Sicherheitseinstellungen für Smartphones

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

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

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
Inhaltliche Verantwortung: Daniela Drobna
Endgerät: Galaxy Nexus 4
BS: Android 4.4.2

Gefördert durch die Europäische Union – Safer Internet Projekt

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 Nutzungs-möglichkeiten 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 Fall eines Verlustes oder Diebstahls hilfreich sind.

1. Doppelt hält besser: 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 abgeschalten 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 der Bildschirmsperre von Android-Smartphones haben Sie für gewöhnlich mehrere Möglichkeiten:

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

Die Gesichtserkennung hat die niedrigste Sicherheitsstufe. Hierbei scannt das Smartphone 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.

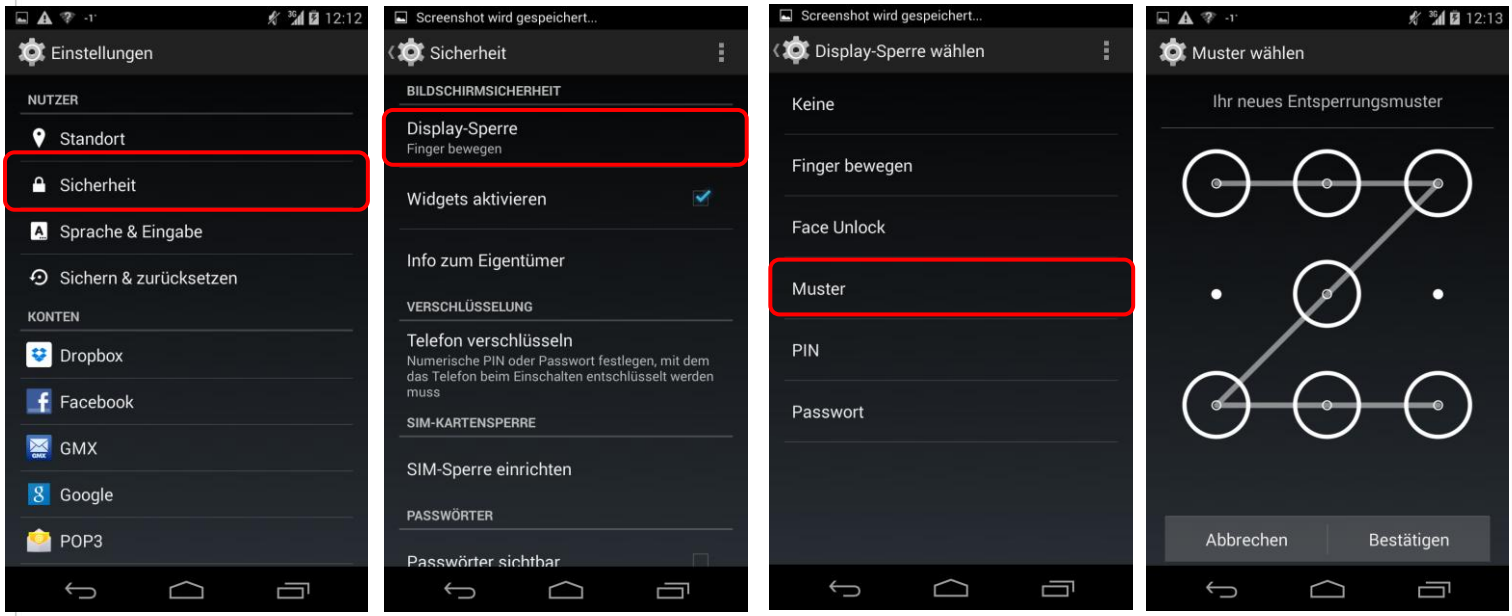
Die Musterentsperrung ist vor allem bei Smartphones eine sehr beliebte Methode zum Schutz des Endgerätes. Die Musterentsperrung bewegt sich als Sicherheitsvorkehrung im mittleren Bereich, da diese unter Umständen leicht beobachtet oder nachvollzogen werden kann. Das Muster legen Sie auf einer 3 x 3-Punkte-Matrix (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.

