

Sicherheitseinstellungen für Smartphones



Saferinternet.at
Das Internet sicher nutzen!

isp**a**
Internet Service Providers Austria

Inhaltsverzeichnis

1. Passwortschutz am Smartphone	1
2. Software-Updates des Geräteherstellers	2
3. Synchronisierung & Backups	3
4. Apps! Nur, wie richtig?	5
5. Virens Scanner	6
6. Kostenfalle In-App-Käufe	7
7. Kostenfalle Datentarife	7
8. WLAN, Bluetooth und mobile Hotspots	8
9. Jailbreak, Root und gesperrte Smartphones	10
10. Verkaufen, Verschenken & Verborgen	10
11. Smartphone-Finder: finden oder sperren	11
12. Das kindersichere Smartphone	11

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
3. aktualisierte Auflage.

Inhaltliche Verantwortung: Daniela Drobna

Endgerät: iPhone 5

BS: iOS 7.0.3

Apple, iPhone, iPad, iCloud und iTunes sind eingetragene Marken der Apple Inc., USA.

Gefördert durch die Europäische Union – Safer Internet Projekt

Alle Angaben erfolgen ohne Gewähr.

Eine Haftung der Autorinnen und Autoren, durch die ISPA oder das Projekt Saferinternet.at ist ausgeschlossen.

Wien, Februar 2014

95% aller Österreicherinnen und Österreicher nutzen ein Mobiltelefon. Davon besitzt die Hälfte ein Smartphone, die Tendenz ist stetig steigend. Durch die höhere Verbreitung und das ständig wachsende Angebot an Nutzungsmöglichkeiten wird das Smartphone immer mehr zu einem personalisierten Gerät mit hoch sensiblen Informationen. Persönliche Daten wie z.B. das Adressbuch mit allen Kontakten oder private und geschäftliche E-Mail-Accounts sind ein „best of“ all jener Daten, die unser Leben bestimmen. Umso mehr gilt es ein paar Verhaltensrichtlinien einzuhalten, die vor allem im Falle eines Verlustes oder Diebstahls hilfreich sind.

1. Passwortschutz am Smartphone

Mittlerweile gibt es bei jedem Smartphone die Möglichkeit das Gerät mittels Passwort zu schützen. Die meisten Smartphones bieten hier 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). Ersteres ist eine Standardeinstellung und sollte keinesfalls aus Bequemlichkeit abgeschaltet werden. Es ist aber auch ratsam, ebenfalls eine Bildschirmsperre zu verwenden – es erscheint zwar zeitaufwendig jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz Ihres Smartphones bzw. Ihrer Daten bei.

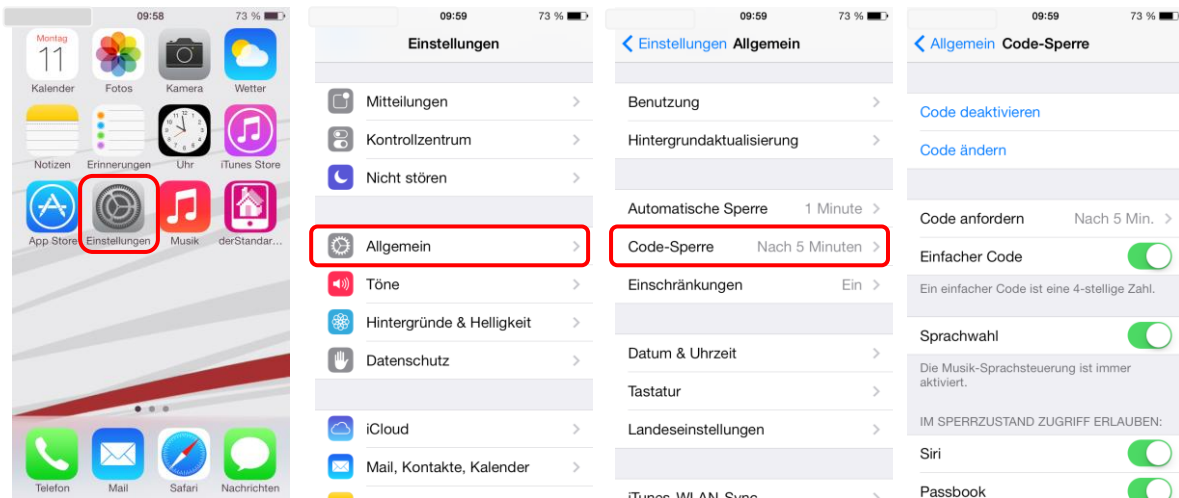
Bei manchen iPhones kann die PIN-Abfrage beim Einschalten des Gerätes deaktiviert sein. Umso wichtiger ist es, den optionalen Passwortschutz zur Aufhebung des Ruhezustandes „Code Sperre“ zu verwenden. Hierbei haben Sie die Wahl zwischen dem „einfachen Code“, der aus einer vierstelligen Zahlenkombination besteht, oder Sie verwenden einen alphanumerischen Code, welcher sich aus einer Zahlen- und Buchstabenkombination zusammensetzt. Durch die Code Sperre wird ihr Gerät gleich mehrfach geschützt. Zur Code-Eingabe werden Sie nun aufgefordert wenn Sie

