Sicherheitseinstellungen für Tablets

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

1. Passwortschutz am Tablet 1
2. Software-Updates des Geräteherstellers 3
3. Synchronisierung & Backups 4
4. Apps! Nur, wie richtig? 5
5. Virenscanner 8
6. Kostenfalle In-App-Käufe 8
7. Kostenfalle Datentarife 10
8. WLAN, Bluetooth und mobile Hotspots 12
9. Jailbreak, Root und gesperrte Tablets 13
10. Datenverschlüsselung 14
11. Verkaufen, Verschenken & Verborgen 15
12. Tablet-Finder: finden oder sperren 16
13. Das kindersichere Tablet 17

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
iOS: 5.1.1, iPad 1
Android: 4.1.2, Samsung Galaxy Tab 2
Inhaltliche Verantwortung: Daniela Drobna

Gefördert durch die Europäische Union – Safer Internet Projekt

Wien, August 2013

ispa Internet Service Providers Austria

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. Alle Sicherheitsvorkehrungen werden anhand von Screenshots für die beiden gängigsten Betriebssysteme für Tablets, iOS und Android, erklärt.

1. Passwortschutz am Tablet

Wie auch beim Smartphone, gibt es beim Tablet zwei Möglichkeiten dieses mittels Passwort zu schützen: einmal die Passwortabfrage beim Einschalten des Gerätes – solange eine SIM-Karte eingesetzt ist (SIM-Kartensperre) – und als weitere Option die Bildschirmsperre.
Ersteres ist eine Standardeinstellung, welche die meisten Userinnen und User von Ihrer Handynutzung kennen und auch verwenden. Sind Tablets ohne SIM-Karte in Gebrauch, ist es besonders ratsam die Bildschirmsperre zu aktivieren, da sonst kein anderer Passwortschutz vorhanden ist. Es erscheint zwar zeitaufwendig jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz Ihres Tablets bzw. Ihrer Daten bei.

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

- Gesichtserkennung
- Musterentsperrung
- PIN-Eingabe
- Passwort-Eingabe

Die Gesichtserkennung hat die niedrigste Sicherheitsstufe. Hierbei scannt das Tablet Ihr Gesicht, sodass Sie dieses zum Entsperren lediglich ansehen müssen. In der Praxis führen aber schlechte Lichtverhältnisse rasch zu einer Nicht-Erkennung und somit zu keiner Entsperrung. Bei dieser Art der Bildschirmsperre wird daher zusätzlich auch ein PIN-Code verwendet, damit Sie bei Nicht-Erkennung zumindest per PIN 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 diese unter Umständen leicht beobachtet oder nachvollzogen

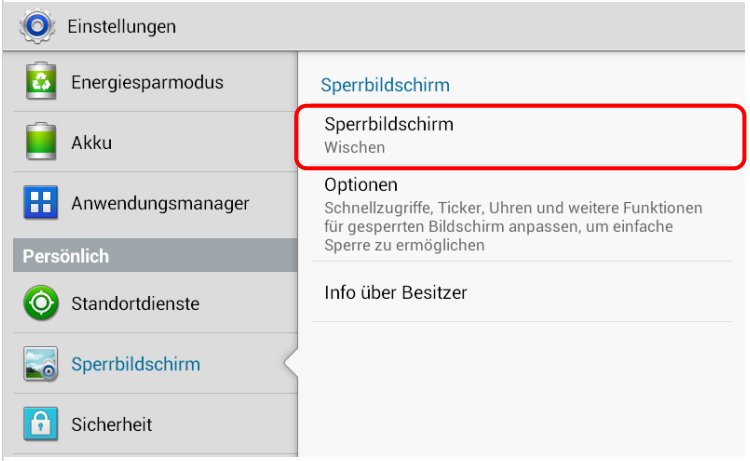
werden kann. Das Muster legen Sie auf einer 3 x 3-Punkte-Matrix (oder alternativ 4 x 4-Punkte-Matrix) als Verbindungslinie von mindestens vier Punkten fest. Zum Entsperren fahren Sie dann nur noch auf dem Touchdisplay die vorher festgelegte Linie nach.