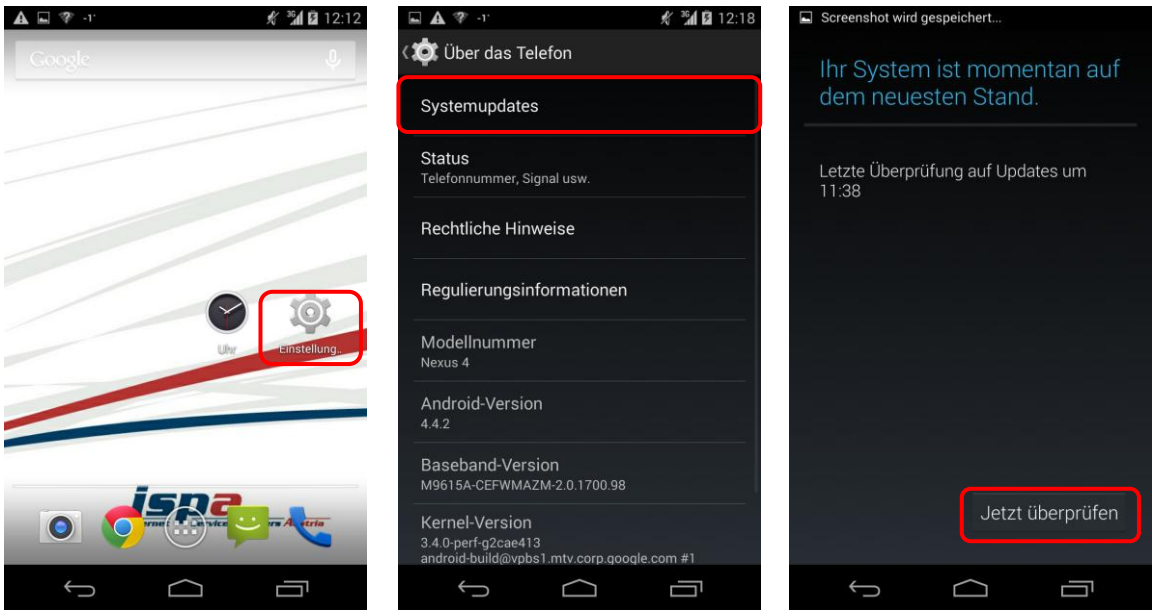
Bildschirmsperre bei Android-Smartphones:
Einstellungen – Sicherheit – Display-Sperre



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 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 Smartphone automatisch auf Software-Aktualisierungen überprüft und Sie gegebenenfalls darauf aufmerksam macht.

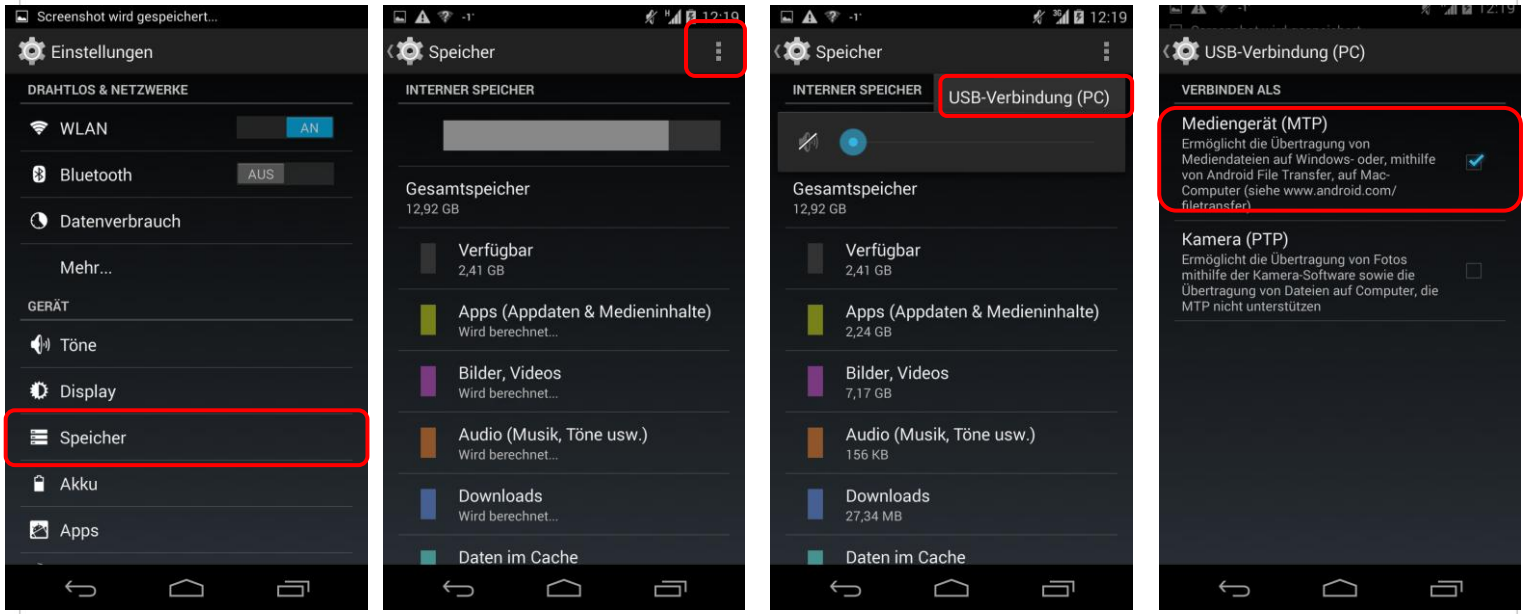
Software-Updates:
Einstellungen – Über das Telephon – Systemupdates