- das iPhone einschalten oder neu starten
- den Ruhezustand aufheben
- die Anzeigensperre deaktivieren

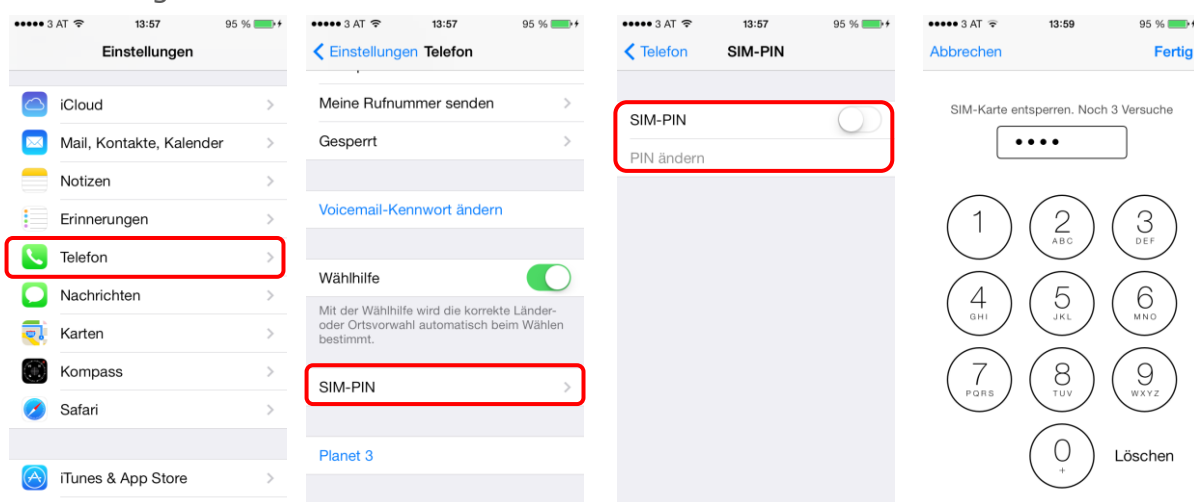
Weiters können Sie bei Ihrem iPhone einstellen, dass die darauf vorhandenen Daten nach zehn fehlgeschlagenen Anmeldeversuchen automatisch gelöscht werden.

Zudem haben Sie beim iPhone die Möglichkeit, einzelne Anwendungen und Apps mittels eines zusätzlichen – also anderen – Codes einzuschränken. Hier können Sie unter dem Menüpunkt „Einschränkungen“ z.B. das Kaufen von Apps deaktivieren oder „anstößige Sprache“ ausblenden lassen, sodass die Spracherkennungssoftware (Siri) diese mit einem Stern oder Piepton ersetzt.

