Sicherheitseinstellungen für Smartphones

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
2. aktualisierte Auflage.
iOS: 6.1.3
Android: 2.3.5, HTC Desire HD
Inhaltliche Verantwortung: Daniela Drobna

Gefördert durch die Europäische Union – Safer Internet Projekt

Wien, August 2013

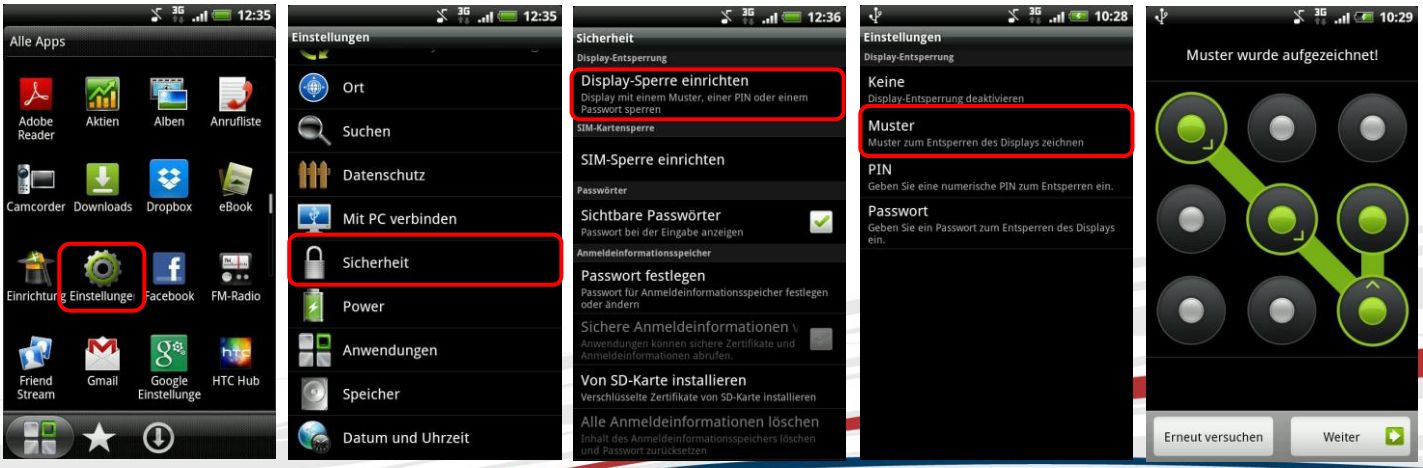
95% aller Österreicherinnen und Österreicher nutzen ein Mobiltelefon. Davon besitzt die Hälfte ein Smartphone, die Tendenz ist stetig steigend. Durch die höhere Verbreitung und das ständig wachsende Angebot an Nutzungsmöglichkeiten wird das Smartphone immer mehr zu einem personalisierten Gerät mit hoch 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. Alle Sicherheitsvorkehrungen werden anhand von Screenshots für die beiden gängigsten Betriebssysteme für Smartphones, iOS und Android, erklärt.

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.
Falls Ihnen die Eingabe eines PIN-Codes für das Deaktivieren der Bildschirmsperre zu umständlich erscheint, ist die Musterentsperrung eine gute Alternative. Hier legen Sie auf einer 3 x 3-Punkte-Matrix (oder alternativ 4 x 4-Punkte-Matrix) eine Verbindungslinie von mindestens vier Punkten fest. Zum Entsperren fahren Sie dann nur noch auf dem Touchdisplay die vorher festgelegte Linie nach. Diese Sperrmuster sind sehr beliebt, da sie schnell und leicht eingegeben werden können. Jedoch bieten sie einen schwächeren Schutz, da das Muster beim Eingeben unter Umständen leicht ausgespäht werden kann.