3. Synchronisierung & Backups

Genau wie bei einem PC ist es auch bei einem Smartphone notwendig, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Daten- oder Smartphoneverlusts können Sie so auf Ihr Backup zugreifen und haben zumindest den letzten Stand Ihrer gesicherten Daten verfügbar.
Bei Geräten mit Android gibt es mittlerweile auch die Möglichkeit ein Sicherungskonto bei Google anzulegen, dieses funktioniert.

Synchronisierung von Smartphone und PC:
Einstellungen – Speicher – Menü – USB-Verbindung mit Pc
(Verbinden Sie vorher das Smartphone 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?

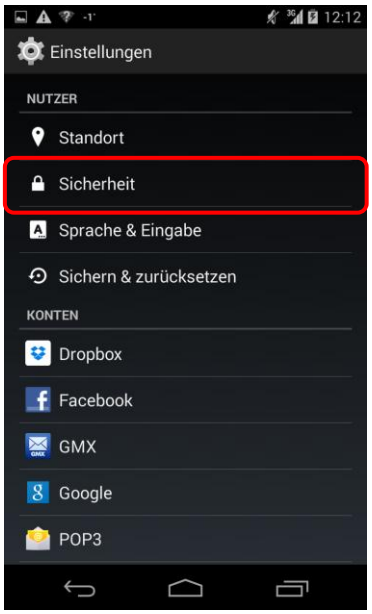
Ein Smartphone ohne Apps ist noch weniger das Wahre als ein Smartphone ohne Apps. Jedoch können die kleinen Anwendungen auch hier genutzt werden um in Ihr Smartphone und somit an Ihre Daten zu gelangen: diese schädlichen Apps heißen „Malware". Wenn Sie beim Kauf und Download von Apps ein paar wenige Punkte beachten, können Sie ganz leicht dieses Sicherheitsrisiko minimieren.

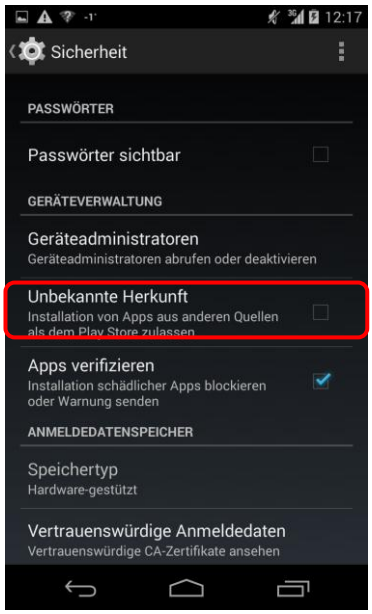
Beziehen Sie Apps nur aus den offiziellen App-Stores!

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.
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-Smartphone komplett sperren.

Sperre unbekannter Quellen:

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.

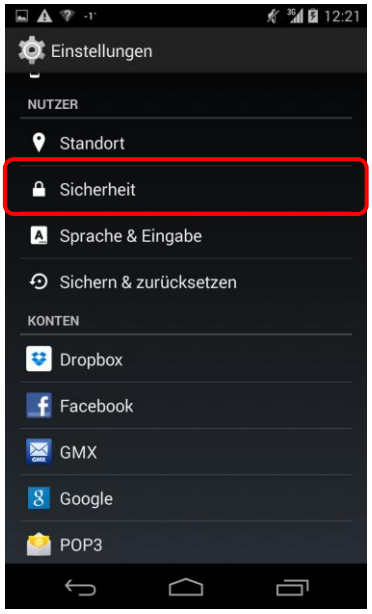
Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