Codesperre beim iPhone: Einstellungen – Allgemein – Code-Sperre



Aktivierung der SIM-Kartensperre: Einstellungen – Telefon – SIM-PIN



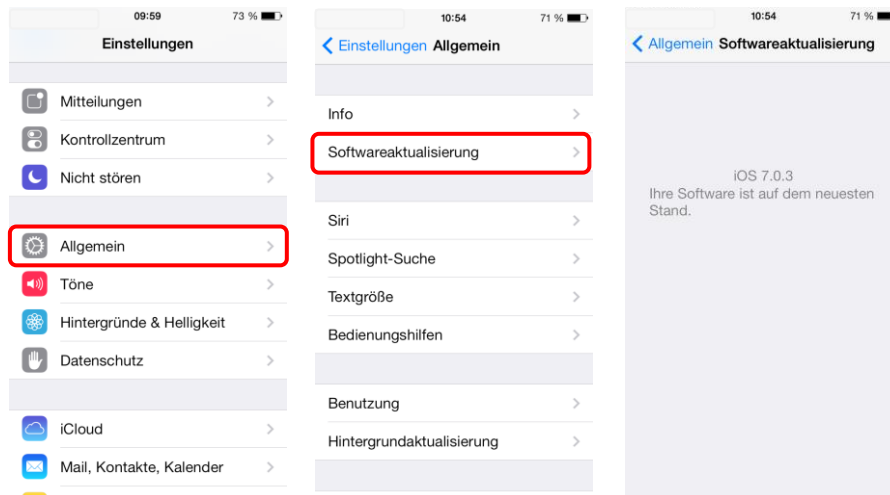
2. Software-Updates des Geräteherstellers

Führen Sie regelmäßig die vom Hersteller empfohlenen Software-Updates für Ihr Smartphone durch. Software-Updates enthalten kleine Systemverbesserungen, sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Smartphone-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.

Üblicherweise sucht Ihr iPad bei bestehender Internetverbindung automatisiert nach Updates und macht Sie gegebenenfalls darauf aufmerksam.

Suche nach Software-Updates:

Einstellungen – Allgemein – Softwareaktualisierung



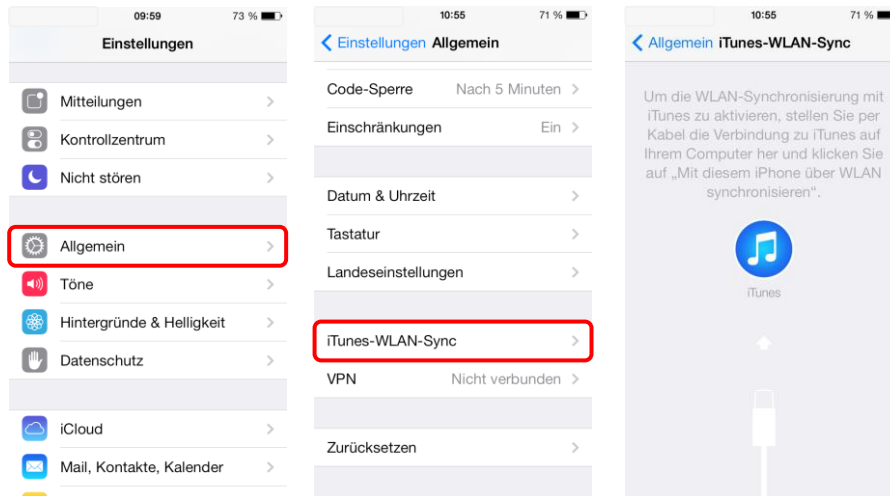
3. Synchronisierung & Backups

Genau wie bei einem PC ist es auch bei einem Smartphone notwendig, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Daten- oder Handyverlusts können Sie so auf Ihr Backup zugreifen und haben zumindest den letzten Stand Ihrer gesicherten Daten verfügbar.

