

Sicherheitseinstellungen für Tablets



Saferinternet.at
Das Internet sicher nutzen!

isp*pa*
Internet Service Providers Austria

Inhaltsverzeichnis

1. Passwortschutz am Tablet	1
2. Software-Updates des Geräteherstellers	2
3. Synchronisierung & Backups	3
4. Apps! Nur, wie richtig?	4
5. Virens Scanner	7
6. Kostenfalle In-App-Käufe	7
7. Kostenfalle Datentarife	8
8. WLAN, Bluetooth und mobile Hotspots	9
9. Jailbreak, Root und gesperrte Tablets	11
10. Datenverschlüsselung	12
11. Verkaufen, Verschenken & Verborgenen	13
12. Tablet-Finder: finden oder sperren	14
13. Das kindersichere Tablet	14

Impressum:

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

Inhaltliche Verantwortung: Daniela Drobna

Endgerät: Nexus 7

BS: Android 4.3

Android ist eine eingetragene Marke von Google Inc. Samsung ist eine eingetragene Marke von Samsung Corp.

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

56% aller Internetnutzerinnen und -nutzer surfen über mobile Geräte im Internet (Smartphone, Tablet etc.), davon besitzen bereits 17% ein Tablet (Quelle: Ipsos MediaCT, Studie Austria Connected Device Usage 1/13).

Die Multimediafähigkeit, das handliche Format und der schnelle Zugriff aufs Internet sind die Hauptgründe für die steigende Verwendung und den Kauf von Tablets. Wie das Smartphone, ist auch das Tablet ein hoch personalisiertes Gerät mit sensiblen und persönlichen Daten. Umso mehr gilt es ein paar Sicherheitseinstellungen vorzunehmen, die sich speziell im Falle eines Verlustes oder Diebstahls als hilfreich erweisen können.

1. Passwortschutz am Tablet

Wie auch beim Smartphone, gibt es die Möglichkeit das Tablet mittels Passwort zu schützen. Die meisten Geräte 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 (Bildschirm Sperre). Ersteres ist eine Standardeinstellung und sollte keinesfalls aus Bequemlichkeit abgeschaltet werden. Es ist aber auch ratsam, ebenfalls eine Bildschirm Sperre zu verwenden – es erscheint zwar zeitaufwendig jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz Ihres Tablets bzw. Ihrer Daten bei.

Bei der Bildschirm Sperre von Android-Tablets haben Sie für gewöhnlich mehrere Möglichkeiten:

- Gesichtserkennung: Face Unlock
- Musterentsperrung
- PIN-Eingabe
- Passwort-Eingabe

Die Gesichtserkennung hat die niedrigste Sicherheitsstufe. Hierbei scannt das Tablet Ihr Gesicht, sodass Sie dieses zum Entsperren lediglich in die Kamera des Tablets halten müssen. In der Praxis führen aber schlechte Lichtverhältnisse rasch zu einer Nicht-Erkennung und somit zu keiner Entsperrung. Bei dieser Art der Bildschirm Sperre wird daher zusätzlich auch ein PIN-Code verwendet, damit Sie notfalls bei Nicht-Erkennung zumindest per PIN-Code Ihr Gerät entsperren können.

Die Musterentsperrung ist vor allem bei Smartphones eine sehr beliebte Methode zum Schutz des Endgerätes. Die Musterentsperrung bewegt sich als Sicherheitsvorkehrung im mittleren Bereich, da sie unter Umständen leicht beobachtet oder nachvollzogen werden kann. Das Muster legen Sie auf einer 3 x 3-Punkte-Matrix (oder alternativ 4 x 4-Punkte-Matrix) als Verbindungslinie von mindestens vier Punkten fest. Zum

Entsperren fahren Sie dann nur noch auf dem Touchdisplay die vorher festgelegte Linie nach.

Die PIN-Eingabe ist der Klassiker beim Passwortschutz. Je nach Schwierigkeitsgrad der Zahlenkombination bietet sie mittlere bis hohe Sicherheit.

Die Passworteingabe weist die höchste Sicherheitsstufe auf, besonders wenn Sie sich für eine Zahlen-, Buchstaben- und Sonderzeichenkombination entscheiden.

Bildschirmsperre bei Android-Tablets:

Einstellungen – Sicherheit – Display-Sperre



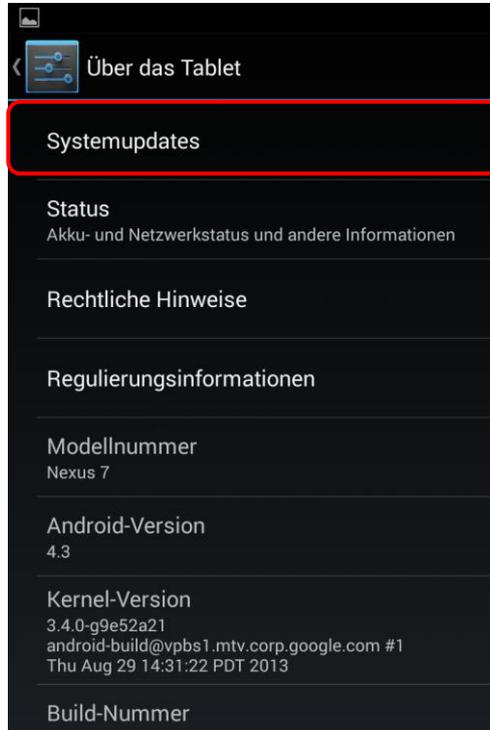
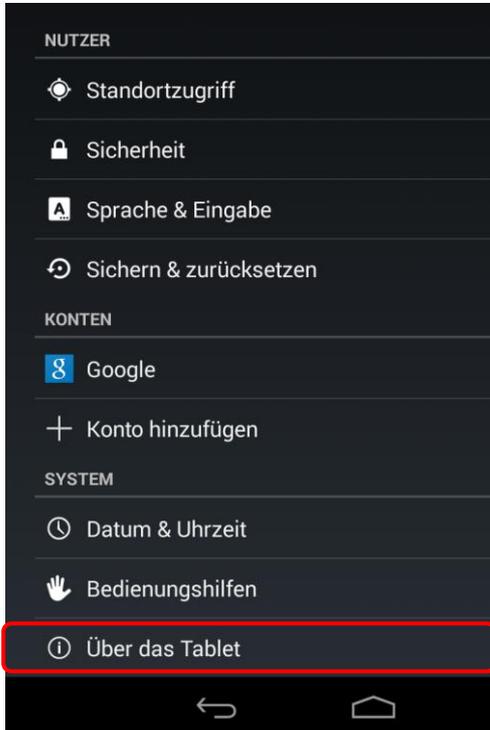
2. Software-Updates des Geräteherstellers