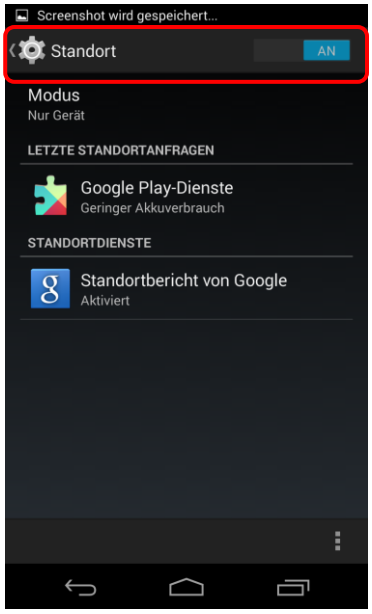
Vor der endgültigen Installation einer App müssen Sie deren Zugriffsberechtigungen zustimmen. Seien Sie hier vorsichtig und stimmen Sie Berechtigungen nur dann zu, wenn diese notwendig erscheinen. Bösartige Apps machen sich hier die Unachtsamkeit

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 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:

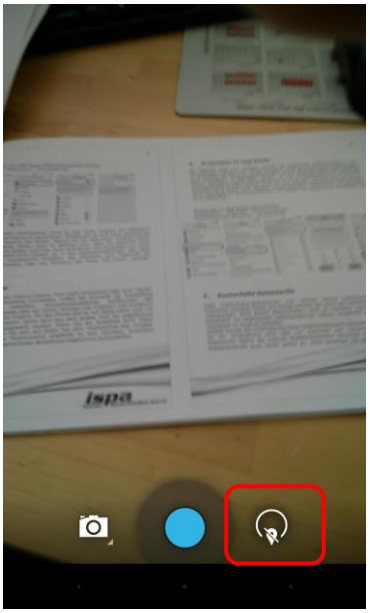
Einstellungen – Standortzugriff

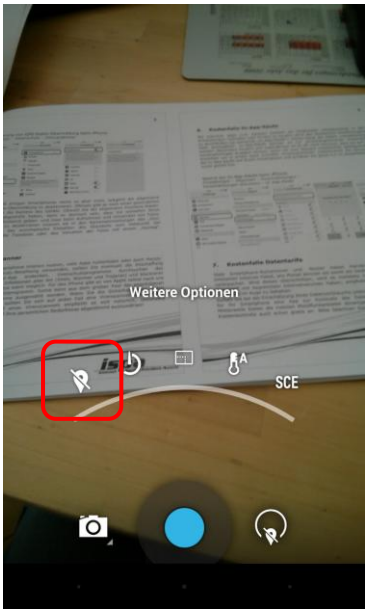




Achtung: Bei einigen Smartphones reicht es aber nicht, lediglich die allgemeine Positions-Daten-Übermittlung zu deaktivieren. Oftmals gibt es noch einen gesonderten Unterpunkt für die Kamera des Geräts. Obwohl Sie die allgemeine Positions-Daten-Übermittlung abgedreht haben, kann es dennoch sein, dass 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.

Deaktivierung des Geo-Taggings bei Fotos:
Kamera – Einstellungen – Geo-Tagging





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 Smartphone 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 Virenscanner-App zulegen. Speziell beim Kauf eines Virenscanners empfiehlt es sich natürlich, besonders aufmerksam und auf Ihre persönlichen Bedürfnisse abgestimmt auszuwählen!