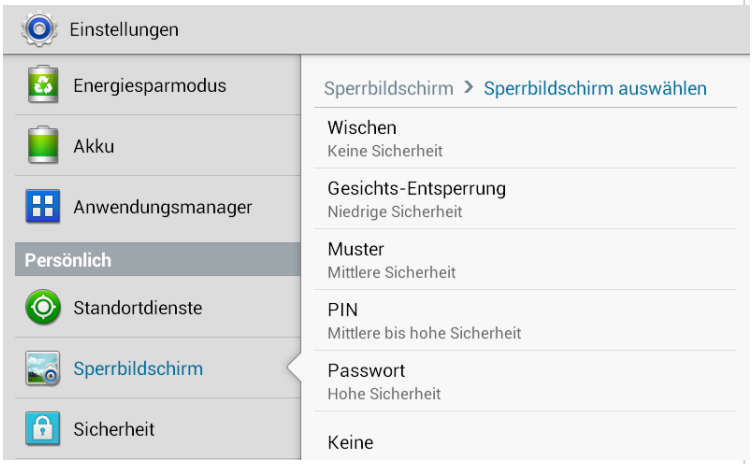
Die PIN-Eingabe ist der Klassiker beim Passwortschutz. Je nach Schwierigkeitsgrad der Zahlenkombination bietet sie mittlere bis hohe Sicherheit.

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

Bildschirmsperre bei Android-Tablets:

Einstellungen – Sperrbildschirm – Sperrbildschirm





Neben der PIN-Abfrage beim Einschalten des iPhones, gibt es den optionalen Passwortschutz „Code Sperre". 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 iPad einschalten oder neu starten
- den Ruhezustand aufheben
- die Anzeigensperre deaktivieren

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

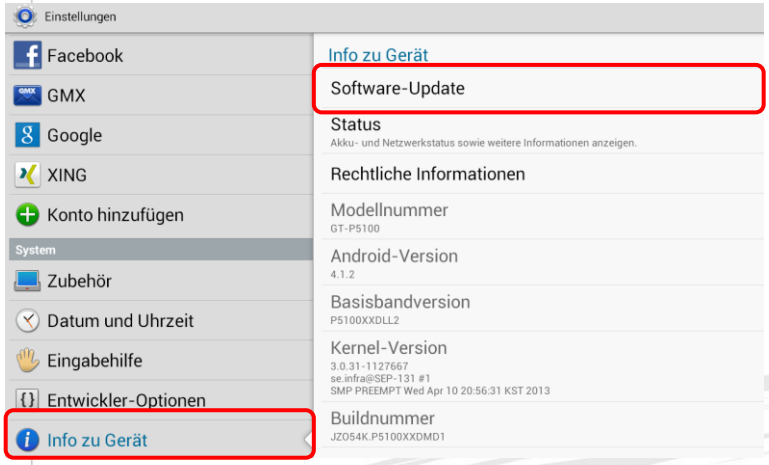
Zudem haben Sie beim iPad die Möglichkeit, einzelne Anwendungen und Apps mittels eines zusätzlichen – also anderen – Codes einzuschränken. Hier können Sie z.B. das Kaufen von Apps deaktivieren oder „anstößige Sprache" ausblenden lassen, sodass die Spracherkennungssoftware (Siri) diese mit einem Stern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

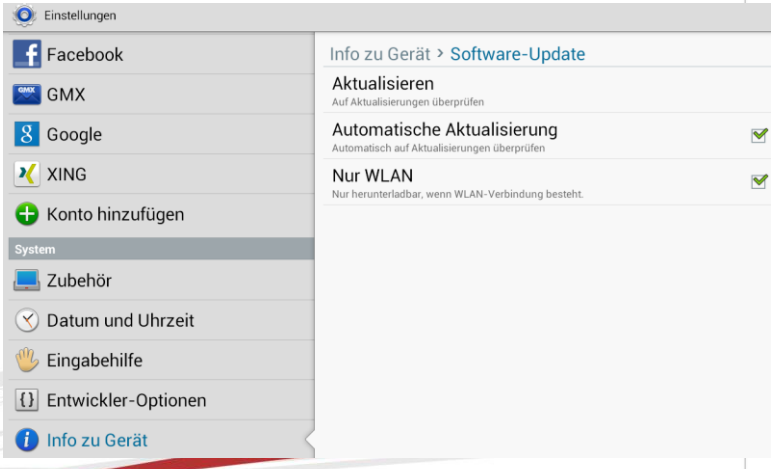
Code Sperre beim iPad:
Einstellungen – Allgemein – Code-Sperre

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 – Info zu Gerät – Software-Update – Aktualisieren





Software-Updates beim iPad:

Einstellungen – Allgemein – Softwareaktualisierung

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:

Startmenü auswählen – USB-Option wählen – Mediengerät
(Verbinden Sie vorher das Tablet per USB-Kabel mit dem Pc)

Synchronisierung von iPad und PC:

Einstellungen – Allgemein – iTunes WLAN Sync

Beim iPad können Sie z.B. Ihr iTunes-Konto vom iPad sehr leicht mit jenem auf Ihrem Computer synchronisieren – und umgekehrt.

