Nutzerinnen und Nutzer für anfallende Kosten bis zur Meldung an den Netzbetreiber. Eine Diebstahlsanzeige bei der Polizei sollte ebenfalls so schnell wie möglich gemacht werden. Zur Vorbereitung einer etwaig notwendigen Verlust- oder Diebstahlsanzeige sollte man vorsorglich die IMEI (International Mobile Equipment Identity) parat haben. Die IMEI ist eine 15-stellige Nummer, mittels derer ein GSM/UMTS/LTE-Endgerät wie ein Smartphone weltweit identifiziert werden kann. Sie steht auf der Verpackung des Endgeräts oder kann über die Tastenkombination *#06# abgerufen und notiert werden.

Um das Smartphone bei Bedarf kindersicher zu machen, bietet iOS eine Reihe an Einschränkungen, die bei Bedarf aktiviert werden können. So lässt sich etwa der Zugriff auf Apps, Filme und Webseiten über Alterseinstufungen begrenzen, es ist möglich, die Kamera oder den Browser zu deaktivieren, und die Installation neuer Apps bzw. der Kauf von zusätzlichen Inhalten (›In-App-Käufe‹) kann ebenfalls unterbunden werden.

Erziehungsberechtigte sollten allerdings bedenken, dass Medienerziehung nicht an Software delegiert werden kann. Besonders wichtig ist es, mit den Kindern über ungeeignete Inhalte und Online-Gefahren zu sprechen und ganz generell die Medienkompetenz der jüngsten Userinnen und User zu fördern. Ebenso sollten Eltern – und ältere Geschwister – bedenken, dass sie eine Vorbildfunktion haben, denn Kinder ahmen gerne das Verhalten von Älteren nach.

Die hier vorgestellten Funktionen sind aber nicht nur für die Geräte von Kindern anwendbar, auch Erwachsene können diese als nützlich empfinden.

Bildschirmzeit aktivieren

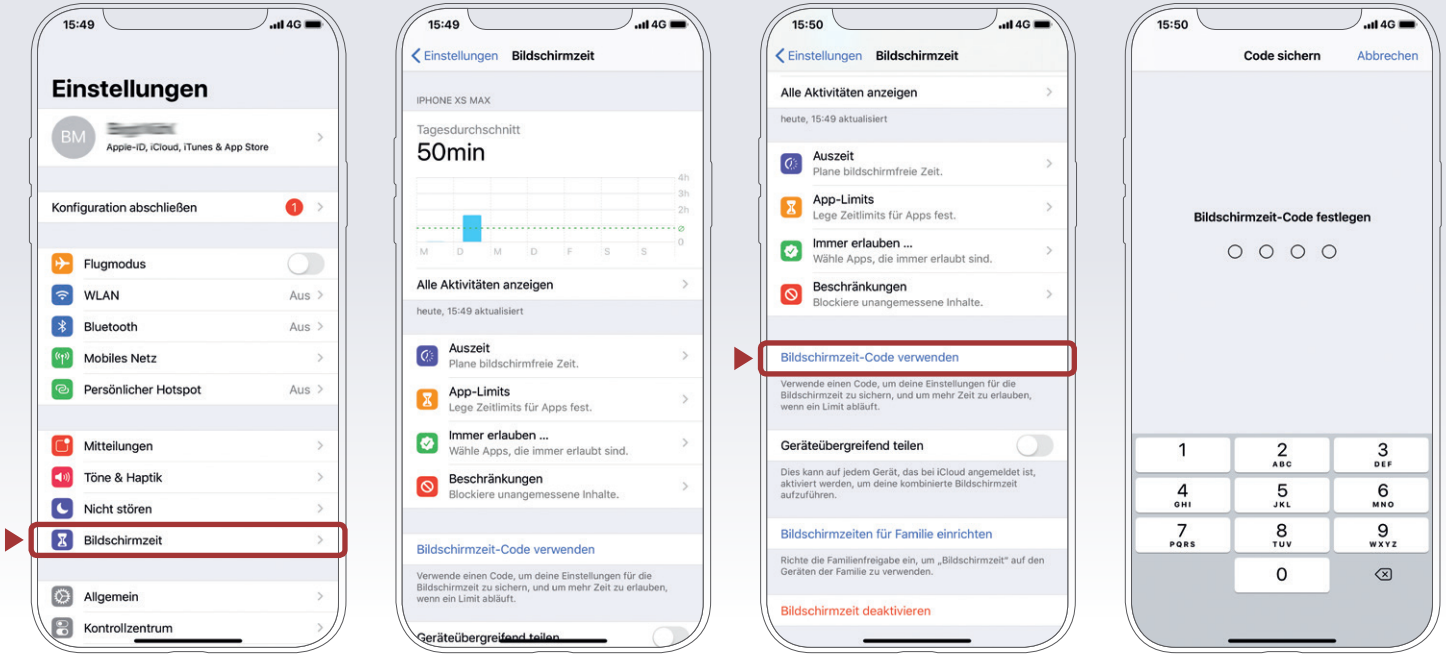
Einstellungen ▸ **Bildschirmzeit** ▸
Bildschirmzeit-Code verwenden ▸ **Code eingeben**