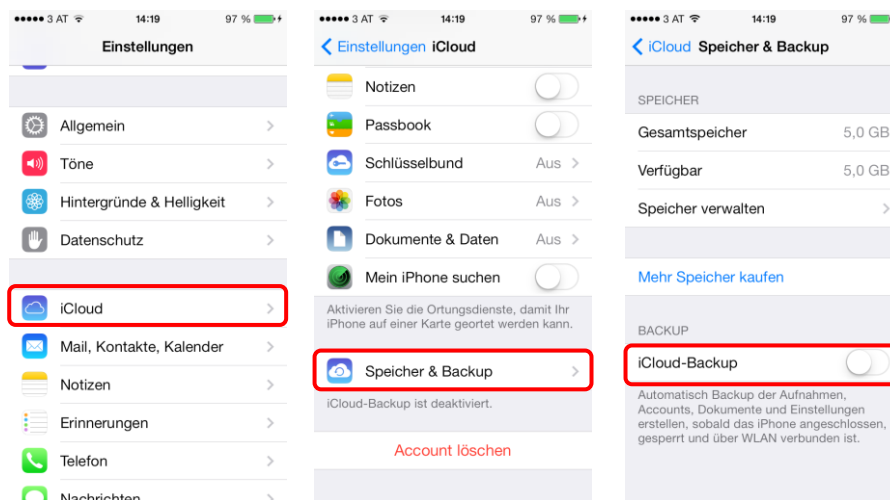
Apple bietet mit der Funktion „iCloud“ die Möglichkeit sich vor Datenverlust zu schützen, indem bestimmte Daten im Cloud-Service von Apple gespeichert werden. Sie können genau festlegen, welche Ihrer Daten in der iCloud abgelegt werden sollen (z.B. Fotodateien, Notizen, Kontakte etc.). Sie können von überall auf Ihre Daten zugreifen und benötigen lediglich Ihr Apple-Konto, welches Sie beim ersten Einrichten des iPhones angelegt haben. Zusätzlich können Sie mit der iCloud-App Ihre Daten automatisch auf Ihren Geräten synchronisieren lassen.

Ihre Daten werden aber nicht auf dem Endgerät gesichert, sondern in einem externen Cloud-Service. Das birgt gewisse Sicherheitsrisiken – von Datenschutz, -integrität und -sicherheit – die Sie bedenken sollten.

Synchronisierung von iPhone und PC: Einstellungen – Allgemein – iTunes-Wlan-Sync



Aktivierung von iCloud: Einstellungen – iCloud – Speicher & Backup



4. Apps! Nur, wie richtig?

Ein Smartphone ohne Apps ist wie Winter ohne Schnee – einfach nicht das Wahre. Jedoch können die kleinen Anwendungen genutzt werden um in Ihr Smartphone und somit an Ihre Daten zu gelangen: diese schädlichen Apps heißen „Malware“. Wenn Sie beim Kauf und Download von Apps ein paar wenige Punkte beachten, können Sie ganz leicht dieses Sicherheitsrisiko minimieren.

Beziehen Sie Apps nur aus den offiziellen App-Stores!

Natürlich kann es auch hier keine endgültige Garantie geben, aber die offiziellen Stores von Apple (App Store: <http://itunes.apple.com>), von Android (Google Playstore: <http://play.google.com>) und Windows (Windows Phone Store: <http://.windowsphone.com/store>) sind definitiv vertrauenswürdiger als andere.

Die iPhone-Apps können lediglich über den App Store von Apple erworben werden (sofern diese Sperre nicht durch einen „Jailbreak“ umgangen wurde – siehe Punkt 9). Das iOS Betriebssystem für iPhones ist ein geschlossenes System und somit prinzipiell relativ sicher.

Beim App Store von Apple können Sie über eine Inhaltsfilterung den Zugriff auf bestimmte Apps unter dem Menüpunkt „Einschränkungen“ begrenzen (z.B. Apps mit nicht jugendfreien Inhalten).

Geben Sie (schlechte) Apps zurück!