Achtung: Blockieren Sie Hintergrundanwendungen! Bei Android synchronisieren sich Ihre Apps laufend im Hintergrund, außer Sie deaktivieren diese Funktion im Menüpunkt „Konten und Synchronisierung". Auch beim iPhone müssen Sie „automatische Downloads" von Apps unter „Einstellungen" und „Store" deaktivieren.

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!

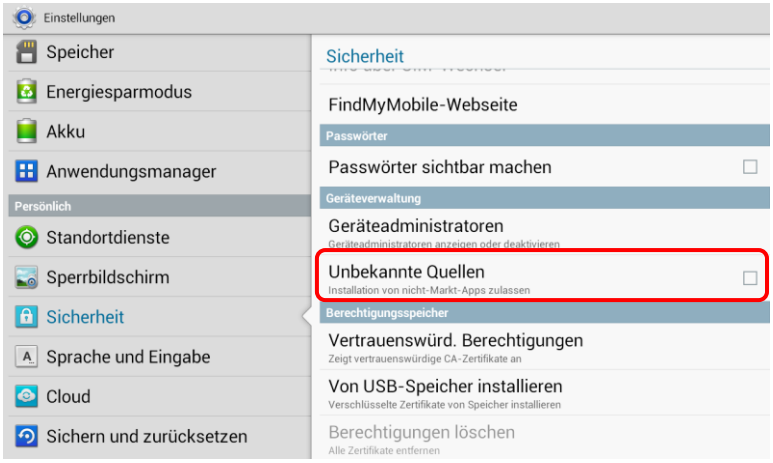
Natürlich kann es auch hier keine endgültige Garantie geben, aber die offiziellen Stores von Apple (App Store: http://itunes.apple.com) und von Android (Google Playstore: http://play.google.com) sind definitiv vertrauenswürdiger als andere.
Die Apple-Apps können lediglich über den iTunes-Store erworben werden (sofern diese Sperre nicht durch einen „Jailbreak" umgangen wurde – siehe Punkt 9). Das iOS Betriebssystem für iPads ist ein geschlossenes System und somit prinzipiell relativ sicher.

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

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 Quellen



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.
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 iTunes Store mittels der Funktion „Problem melden" eine Rückgabe unter Angabe des Grundes zu beantragen.

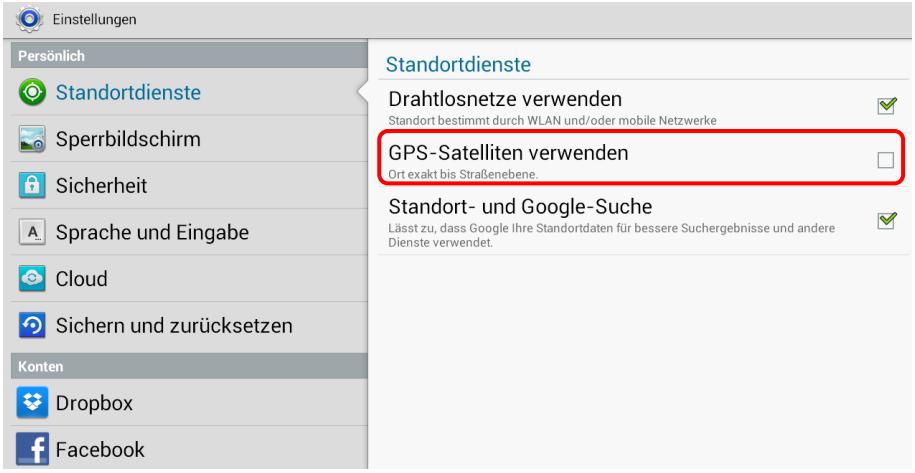
Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

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. Bösartige 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 eine richterliche Anordnung brauchen?