Führen Sie regelmäßig die vom Hersteller empfohlenen Software-Updates für Ihr Tablet durch. Software-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.

Sie können natürlich auch vorsehen, dass Ihr Tablet automatisch auf Software-Aktualisierungen überprüft und Sie gegebenenfalls darauf aufmerksam macht.

Software-Updates bei Android-Tablets:

Einstellungen – Über das Tablet – Systemupdates

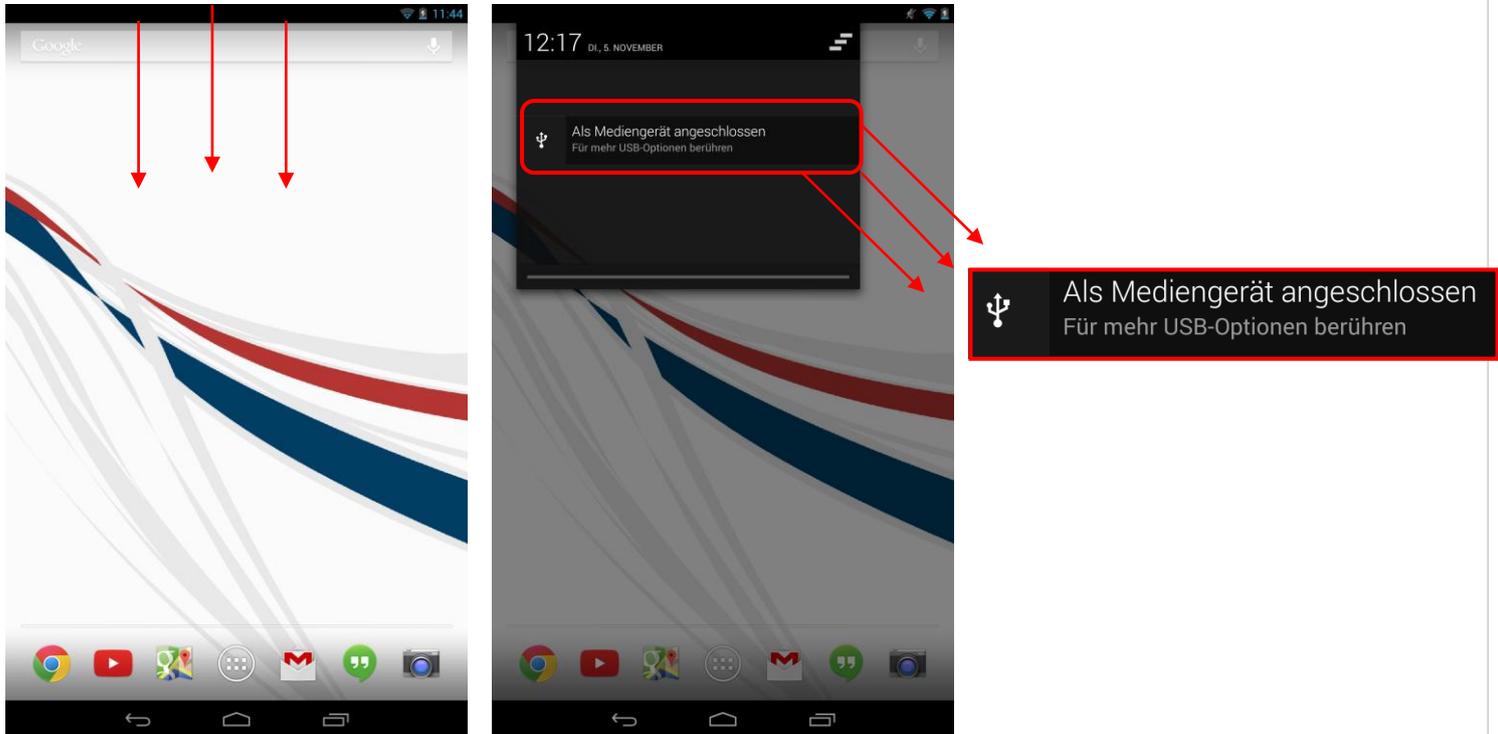


3. Synchronisierung & Backups

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

Synchronisierung von Android-Tablet und PC:

Startbildschirm – Bildschirm von oben nach unten ziehen - USB-Option wählen
(Verbinden Sie vorher das Tablet per USB-Kabel mit dem Pc)



Achtung: Blockieren Sie Hintergrundanwendungen! Bei Android synchronisieren sich Ihre Apps laufend im Hintergrund, außer Sie deaktivieren diese Funktion im Menüpunkt „Konten und Synchronisierung“.

4. Apps! Nur, wie richtig?

Ein Tablet ohne Apps ist noch weniger das Wahre als ein Smartphone ohne Apps. Jedoch können die kleinen Anwendungen auch hier genutzt werden um in Ihr Tablet 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!