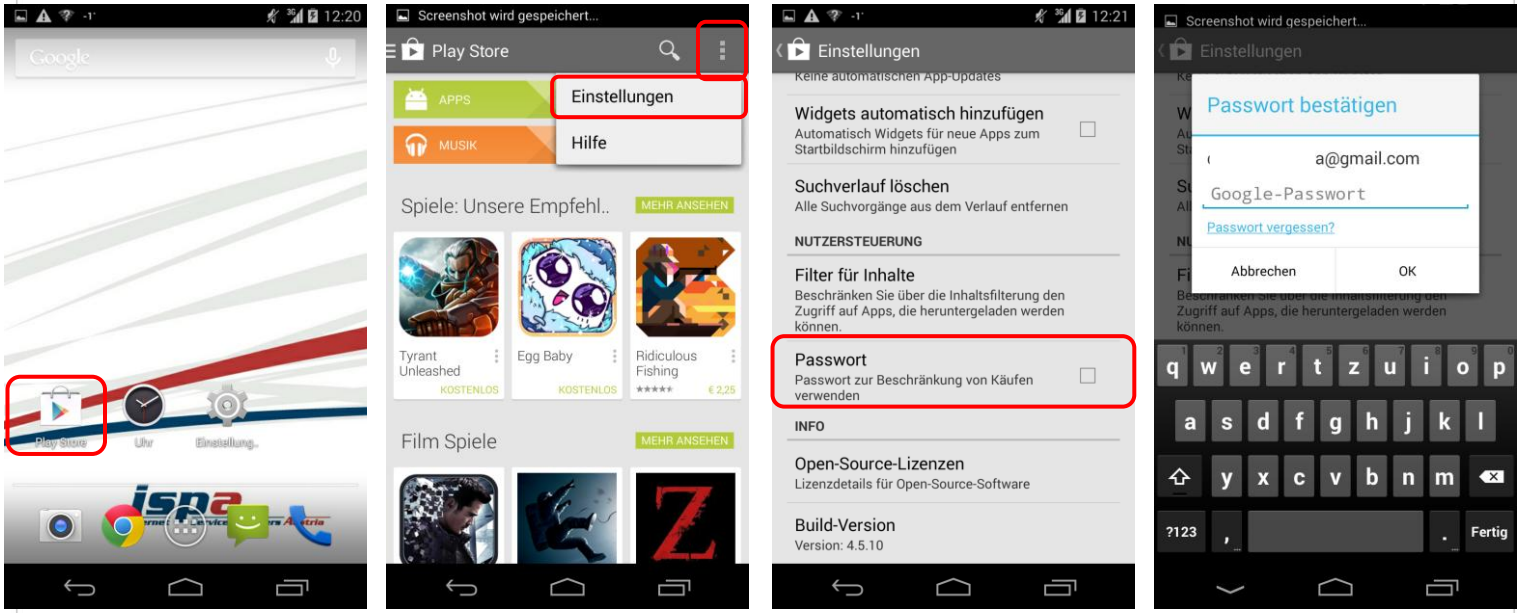
6. Kostenfalle In-App-Käufe

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 Smartphone und schalten Sie diese nur im Bedarfsfall und somit gezielt frei.

Sperre der In-App-Käufe:

Google Playstore – Einstellungen – Passwort

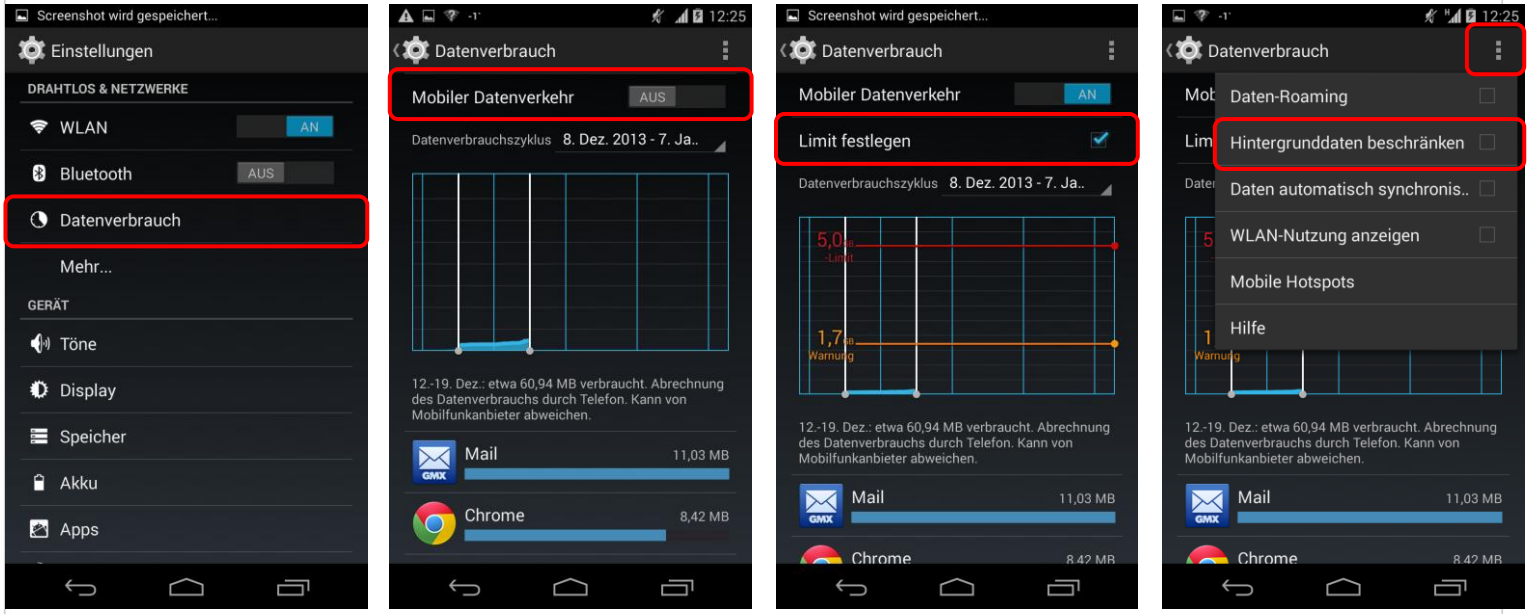


7. Kostenfalle Datentarife

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 Hintergrundsynchronisationen abzuschalten. Um Ihr limitiertes Internet-Paket zu

schonen, sollten Sie Updates und Synchronisierungen manuell über verfügbare Wlan-Netzwerke durchführen.