Deaktivierung von GPS-Daten-Übermittlung bei Android:

Einstellungen – Standortdienste – GPS-Satelliten deaktivieren



Deaktivieren von GPS-Daten-Übermittlung beim iPad:

Einstellungen – Ortungsdienste – Ortungsdienste deaktivieren

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. Virenscanner

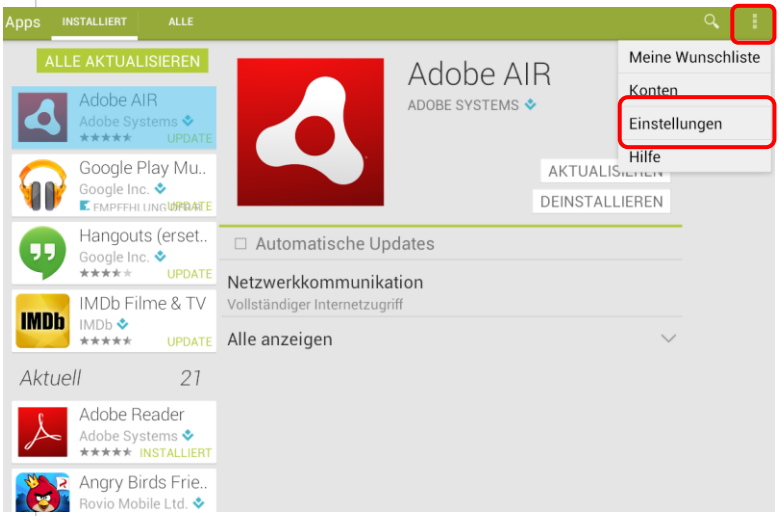
Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Online-Banking verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Tablet nach Infektionen aller Art (Viren, Würmer und Trojaner) blockieren und beseitigen diese wenn möglich. Für das iPhone gibt es von Apple selbst nach wie vor kein Virenschutzprogramm. Somit kann wie bei Android aus dem großen Pool der angebotenen Virenschutzprogramme ausgewählt 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 Virenscanner-App zulegen. Speziell beim Kauf eines Virenscanners empfiehlt es sich natürlich, besonders aufmerksam und auf Ihre persönlichen Bedürfnisse abgestimmt auszuwählen!

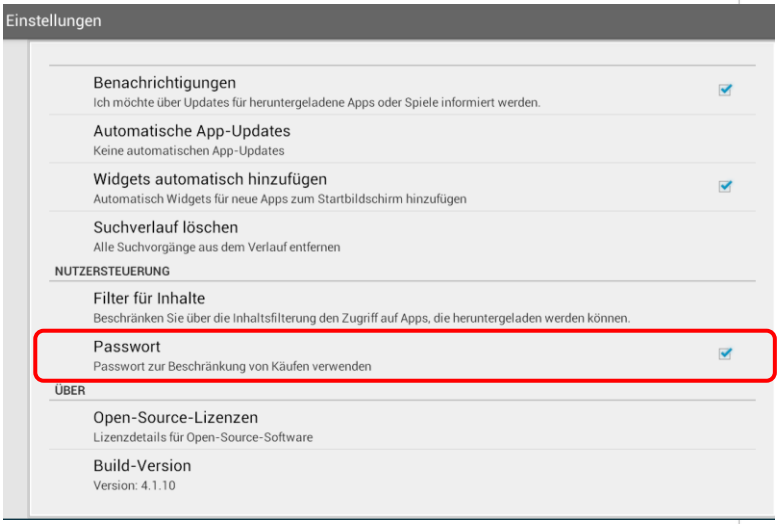
6. Kostenfalle In-App-Käufe

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

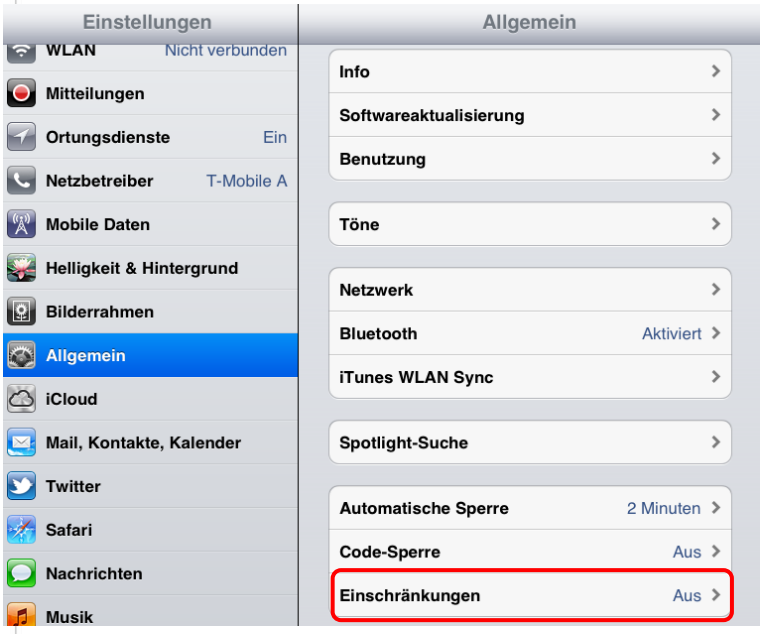




Das iPad hat hierzu einen eigenen Menüpunkt in den Einstellungen, bei dem In-App-Käufe komplett deaktiviert werden können.