Nach Vergabe eines ›Bildschirmzeit-Codes‹ (ein vierstelliger Code, mit dem diese Einstellungen geschützt werden) lässt sich eine Vielzahl an Einstellungen treffen. So können etwa eine zeitliche digitale Auszeit und bestimmte App-Limits eingerichtet werden.

Der Zugriff auf einzelne Apps, z. B. den Browser Safari, die Kamera oder den Sprachassistenten Siri, kann unterbunden werden, es ist möglich, den iTunes Store zu sperren oder zu verhindern, dass Kinder Apps installieren bzw. löschen können. Auch die vollständige Deaktivierung von In-App-Käufen ist möglich.

Apps und Inhalte wie Musik, Filme und Webseiten können mit Alterseinschränkungen versehen werden. Diese Filter bieten naturgemäß keinen absoluten Schutz, sie können aber dabei helfen, nicht kindgerechte Inhalte auf dem Gerät zu unterbinden.

Zudem lassen sich die Datenschutzeinstellungen des Geräts (siehe Kapitel ›Datenschutzeinstellungen‹) gegen Änderungen schützen. So ist es zum Beispiel möglich, neu installierten Apps keinen Zugriff auf die Kontakte oder die Ortungsdienste zu gewähren.

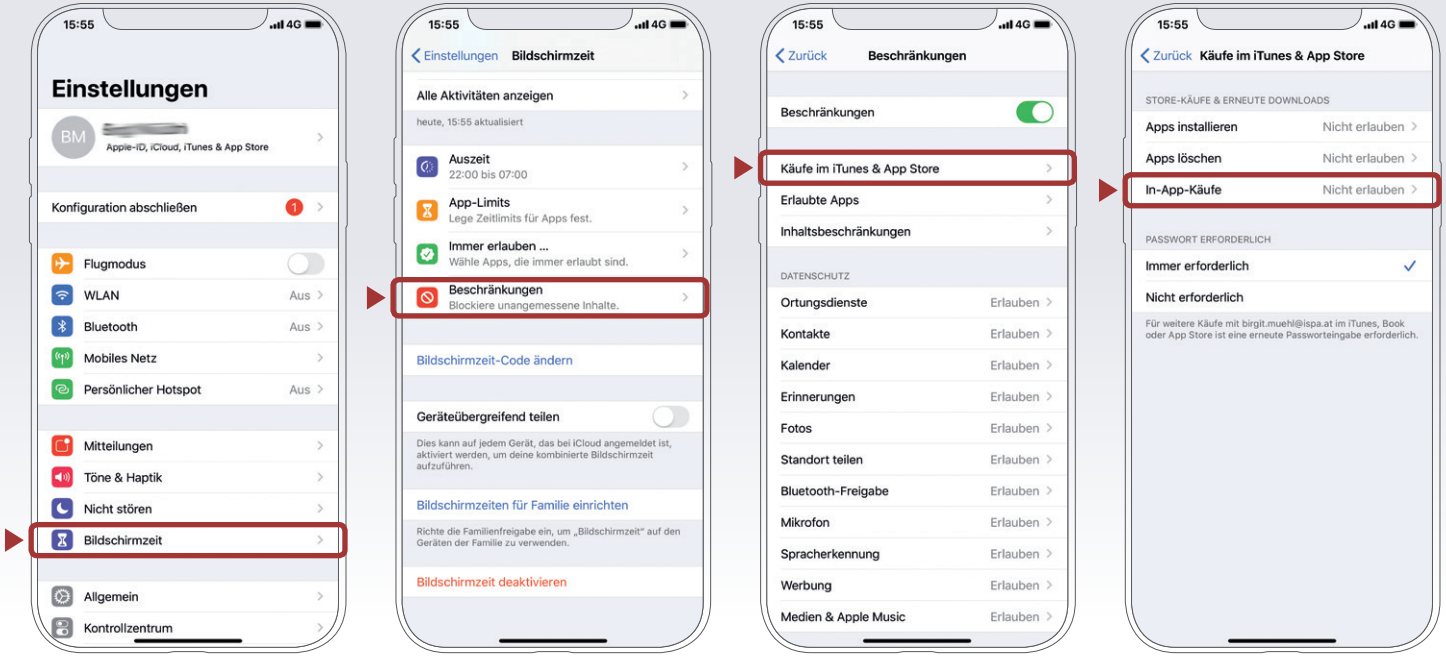


Das kindersichere Smartphone