Datenvolumen beschränken:
Einstellungen – Datenverbrauch – Mobiler Datenverkehr

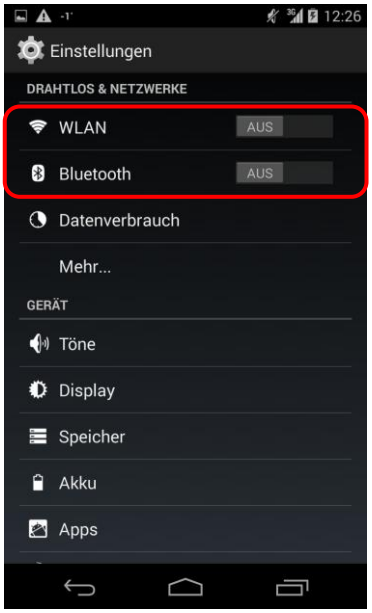


8. WLAN, Bluetooth und mobile Hotspots

„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:

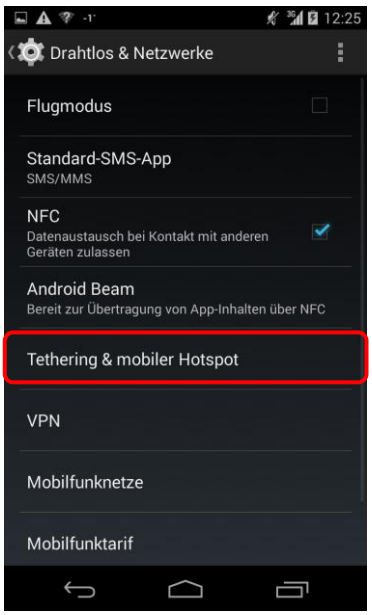
Einstellungen – WLAN
Einstellungen – Bluetooth

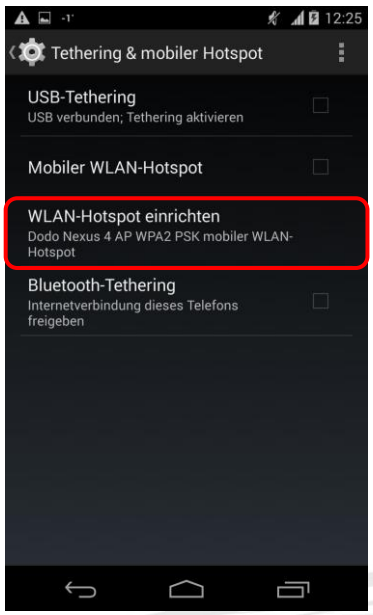


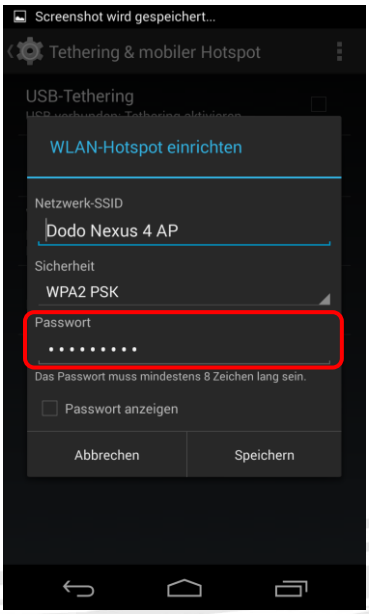
Viele Smartphones mit Datenverbindung bieten die Möglichkeit das Smartphone als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort sichern und ebenfalls nur bei Bedarf aktivieren.

Sicherheitseinstellungen für WLAN-Hotspot:

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







9. Jailbreak, Root und gesperrte Smartphones

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

Achtung: Durch das Rooten können die Betriebssysteme der Smartphones beeinträchtigt oder sogar beschädigt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Root-Programmen oder von Schadsoftware werden. Zudem fällt das Rooten in eine rechtliche Grauzone und kann unter Umständen die Garantie beeinträchtigen!