Sperre der In-App-Käufe beim iPad:

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

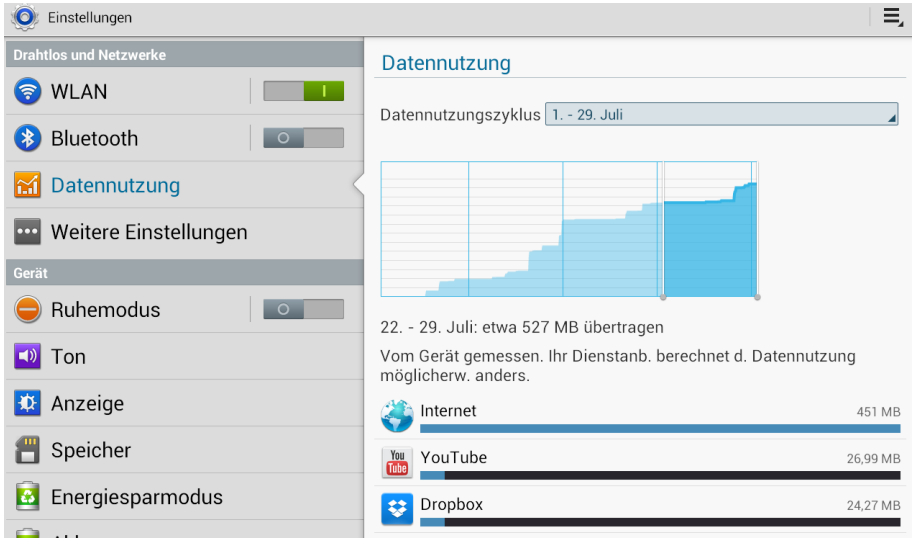


7. Kostenfalle Datentarife

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 Beschränkungsfunktionen. 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.

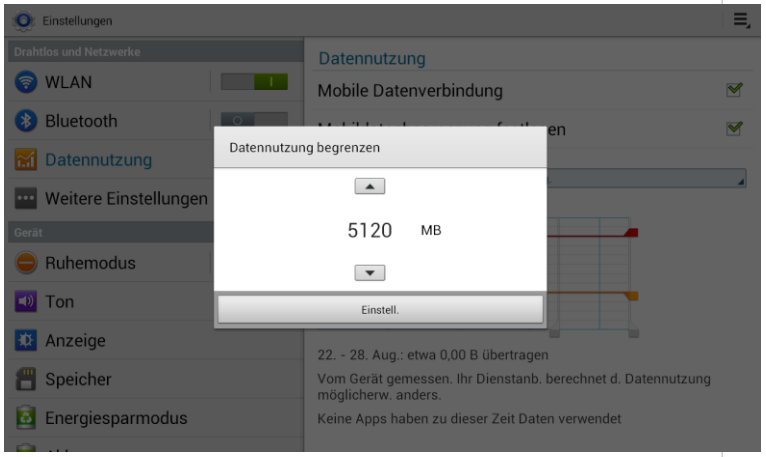
Volumeneinsicht bei Android:

Einstellungen - Datennutzung



Volumenbeschränkung bei Android mit SIM-Karte:

Einstellungen – Datennutzung – Mobildatenbegrenzung festlegen – Grenzwerte antippen und einstellen



Volumeneinsicht beim iPad:

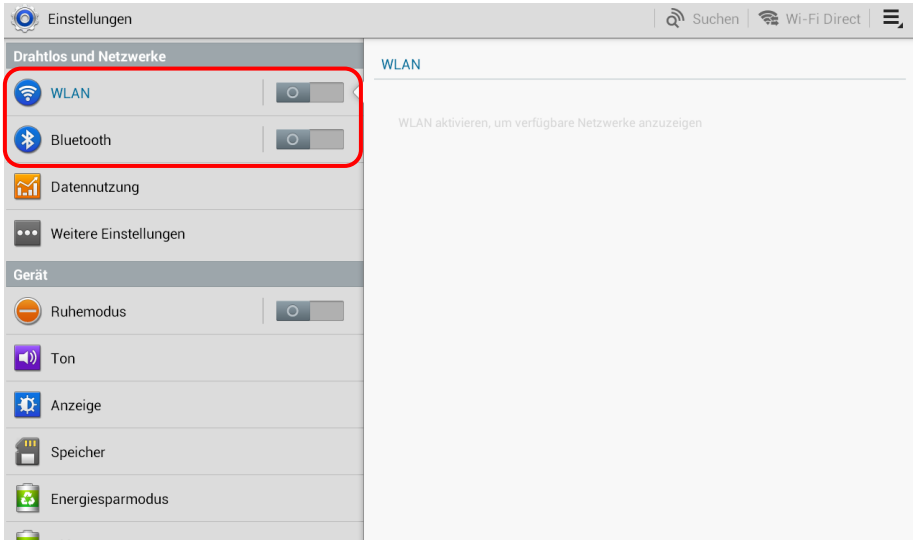
Einstellungen – Allgemein – Benutzung – Mobile Datennutzung