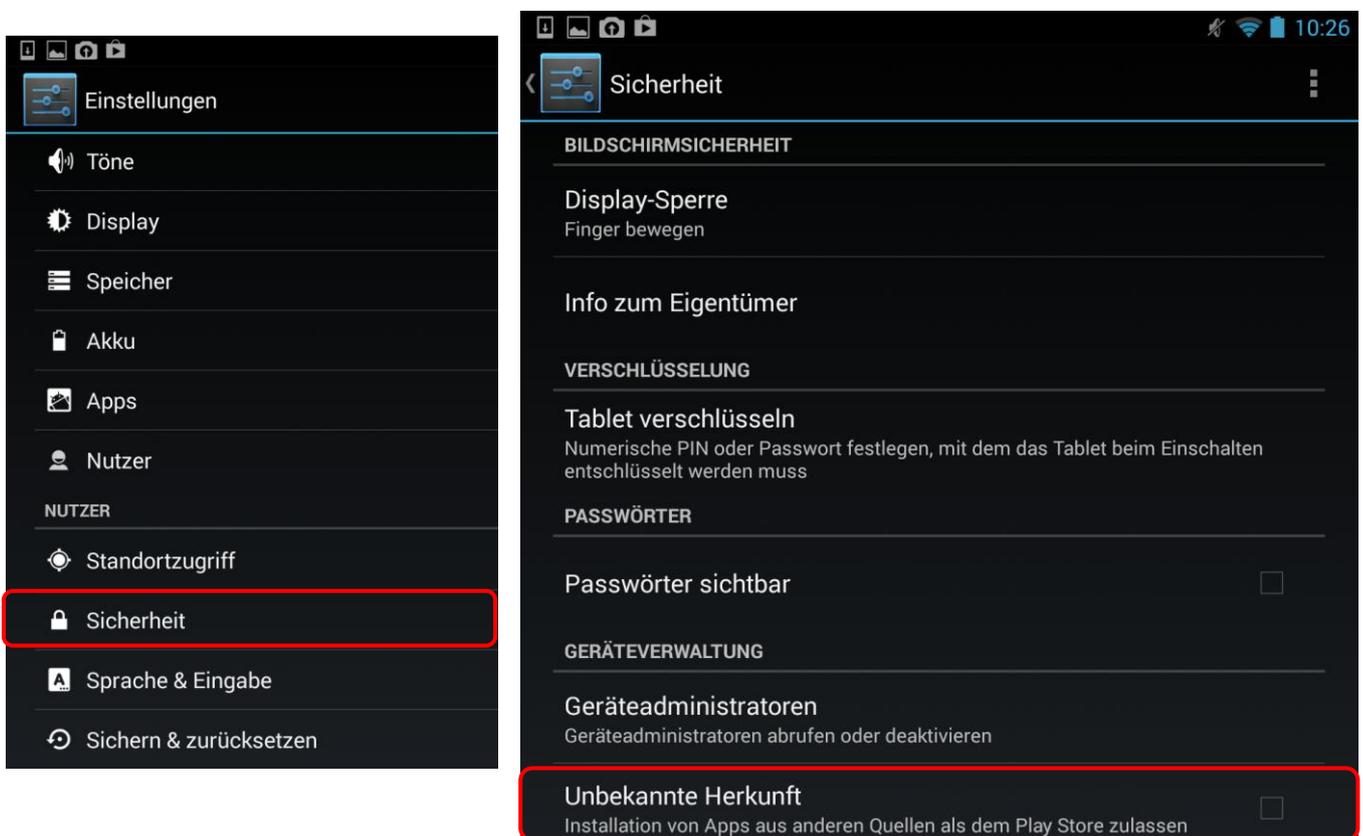
Natürlich kann es auch hier keine endgültige Garantie geben, aber die offiziellen Stores von Apple (App Store: <http://itunes.apple.com>), von Android (Google Playstore: <http://play.google.com>) und Windows (Windows Phone Store: <http://windowsphone.com/store>) sind definitiv vertrauenswürdiger als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

Beim Google Playstore können Sie außerdem in den Einstellungen den „Filter für Inhalte“ aktivieren. Hier beschränken Sie über eine Inhaltsfilterung den Zugriff auf Apps, die heruntergeladen werden können (z.B. Apps mit sexuellen Inhalten und Gewaltdarstellungen oder Apps welche Standortdaten der Nutzerinnen und Nutzer sammeln).

Bei Android können Apps auch aus anderen und somit fremden Quellen bezogen werden. Diese Möglichkeit der Installation von fremden, also Nicht-Market-Anwendungen, können Sie auf Ihrem Android-Tablet komplett sperren.

Sperre unbekannter Quellen bei Android:

Einstellungen – Sicherheit – Unbekannte Herkunft



Geben Sie (schlechte) Apps zurück!

Ein weiterer Vorteil des Kaufes über die offiziellen Stores ist, dass sie ein Rückgaberecht haben. Beim Google Playstore können Sie eine App innerhalb von 15 Minuten ab dem Erwerb problemlos und unbürokratisch durch die Deinstallation zurückgeben.