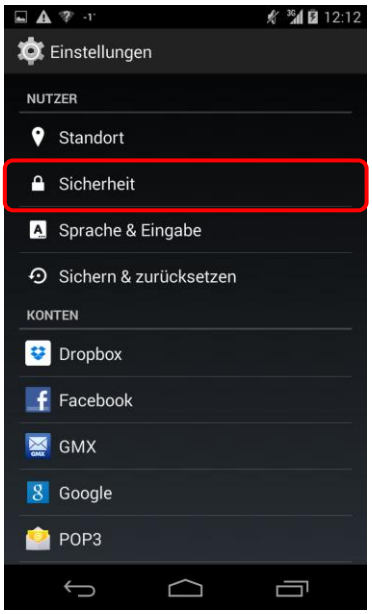
10. Datenverschlüsselung

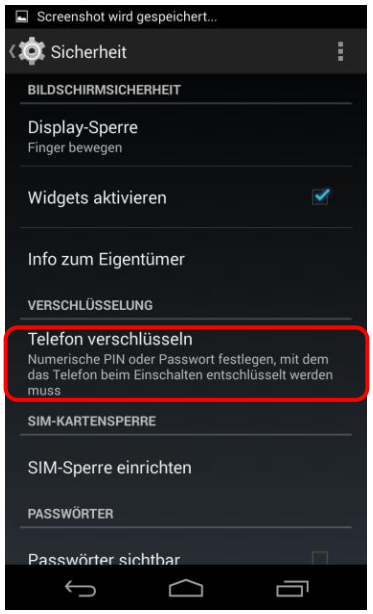
Viele Android-Smartphones bieten die Funktion der Datenverschlüsselung für die Micro-SD-Karte – wenn eine im Smartphone eingesetzt und in Verwendung ist. Damit können Sie Daten, welche extern – also auf Ihrer Micro-SD-Karte – gespeichert sind, zusätzlich schützen. Hier gibt es oftmals die Möglichkeit 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 Smartphone-Inhalte überlegen. Diese Option wird jedoch nicht von allen Smartphones unterstützt. Wird das Smartphone gestohlen oder geht es verloren, sind Konten, Einstellungen, Apps, Musik und Videos nur mit einem von Ihnen festgelegten PIN-Code einsehbar. Die Passwortabfrage erfolgt bei jedem Einschalten des Gerätes zusätzlich zur SIM-Codesperre.

Geräteverschlüsselung:

Einstellungen – Sicherheit – Telefon verschlüsseln





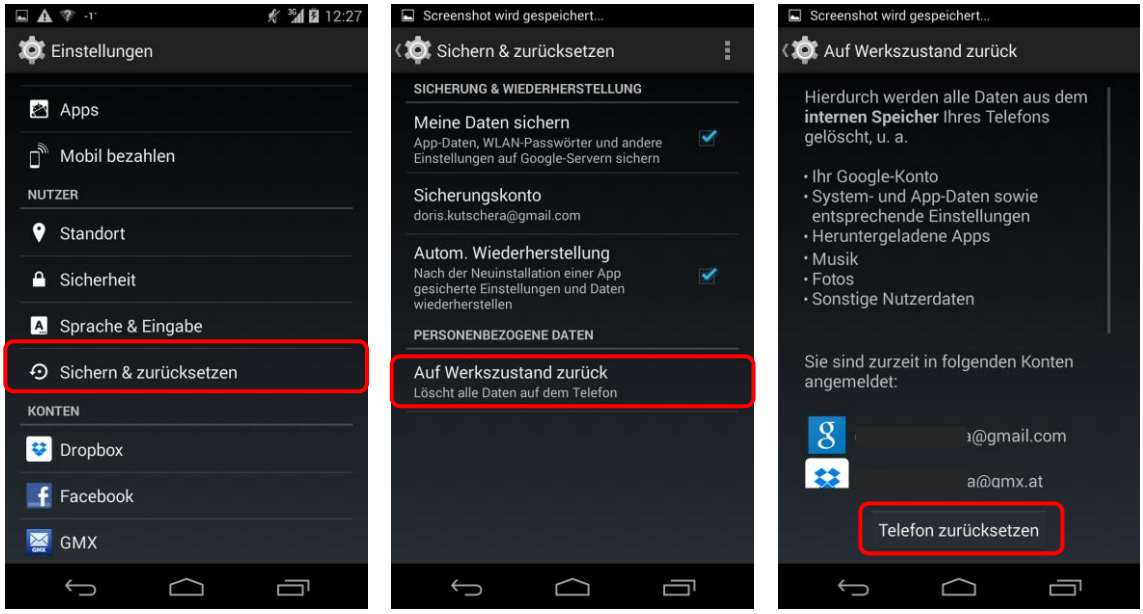
Achtung: Sie können die Verschlüsselung nicht rückgängig machen! Die Verschlüsselung kann nur aufgehoben werden, wenn Sie das Gerät auf den Werkzustand zurücksetzen, wodurch Ihre Daten gelöscht werden.