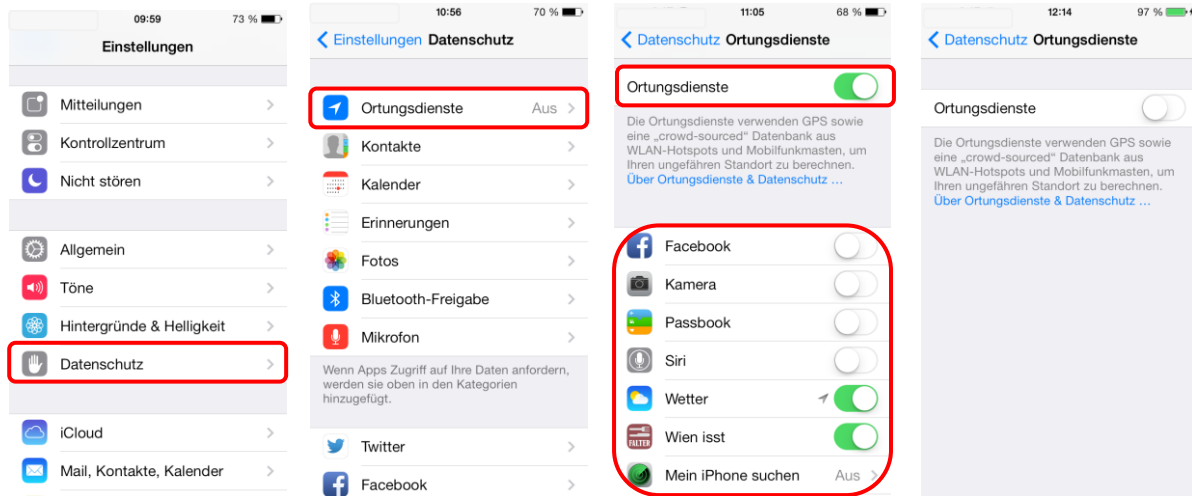
Beim App Store von Apple ist die Rückgabe nicht ganz so einfach, da Apple strenge Verkaufsbedingungen hat. Es besteht dennoch die Möglichkeit über Ihre Einkaufsstatistik im App Store mittels der Funktion „Problem melden“ eine Rückgabe unter Angabe des Grundes zu beantragen.

Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

Vor der endgültigen Installation einer App müssen Sie deren Zugriffsberechtigungen zustimmen. Seien Sie hier vorsichtig und stimmen Sie Berechtigungen nur dann zu, wenn diese notwendig erscheinen. Böartige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen, die einerseits nicht notwendig sind und andererseits Ihr Smartphone und Ihre Daten angreifbar machen. Handelt es sich zum Beispiel um eine Game-App, braucht diese auch keinen Zugriff auf Ihr Telefonbuch.

Wählen Sie ganz bewusst aus, welche Daten Sie welcher App zur Verfügung stellen wollen. Beispielsweise können Sie vorsehen, dass GPS-Daten Programmen wie einem Navigationssystem oder Routenplaner vorbehalten bleiben. Warum sollten Sie einer App Zugriff zu Daten gestatten, wofür staatliche Einrichtungen in der Regel eine richterliche Anordnung brauchen?

Deaktivierung von GPS-Daten-Übermittlung: Einstellungen – Datenschutz – Ortungsdienste



Achtung: Bei einigen Smartphones reicht es aber nicht, lediglich die allgemeine Positions-Daten-Übermittlung zu deaktivieren. Oftmals gibt es noch einen gesonderten Unterpunkt für die Kamera des Geräts. Obwohl Sie die allgemeine Positions-Daten-Übermittlung abgedreht haben, kann es dennoch sein, dass Sie weiterhin Ihren Aufenthaltsort bekannt geben: und zwar beim Aufnehmen und Versenden von Fotos. Um auch das zu deaktivieren müssen sie in den Kameraeinstellungen das „Geo-Tagging“, also das automatische Einbetten des Standorts zum Zeitpunkt der Aufnahme in die Fotodatei oder das Versehen der Fotos mit einem „Geotag“, deaktivieren. Beim iPhone können Sie dies ebenfalls unter dem Menüpunkt „Ortungsdienste“ deaktivieren.