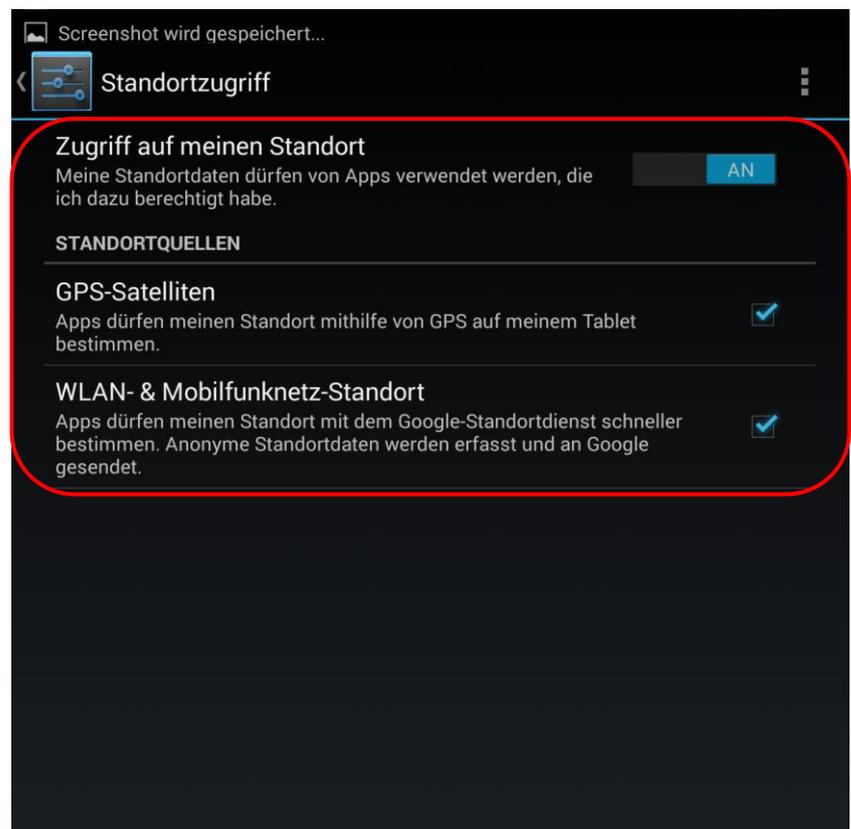
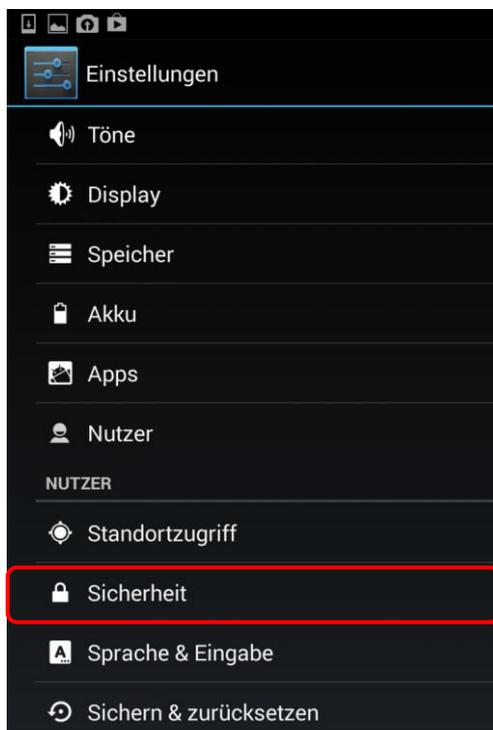
Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

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. Bösertige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen, die einerseits nicht notwendig sind und andererseits Ihr Tablet und Ihre Daten angreifbar machen. Handelt es sich zum Beispiel um eine Game-App, braucht diese 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 bei Android:

Einstellungen – Standortzugriff



Achtung: Bei einigen Tablets 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.