8. WLAN, Bluetooth und mobile Hotspots

Wenn sich das Tablet automatisch im Büro oder zu Hause 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



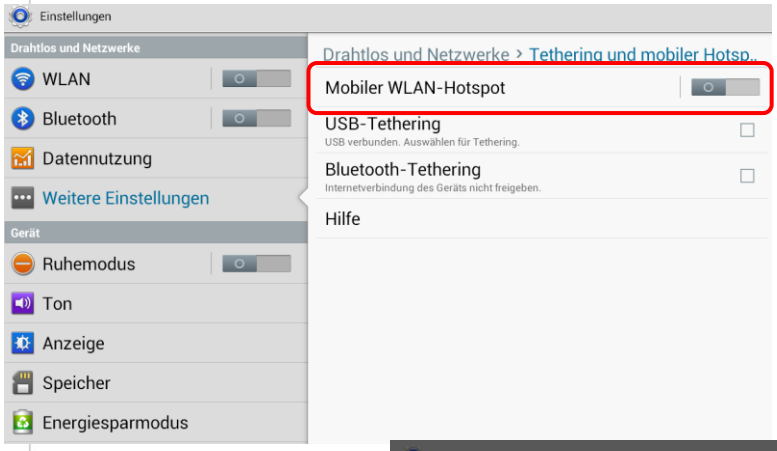
WLAN und Bluetooth beim iPad deaktivieren:

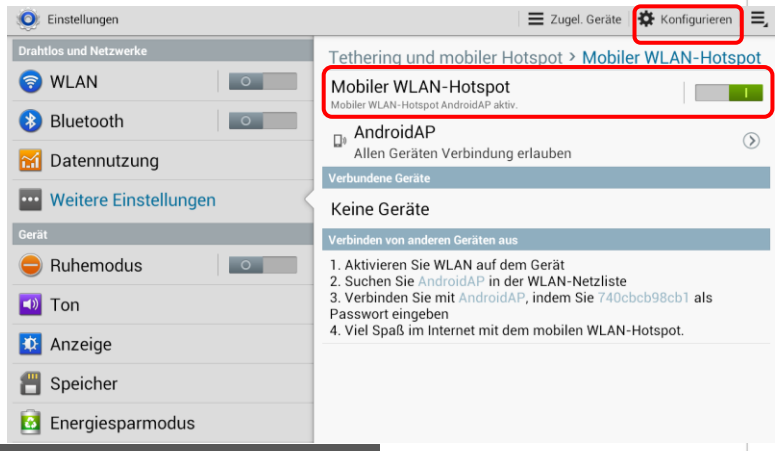
Einstellungen – WLAN
Einstellungen – Allgemein – Bluetooth

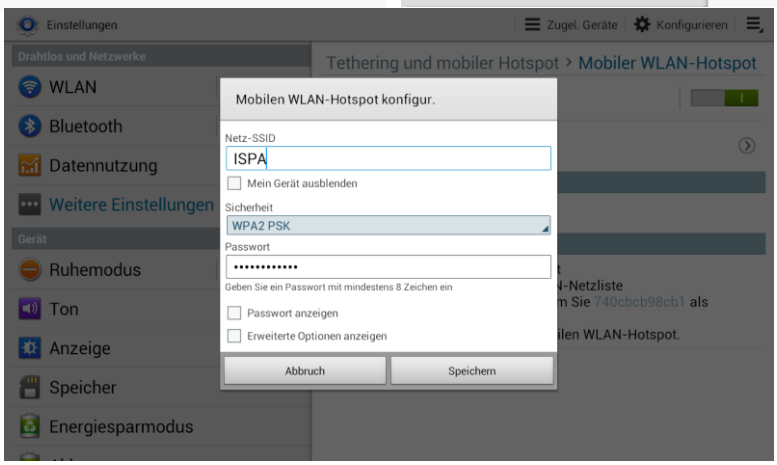
Viele Tablets mit Datenverbindung bieten die Möglichkeit das Tablet als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort sichern und ebenfalls nur bei Bedarf aktivieren.