5. Virenschanner

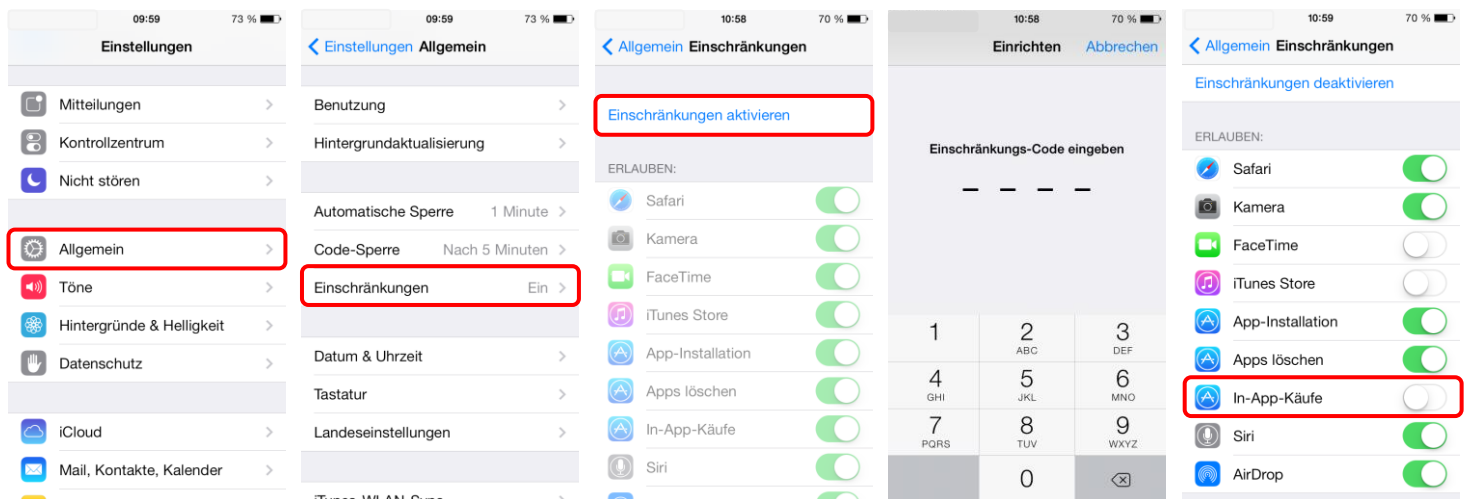
Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Handy-Banking bzw. Handy-Bezahlung verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Smartphone nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren bzw. beseitigen diese wenn möglich. Für das iPhone gibt es von Apple selbst nach wie vor kein Virenschutzprogramm. Somit kann aus dem großen Pool der angebotenen Virenschutzprogramme ausgewählt werden. Wenn Sie die Sicherheit Ihrer Daten erhöhen möchten, sollten Sie sich auf jeden Fall eine Virenschanner-App zulegen. Speziell beim Kauf eines Virenschanners empfiehlt es sich natürlich, besonders aufmerksam und auf Ihre persönlichen Bedürfnisse abgestimmt auszuwählen!

6. Kostenfalle In-App-Käufe

Bei manchen Apps (z.B. Spielen) besteht die Möglichkeit unbeabsichtigt in den Anwendungen Guthaben oder Punkte zu kaufen, ohne den klassischen Bestellvorgang zu durchlaufen (so genannte „In-App-Käufe“). Damit steigt die Gefahr unbeabsichtigt Geld auszugeben. In-App-Käufe können leicht zur unvorhergesehenen Kostenfalle werden: Besonders Kindern und Jugendlichen ist oft nicht bewusst, dass sie auf ein kostenpflichtiges Angebot klicken, wenn sie zum Beispiel zusätzliches Spielguthaben erwerben um in einem Spiel schneller voranzukommen. Deaktivieren Sie deswegen die In-App-Käufe auf Ihrem Smartphone und schalten Sie diese nur im Bedarfsfall und somit gezielt frei.

Sperre der In-App-Käufe:

Einstellungen – Allgemein – Einschränkungen –
Einschränkungen aktivieren – In-App-Käufe



7. Kostenfalle Datentarife

Viele Smartphone-Nutzerinnen und -Nutzer haben Handyverträge mit einem limitierten Internet-Paket, pro Monat können sie somit ein bestimmtes Datenvolumen verbrauchen. Wird dieses überschritten, wird es meistens teuer. Wenn Sie einen Datentarif mit begrenztem Internetvolumen haben, empfiehlt es sich den eigenen Verbrauch im Auge zu behalten.