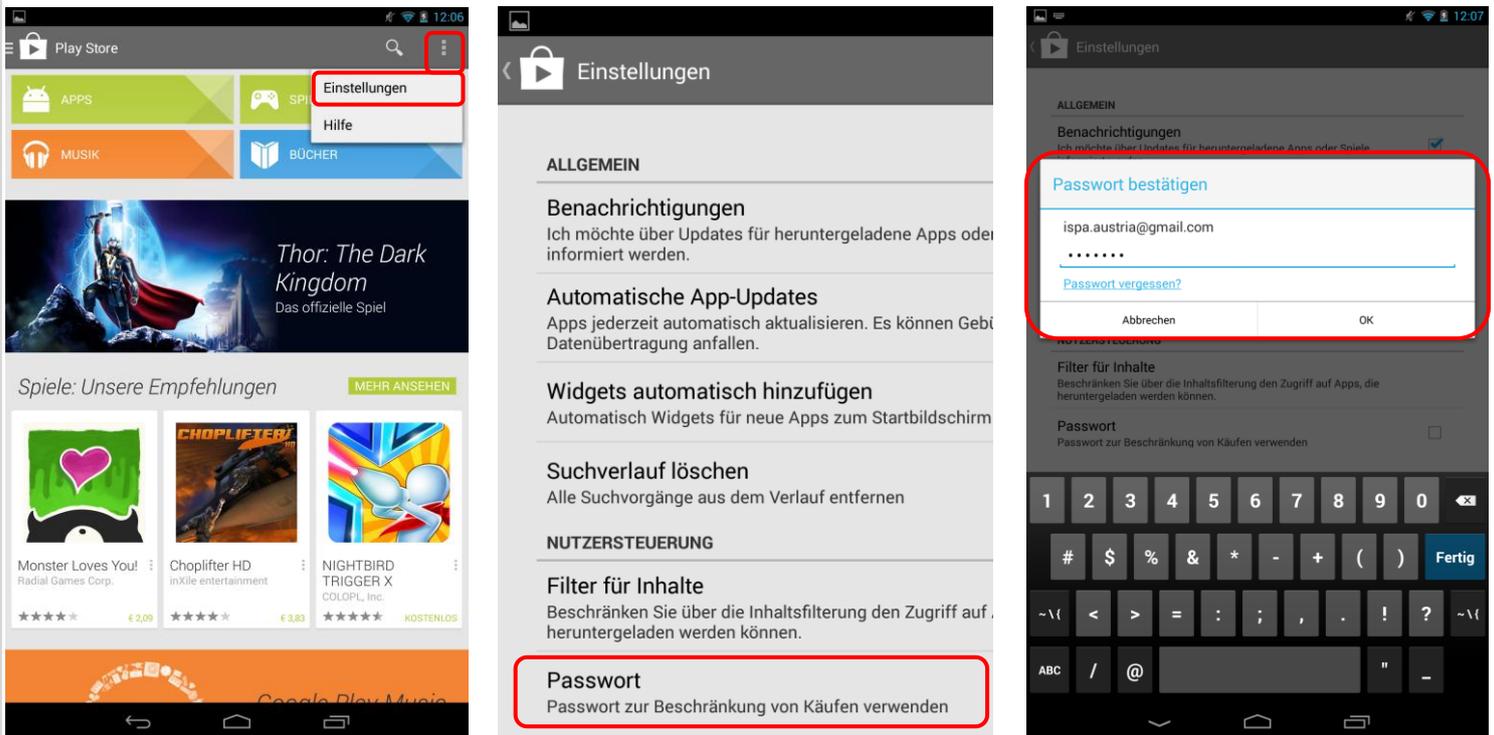
5. Virens Scanner

Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Online-Banking verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Tablet nach Infektionen aller Art (Viren, Würmer und Trojaner) blockieren und beseitigen diese wenn möglich. Bei Android kann aus dem großen Pool der angebotenen Virenschutzprogramme gewählt werden (z.B. die kostenlose Ikarus mobile.security App für Android). Wenn Sie die Sicherheit Ihrer Daten erhöhen möchten, sollten Sie sich auf jeden Fall eine Virens Scanner-App zulegen. Speziell beim Kauf eines Virens Scanners 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, 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 so zur 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. Deaktivieren Sie deswegen die In-App-Käufe auf Ihrem Tablet und schalten Sie diese nur im Bedarfsfall und somit gezielt frei.

Sperre der In-App-Käufe bei Android: Google Playstore – Einstellungen – Passwort



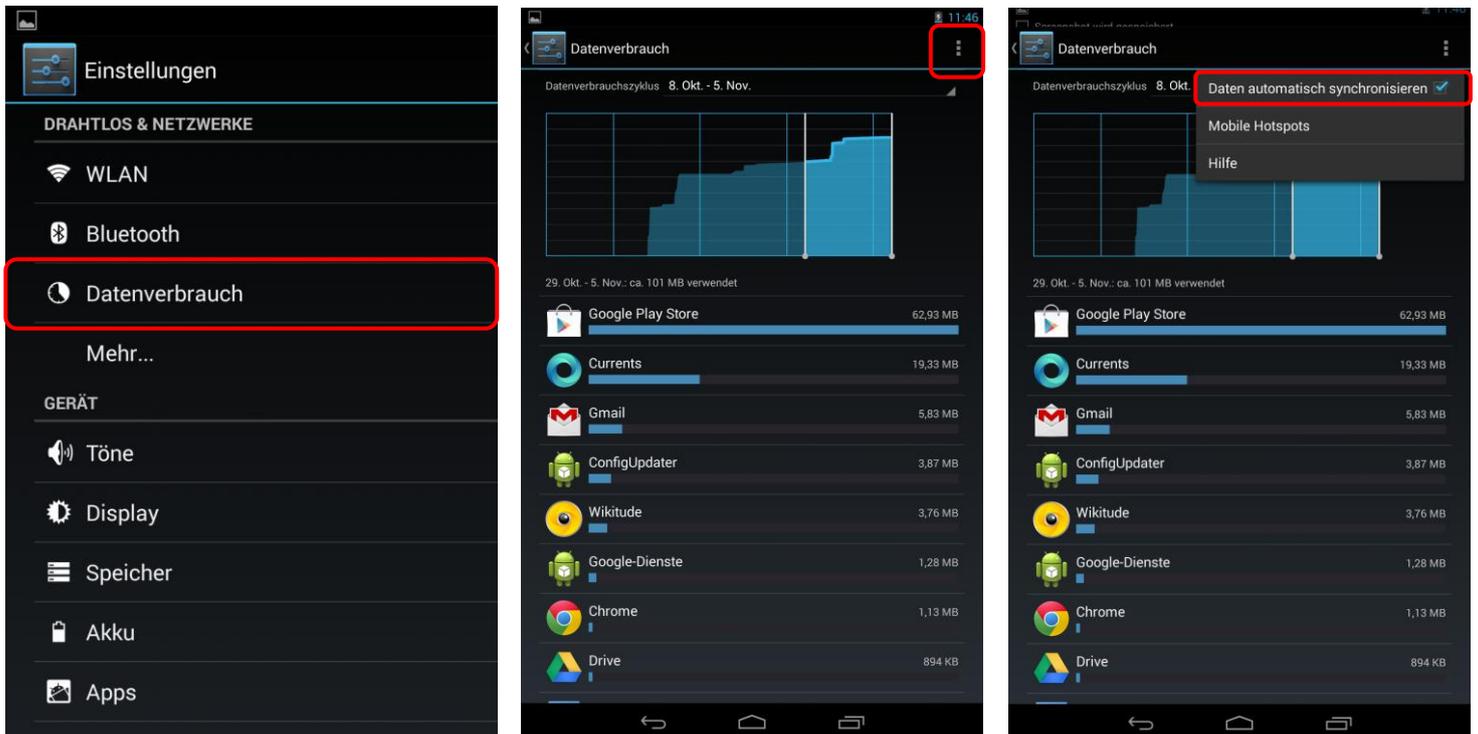
7. Kostenfalle Datentarife

Nicht alle nutzen Tablets mit einer SIM-Karte eines Mobilfunkanbieters, es besteht auch die Möglichkeit Tablets ohne SIM-Karte zu verwenden. Verwenden Sie aber eine SIM-Karte und haben einen entsprechenden Mobilfunkvertrag, sollten Sie Ihr Internetvolumen im Auge behalten. Viele Tablet-Nutzerinnen und -Nutzer haben Verträge mit einem limitierten Internet-Paket, pro Monat können sie somit nur ein bestimmtes Datenvolumen verbrauchen. Wird dieses überschritten, wird es meistens teuer.