11. Verkaufen, Verschenken & Verborgen

E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: auf Ihrem 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 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 Smartphone 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:

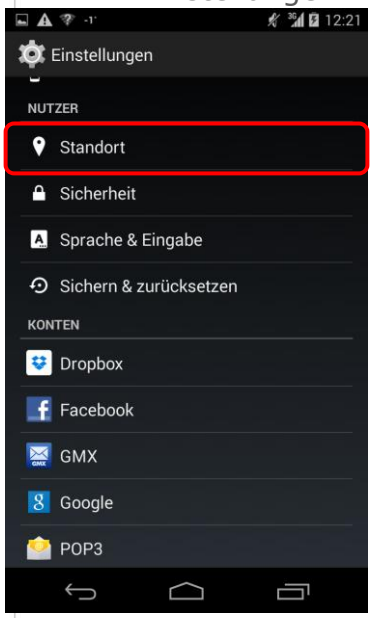
Einstellungen – Sichern & zurücksetzen – Auf Werkzustand zurück – Telefon zurücksetzen

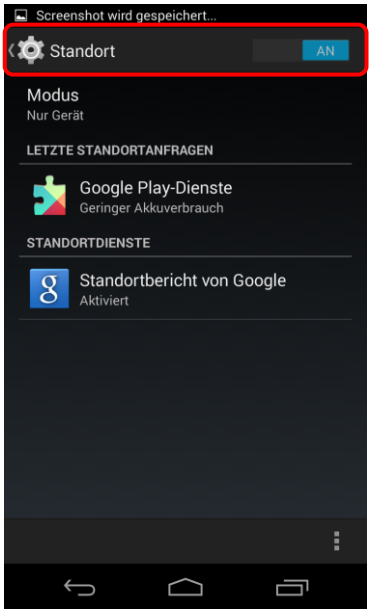


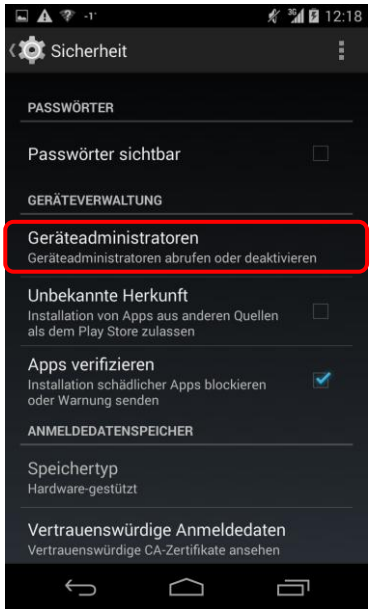
12. Smartphone-Finder: finden oder sperren

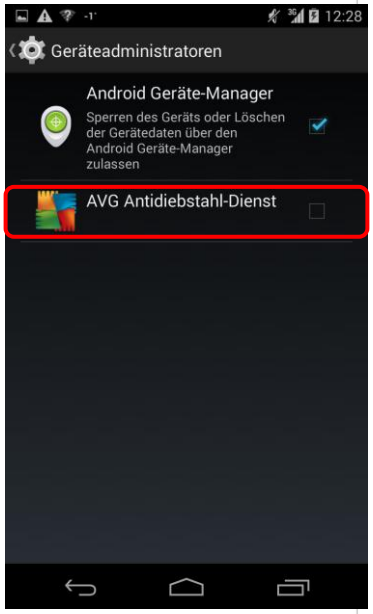
Die meisten Smartphones bieten die Möglichkeit es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen.
Android unterstützt diese Funktion. Bei Samsung Smartphones heißt diese z.B. „Fernzugriff" oder „Antidiebstahl-Dienst". Ist diese aktiviert, kann das Smartphone über das Konto bei Samsung geortet, gesperrt oder die Daten aus der Ferne gelöscht werden. Falls Ihr Smartphone diese Funktion nicht integriert hat, können Sie auch auf verschiedene Sicherheitsapps zurückgreifen. Bei Lokalisierungsfunktionen gilt es aber zwischen Privatsphäre und Sicherheit abzuwägen!

Telefonfinder aktivieren:
Einstellungen – Standort
Einstellungen – Sicherheit – Geräteadministratoren – Antidiebstahl-Dienst









13. Das kindersichere Smartphone

Um Ihr Smartphone bei Bedarf kindersicher zu machen, sollten Sie das Roaming sowie In-App-Käufe deaktivieren, den App-Filter auf jugendfrei stellen und ebenso Mehrwertdienste sperren. In letzter Konsequenz können Sie 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.