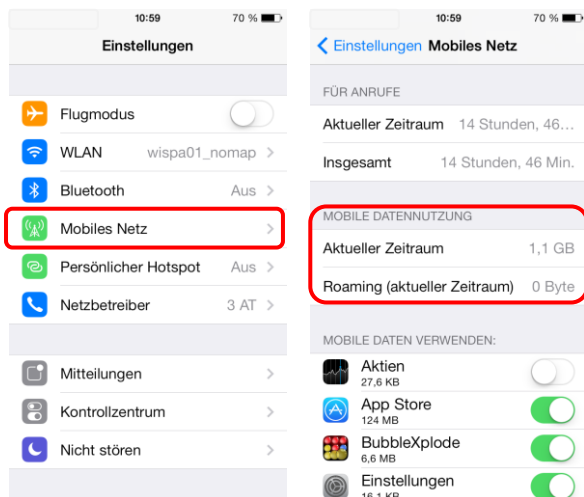
Sollten Sie bei der Einschätzung Ihres Datenverbrauchs unsicher sein, können Sie sich für Ihr Smartphone eine App zur Kontrolle des Datenvolumens downloaden. Mittlerweile bieten die meisten Mobilfunkanbieter derartige Apps zur Volumen- und Kostenkontrolle auch schon gratis an. Bitte beachten Sie aber bei allen Lösungen, dass diese Programme keine endgültige Genauigkeit haben. Sollten Sie also sehr

knapp an Ihrem Datenlimit angelangt sein, verzichten Sie lieber auf den weiteren Verbrauch um so Extrakosten zu vermeiden. Zur Reduktion des Datenverbrauchs empfiehlt es sich auch Hintergrundsynchrosationen abzuschalten. Um Ihr limitiertes Internet-Paket zu schonen, sollten Sie Updates und Synchronisierungen manuell über verfügbare WLAN-Netzwerke durchführen.

Das iPhone bietet zur Volumenkontrolle den Menüpunkt „Mobile Datennutzung“, bei dem der eigene Verbrauch ermittelt werden kann.

Kontrolle des Datenvolumens:

Einstellungen – Mobiles Netz – Mobile Datennutzung



8. 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 zwar 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. Sie sollten die WLAN- und Bluetooth-Funktion nur dann einschalten, wenn Sie auf ein lokales WLAN-Netzwerk zugreifen wollen, oder Sie die Bluetooth-Funktion unmittelbar benötigen. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist ein stark reduzierter Akku-Verbrauch.

WLAN und Bluetooth deaktivieren:

Einstellungen – Wlan

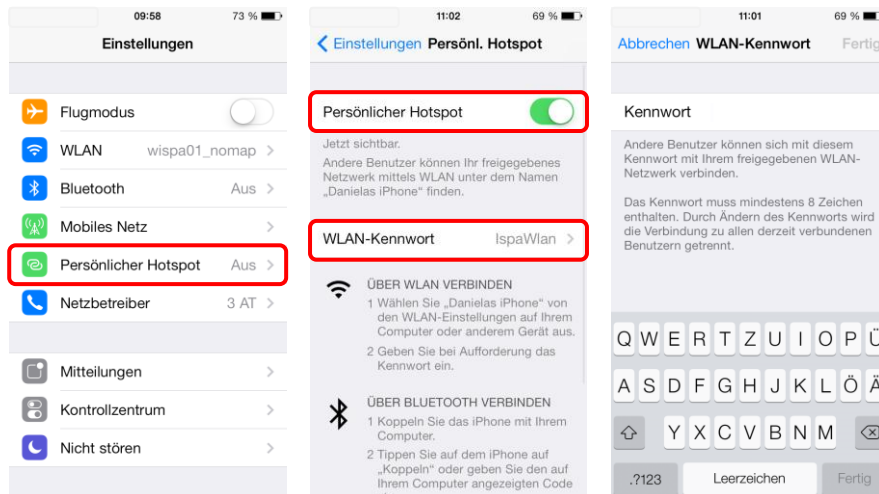
Einstellungen – Bluetooth



Viele Smartphones mit Datenverbindung bieten die Möglichkeit das Handy als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot für den eigenen Laptop zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort das aus Zahlen und Buchstaben besteht sichern und ebenfalls nur bei Bedarf aktivieren.