Einige Tablets haben bezüglich des Datenverbrauchs Kontroll- und Beschränkungs-funktionen. Hat Ihr Tablet keine solche Funktion und sind Sie sich bei der Einschätzung Ihres Datenverbrauchs unsicher, können Sie für Ihr Tablet 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 Hintergrund synchronisationen abzuschalten. Um Ihr limitiertes Internet-Paket zu schonen, sollten Sie Updates und Synchronisierungen manuell über verfügbare WLAN-Netzwerke durchführen.

Einsicht Datenvolumenverbrauch bei Android: Einstellungen – Datenverbrauch



8. WLAN, Bluetooth und mobile Hotspots

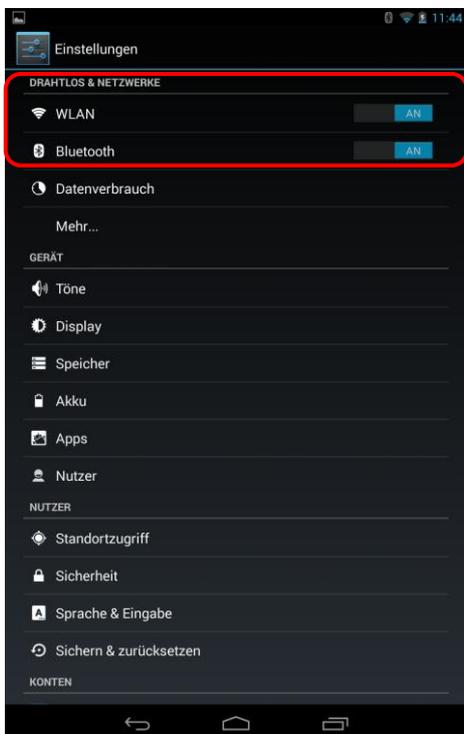
„Home is where your wifi connects automatically.“

Wenn sich das Tablet 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 bei Android deaktivieren:

Einstellungen – WLAN

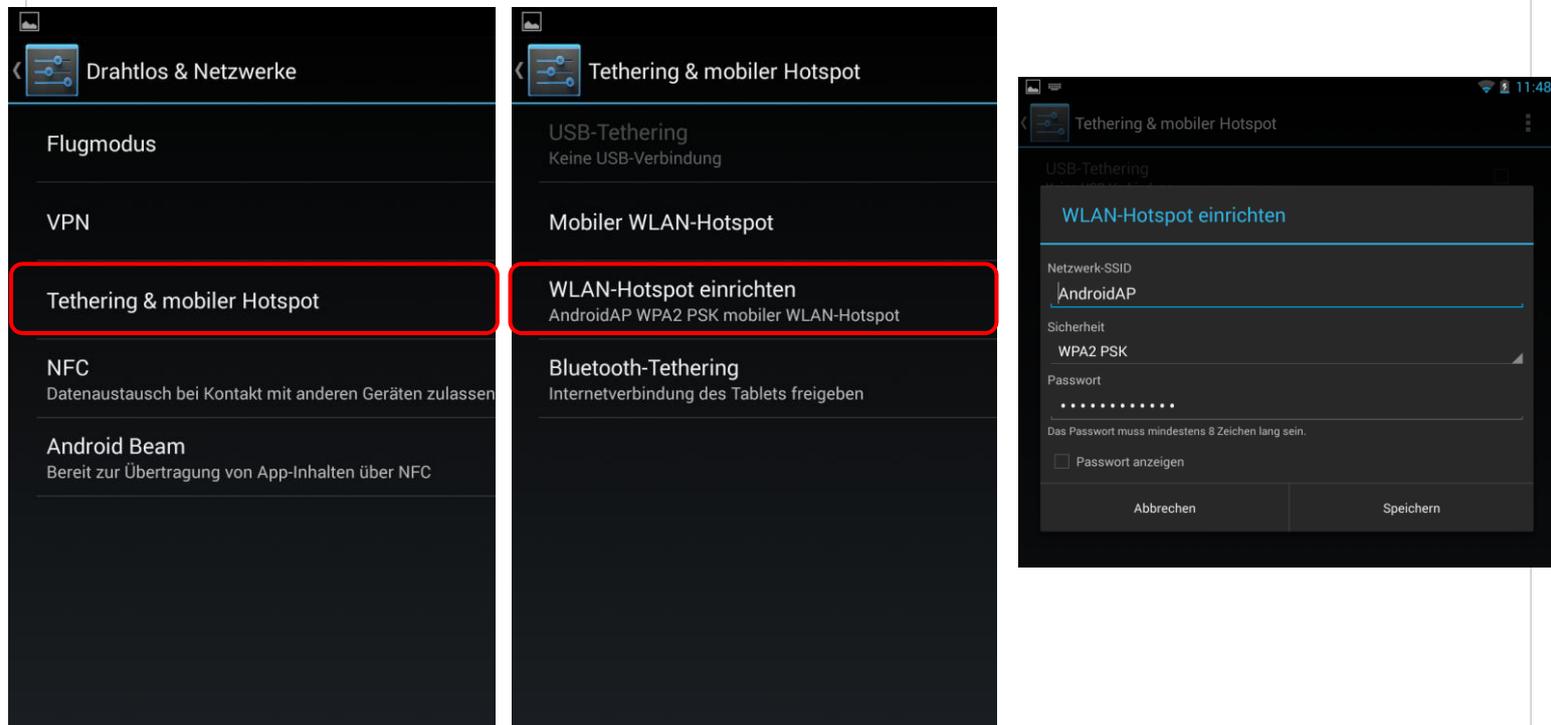
Einstellungen – Bluetooth



Viele Tablets mit Datenverbindung bieten die Möglichkeit das Tablet als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort sichern und ebenfalls nur bei Bedarf aktivieren.