In-App-Käufe

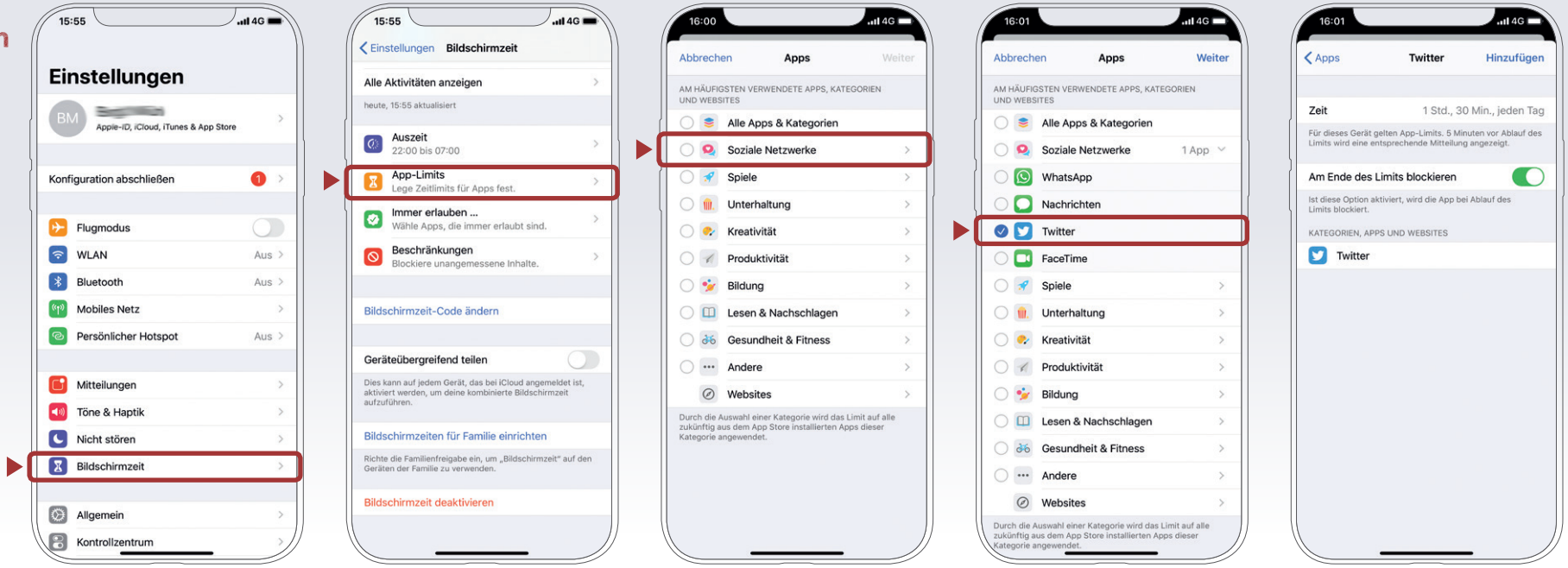
Einstellungen ▸ Bildschirmzeit ▸ Beschränkungen ▸ Käufe im App Store ▸ In-App-Käufe ▸ Erlauben bzw. nicht erlauben

Bei iOS können In-App-Käufe in den Einstellungen ganz ausgeschaltet werden.



Zeitbeschränkungen für Apps

Einstellungen ▸ Bildschirmzeit ▸ App-Limits ▸ Limit hinzufügen ▸ Kategorie auswählen ▸ App auswählen



Geführter Zugriff

Einstellungen ▸ Bedienungshilfen ▸ Geführter Zugriff

Beim geführten Zugriff wird nur Zugriff auf eine einzige App erlaubt. Diese Funktion ist sinnvoll, wenn man das iPhone kurzfristig einem Kind oder Dritten überlässt, die nicht Zugriff auf andere Funktionen oder Informationen haben sollen. In den Einstellungen muss der geführte Zugriff zuerst erlaubt werden. Danach kann er durch 3-fach-Klick auf die Seitentaste aktiviert werden. Zum Beenden muss ein 6-stelliger Code eingegeben werden, den man entweder vorher in den Einstellungen festlegt oder direkt beim Aktivieren angeben kann.

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.

Notizen

Notizen

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