WLAN-Hotspot:

Einstellungen – Persönlicher Hotspot



9. Jailbreak, Root und gesperrte Smartphones

„Jailbreaking“ ist das inoffizielle Entsperren von Software und Hardware, meint in den meisten Fällen aber das Entsperren von Smartphones. Gerade das sehr beliebte iPhone gerät mit seinem geschlossenen System immer wieder in die Kritik, da zum Beispiel keine Apps installiert werden können, die nicht im Apple Store erhältlich sind. 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. 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!

10. Verkaufen, Verschenken & Verborgern

E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: auf Ihrem Smartphone sind sehr viele persönliche Daten gesammelt. Sollten Sie sich dazu entschließen, Ihr Smartphone weiterzugeben oder es sogar zu verkaufen, sollten Sie Ihr Gerät unbedingt auf den Werkzustand zurücksetzen.

Auf Werkzustand zurücksetzen:

Einstellungen – Allgemein – Zurücksetzen



Um die Weitergabe Ihrer persönlichen Daten zu verhindern sollten Sie alle vorhandenen Speicher löschen. 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.

11. Smartphone-Finder: finden oder sperren

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

Apple hat hierzu die „Find my iPhone“-Funktion integriert. Ist die Funktion auf dem Gerät aktiviert, ist die (ungefähre) Position des Smartphones über die iCloud einsehbar.

Es gilt aber bei dieser Funktion zwischen Privatsphäre und Sicherheit abzuwägen: möchten Sie solche Funktionen nutzen, müssen Sie das GPS-Tracking aktivieren.

Aktivierung des Telefonfinders:

Einstellungen – Ort – Telefonfinder



12. Das kindersichere Smartphone

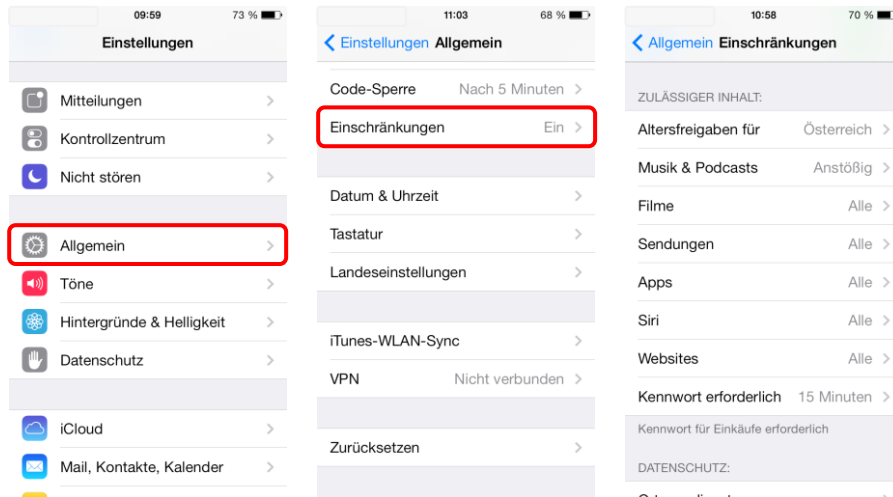
Um Ihr Smartphone bei Bedarf kindersicher zu machen, sollten Sie das Roaming sowie In-App-Käufe deaktivieren und ebenso Mehrwertdienste sperren. In letzter Konsequenz können Sie das Internet deaktivieren und in den Flugmodus wechseln.

Beim App Store können Sie über eine Inhaltsfilterung den Zugriff auf bestimmte Apps unter dem Menüpunkt „Einschränkungen“ begrenzen (z.B. Apps mit nicht jugendfreien Inhalten).

Mittlerweile gibt es auch zahlreiche Apps, die sich dem Thema Kindersicherheit widmen. Diese sind dann aber Endgerät-basiert und funktionieren primär über Sperren und Filter.

Einschränkungen:

Einstellungen – Allgemein – Einschränkungen



Achtung: Falls Sie die „Daten löschen“-Funktion aktiviert haben, sollten Sie bedenken, dass bei iPhones mit aktiver Code-Sperre nach zehnmöglicher Falscheingabe des Codes die gesamten Daten gelöscht werden! Sie sollten diese sicherheitshalber aufheben bevor Sie Ihr iPhone an Kinder weitergeben.