Sicherheitseinstellungen für WLAN-Hotspot bei Android:

Einstellungen – Drahtlos & Netzwerke – Tethering & mobiler Hotspot – WLAN-Hotspot einrichten



9. Jailbreak, Root und gesperrte Tablets

„Jailbreaking“ meint das inoffizielle Entsperren von Software und Hardware, meint in den meisten Fällen aber das Entsperren von Smartphones. Gerade die sehr beliebten iPhones und iPads geraten mit ihren geschlossenen System immer wieder in die Kritik, da z.B. 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 Tablets 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!

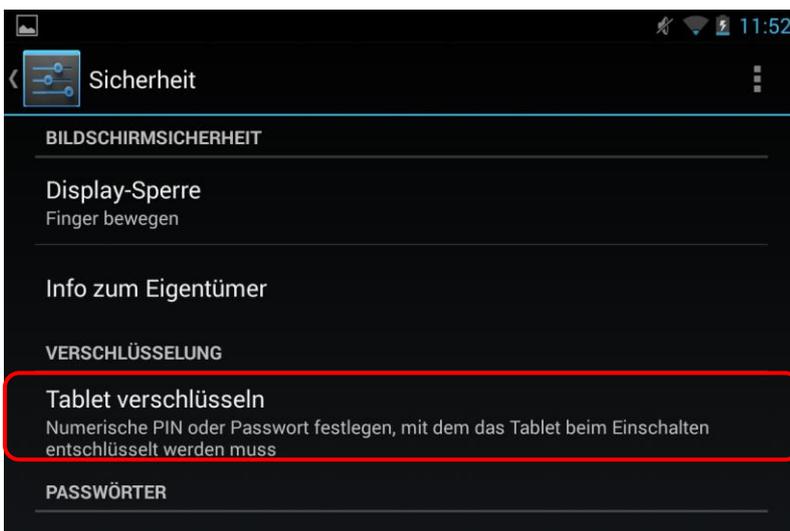
10. Datenverschlüsselung

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

Möchten Sie Ihre Daten noch effektiver vor Missbrauch schützen, können Sie eine Datenverschlüsselung für alle Ihre Tablet-Inhalte überlegen. Diese Option wird jedoch nicht von allen Tablets unterstützt. Wird das Tablet gestohlen oder geht es verloren, sind Konten, Einstellungen, Apps, Musik und Videos nur mit einem von Ihnen festgelegten PIN-Code einsehbar. Die Passwortabfrage erfolgt bei jedem Einschalten des Gerätes zusätzlich zur SIM-Codesperre.

Geräteverschlüsselung bei Android:

Einstellungen – Sicherheit – Tablet verschlüsseln



Achtung: Sie können die Verschlüsselung nicht rückgängig machen! Die Verschlüsselung kann nur aufgehoben werden, wenn Sie das Gerät auf den Werkzustand zurücksetzen, wodurch Ihre Daten gelöscht werden.

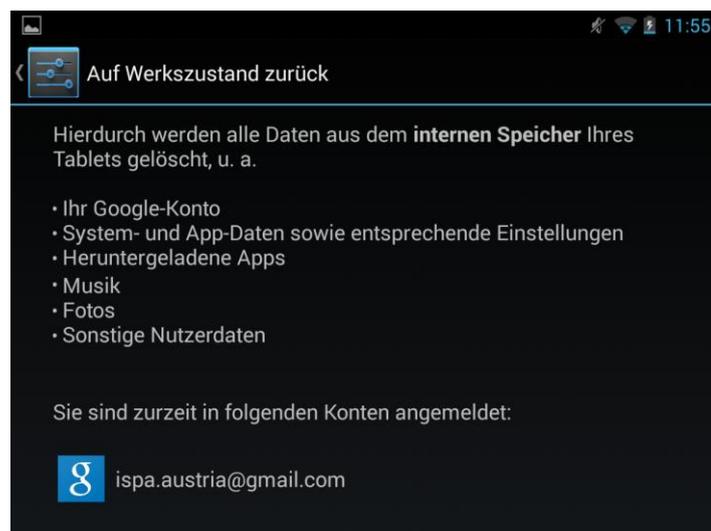
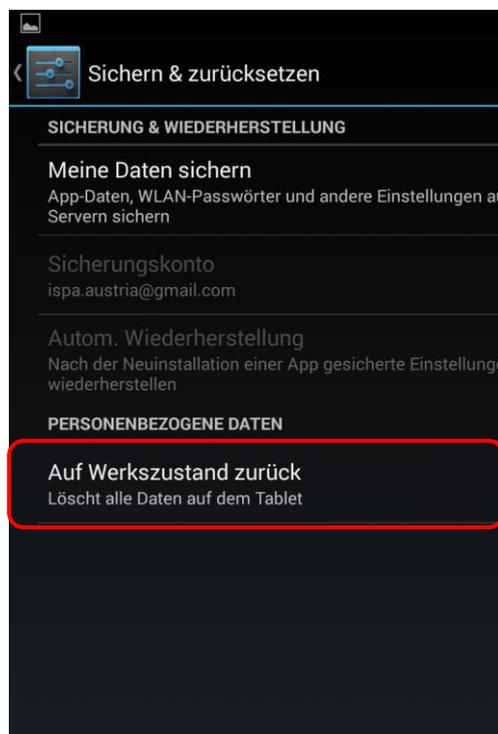
11. Verkaufen, Verschenken & Verborgen

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

Um die Weitergabe Ihrer persönlichen Daten zu verhindern sollten Sie alle vorhandenen Speicher löschen, also nicht nur den internen Speicher, sondern auch den externen (die Micro-SD-Karte). Hierfür reicht es nicht diese einfach nur zu löschen oder das Tablet auf die Werkseinstellungen zurückzusetzen, da mittels einiger Programme gelöschte Daten wiederhergestellt werden können. Erst spezielle Löschroutinen machen durch mehrfaches Überschreiben des Speichers eine Wiederherstellung der Daten unmöglich.