Sicherheitseinstellungen für WLAN-Hotspot bei Android:

Einstellungen – Weitere Einstellungen – Tethering und mobiler Hotspot – Mobiler WLAN-Hotspot aktivieren – erneut Mobiler WLAN-Hotspot antippen - Konfigurieren







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.

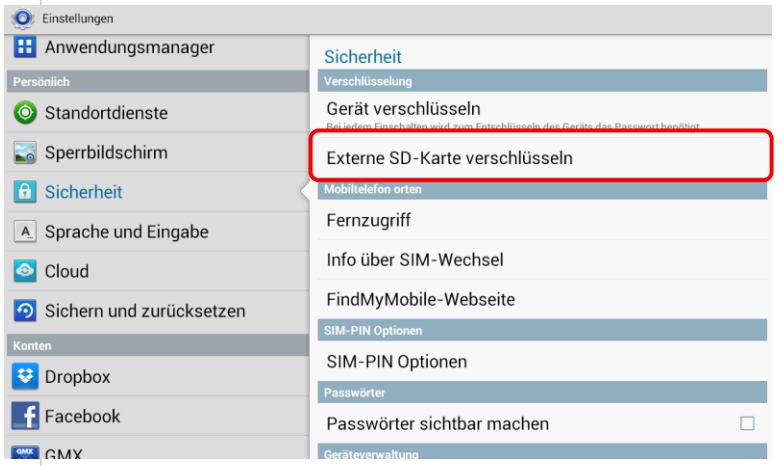
Das Gegenstück zum Jailbreak bei Apple ist das „Rooten" bei Android: ein „Root" ist vergleichbar mit einem Administrator-Konto, welches volle Zugriffs- und Schreibrechte hat und über welches somit das gesamte System verändert werden kann.

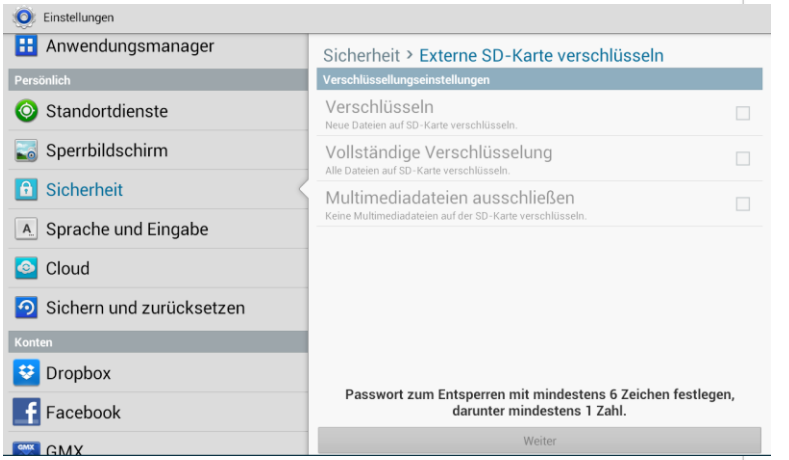
Achtung: Durch den Jailbreak und das Rooten können die Betriebssysteme der Tablets beeinträchtigt oder sogar beschädigt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Jailbreak-Programmen oder von Schadsoftware werden. Zudem fällt das Jailbreaking und Rooten in eine rechtliche 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.

Datenverschlüsselung der Speicherkarte bei Android:
Sicherheit – Externe SD-Karte verschlüsseln





Möchten Sie Ihre Daten noch effektiver vor Missbrauch schützen, können Sie eine Datenverschlüsselung für alle Ihre Tablet-Inhalte überlegen. Diese Option wird z.B. von Samsung-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:

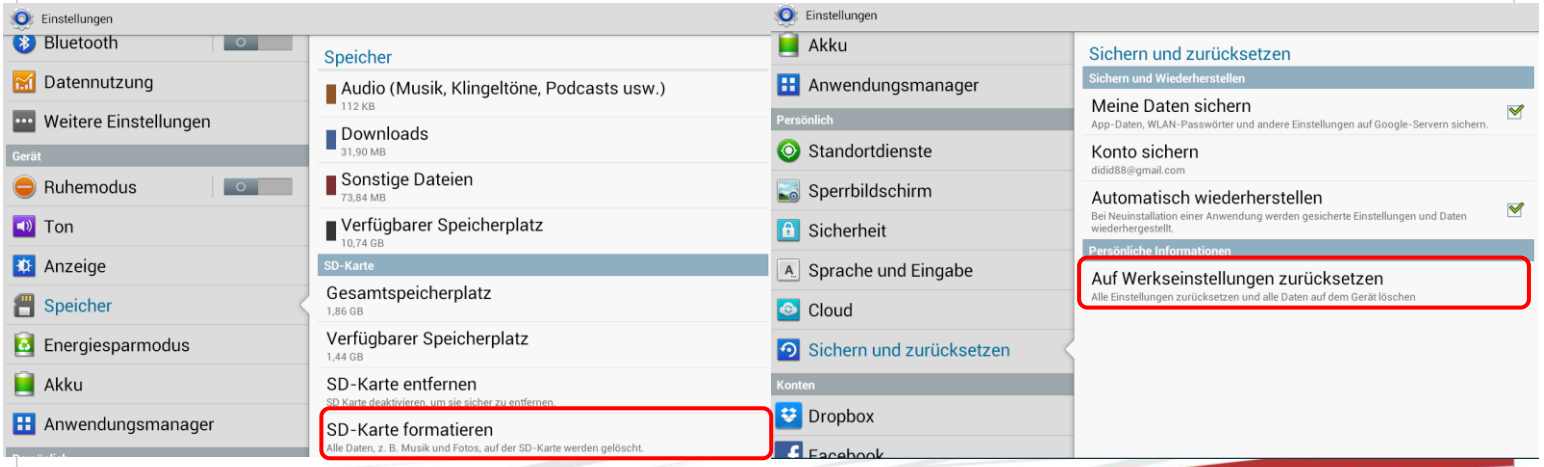
Einstellungen – Sicherheit – Gerät verschlüsseln

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 Löschprogramme machen durch mehrfaches Überschreiben des Speichers eine Wiederherstellung der Daten unmöglich.

Auf Werkzustand zurücksetzen bei Android:

Einstellungen – Speicher – SD-Karte formatieren
Einstellungen – Sichern und zurücksetzen – Auf Werkzustand zurücksetzen

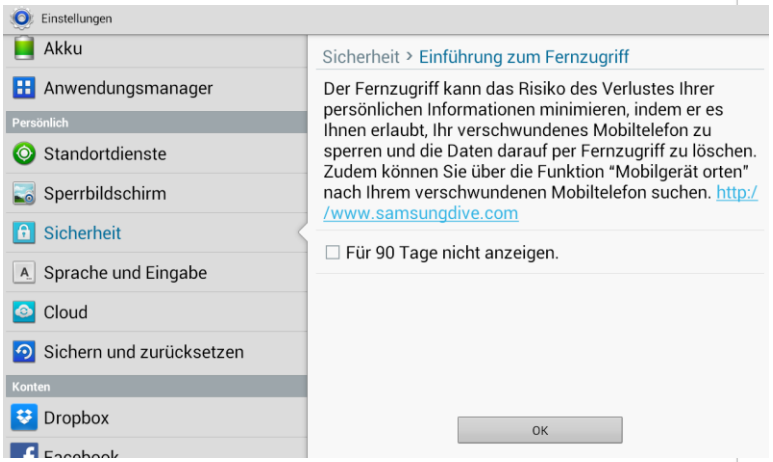


Auf Werkzustand zurücksetzen beim iPad:
Einstellungen – Allgemein – Zurücksetzen

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.
Apple hat hierzu die „Find my iPad"-Funktion integriert. Die Funktion wird über das persönliche iCloud-Konto eingeschalten. Ist die Funktion aktiviert, ist die (ungefähre) Position des Tablets über die iCloud einsehbar. Über den „Lost Mode" kann das iPad gesperrt werden und eine Nachricht mit den Kontaktdaten kann auf das Gerät geschickt werden. Hierdurch kann der Finder oder die Finderin Sie unter der angegebenen Nummer anrufen, ohne dass er oder sie sonstigen Zugriff auf das iPad hat.
Auch bei Android gibt es eine äquivalente Funktion, bei Samsung Tablets heißt diese z.B. „Fernzugriff". Ist diese 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.

Aktivierung des Telefonfinders bei Android:
Einstellungen – Sicherheit – Fernzugriff



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.
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: Bedenken Sie, dass bei iPads mit aktiver Code-Sperre nach zehnmaliger Falscheingabe des Codes die gesamten Daten gelöscht werden! Sie sollten diese sicherheitshalber aufheben, bevor Sie Ihr Tablet an Kinder weitergeben.