Auf Werkzustand zurücksetzen bei Android:

Einstellungen – Sichern & zurücksetzen – Auf Werkzustand zurück



12. Tablet-Finder: finden oder sperren

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

Android unterstützt diese Funktion. Bei Samsung Tablets heißt diese z.B. „Fernzugriff“. Ist die Funktion aktiviert, kann das Tablet über das Konto bei Samsung geortet, gesperrt oder die Daten aus der Ferne gelöscht werden.

Bei Lokalisierungsfunktionen gilt es aber zwischen Privatsphäre und Sicherheit abzuwägen.

13. Das kindersichere Tablet

Hat Ihr Tablet eine SIM-Karte eingesetzt, sollten Sie das Roaming deaktivieren und Mehrwertdienste sperren. Allenfalls empfiehlt es sich, die SIM-Karte zu entnehmen.

Ein weiterer Schritt um das Tablet kindersicher zu machen, ist die Deaktivierung der In-App-Käufe und ein kinderfreundlicher App-Filter, welcher Apps mit eindeutigen Inhalten gar nicht erst anzeigt. In letzter Konsequenz können Sie auch das Internet deaktivieren und in den Flugmodus wechseln.

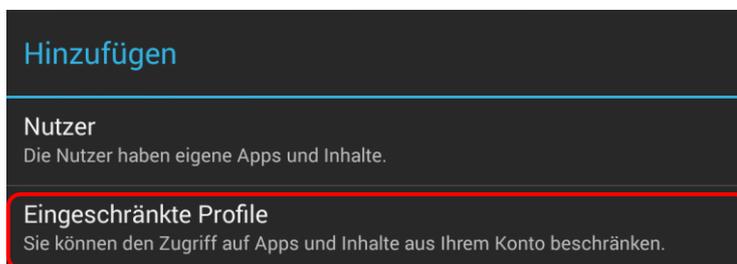
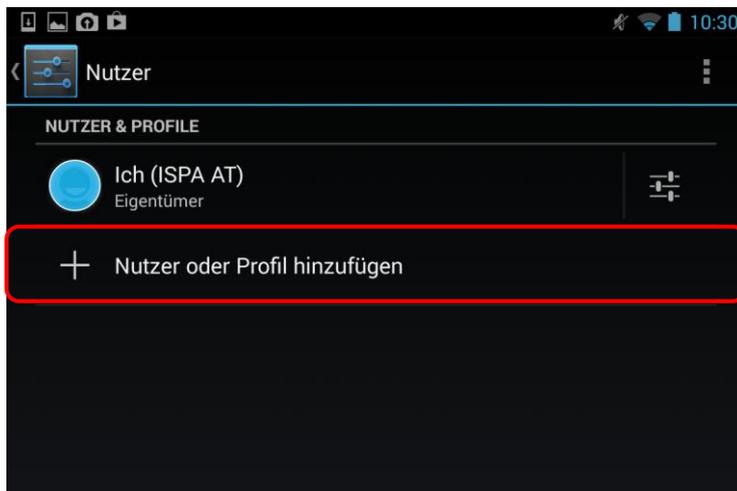
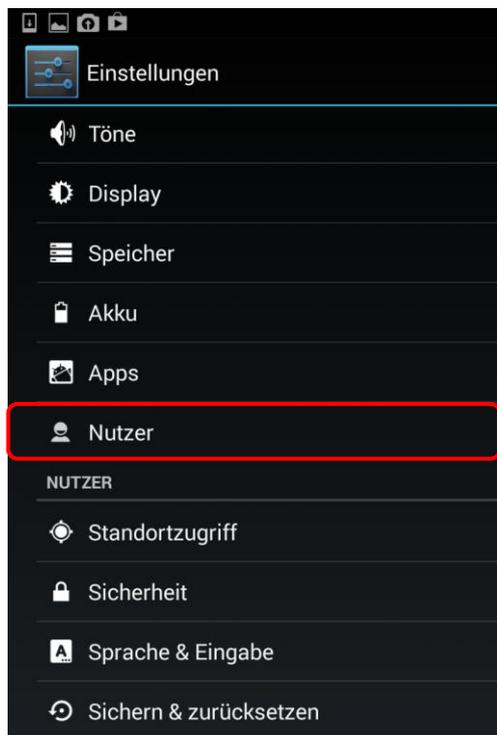
Viele Geräte bieten mittlerweile die Option, mehrere Benutzerkonten anzulegen. Hier können Sie ein eigenes Profil für kleine Userinnen und User einrichten, indem Sie genau festlegen, welche Programme, Videos und Fotos verfügbar sein sollen und welche nicht. Ist das Kinderprofil einmal eingerichtet, können Sie je nach Bedarf zwischen den verschiedenen Konten wechseln. Zudem können Sie Zeitlimits und -guthaben, als auch Sperr- und Ruhezeiten festlegen. Ist das Kinderkonto einmal eingerichtet, können Sie dieses individuell anpassen und nach Bedarf ein- und ausschalten.

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

Achtung: Vor dem Erstellen eines eingeschränkten Profils müssen Sie eine Display-Sperre einrichten, um Ihre Apps und personenbezogenen Daten zu schützen.

Profil anlegen bei Android:

Einstellungen – Nutzer – Nutzer oder Profil hinzufügen



Profileinschränkungen vornehmen bei Android:

Einstellungen – Nutzer – Nutzer oder Profil hinzufügen