Bildschirmsperre bei Android:

Einstellungen – Sicherheit – Display-Sperre einrichten



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 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

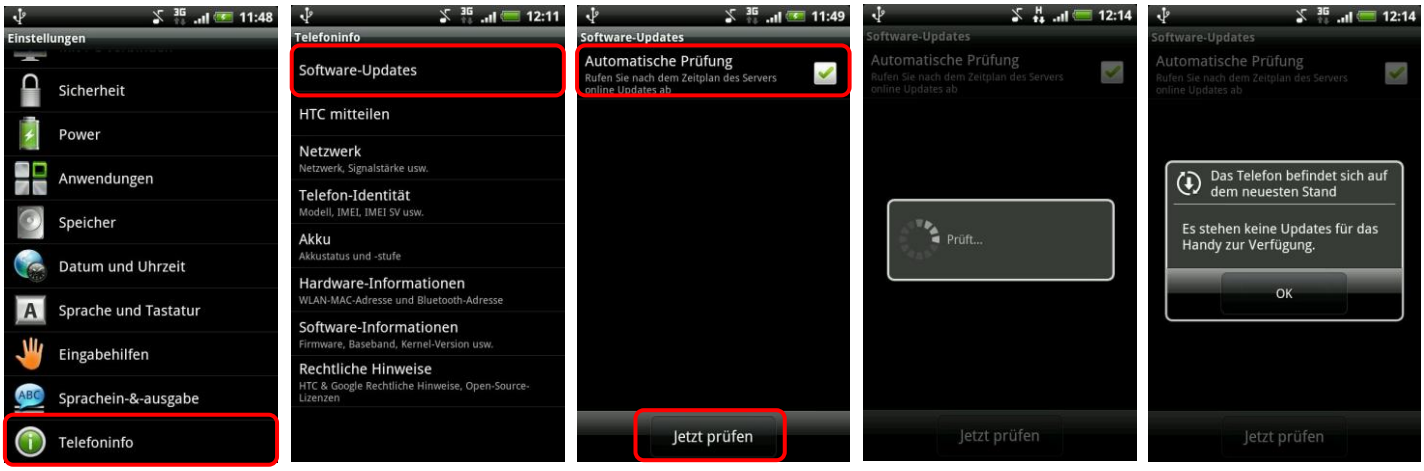
2. Software-Updates des Geräteherstellers

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.

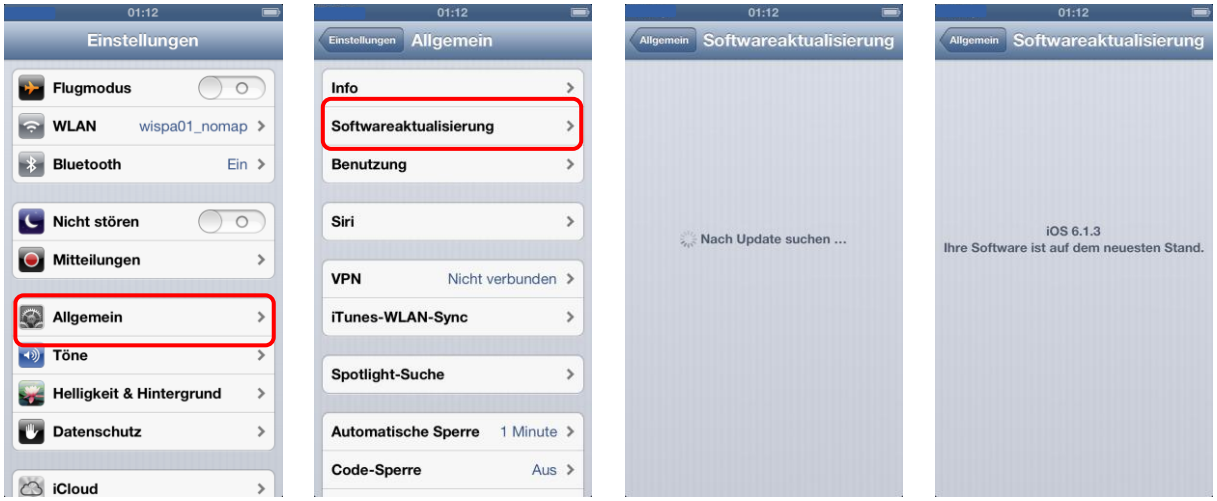
Suche nach Software-Updates bei Android:

Einstellungen – Telefoninfo – Software-Updates – Automatische Prüfung



Suche nach Software-Updates beim iPhone:

Einstellungen – Allgemein – Softwareaktualisierung

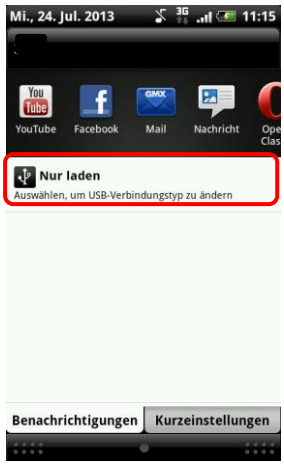


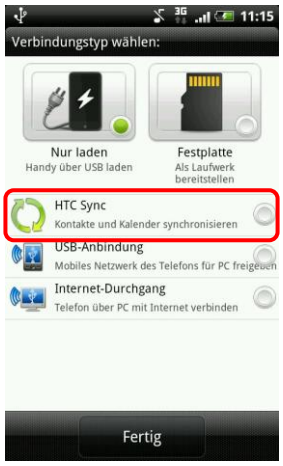
3. Synchronisierung & Backups

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.

Synchronisierung von Smartphone und PC bei Android:

Oberste Leiste runterziehen – Sync-Option auswählen





Synchronisierung von Smartphone und PC bei iPhone:

Einstellungen – iTunes-Wlan-Sync

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) und von Android (Google Playstore: http://play.google.com) 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.
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 bei Android:

Einstellungen – Anwendungen – 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 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. 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 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 eine richterliche Anordnung brauchen?
Bei der neuesten Android-Version 4.3 gibt es ein Feature zur Rechteverwaltung: hier können Sie einzelnen Apps bei der Installation erteilte Berechtigungen wieder entziehen.

Deaktivierung von GPS-Daten-Übermittlung bei Android:

Einstellungen – Ort – GPS-Satelliten verwenden

Deaktivierung von GPS-Daten-Übermittlung beim iPhone:

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.

5. Virenscanner

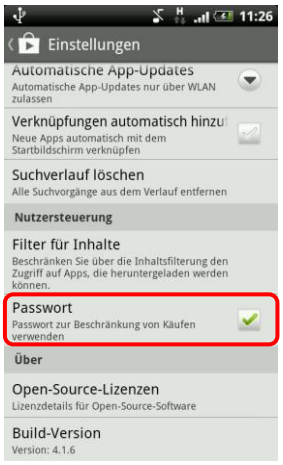
Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Handy-Banking bzw. Handy-Bezahlung verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Smartphone nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren bzw. beseitigen diese wenn möglich. Für das iPhone gibt es von Apple selbst nach wie vor kein Virenschutzprogramm. Somit kann 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 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 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 bei Android:

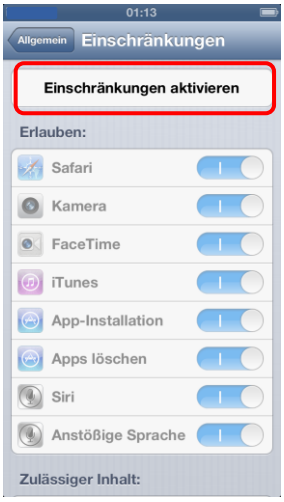
Google Playstore – Einstellungen – Passwort



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

Sperre der In-App-Käufe beim iPhone:

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

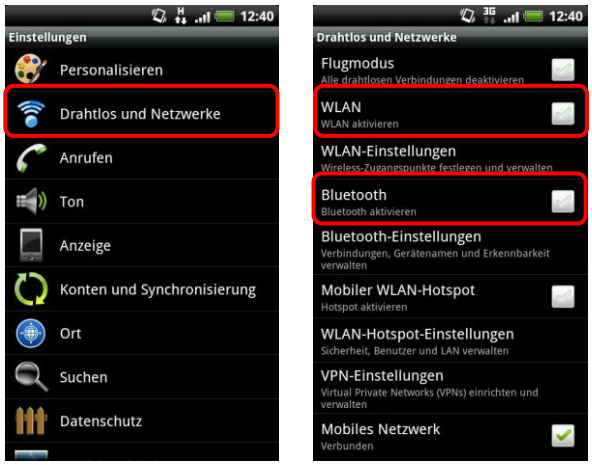
Datentarif mit begrenztem Internetvolumen haben, empfiehlt es sich den eigenen Verbrauch im Auge zu behalten.
Sollten Sie bei der Einschätzung Ihres Datenverbrauchs unsicher sein, können Sie sich für Ihr Smartphone eine App zur Kontrolle des Datenvolumens downloaden. Mittlerweile bieten die meisten Mobilfunkanbieter 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.
Das iPhone bietet zur Volumenkontrolle den Menüpunkt „Mobile Datennutzung", bei dem der eigene Verbrauch ermittelt werden kann.

8. WLAN, Bluetooth und mobile Hotspots

Wenn sich das Smartphone 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:

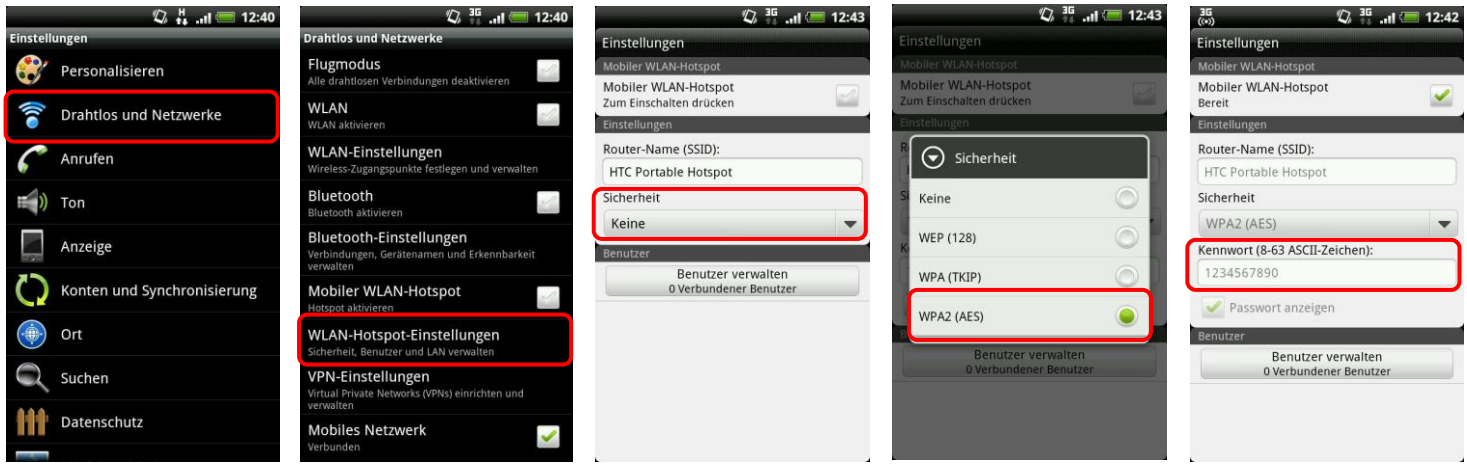
Einstellungen – Drahtlos und Netzwerke – WLAN/Bluetooth



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 sichern und ebenfalls nur bei Bedarf aktivieren.

Sicherheitseinstellungen für WLAN-Hotspot bei Android:

Einstellungen – Drahtlos und Netzwerke – WLAN-Hotspot-Einstellungen



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 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 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. 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 nur einzelne Inhalte zu verschlüsseln.

Datenverschlüsselung der Speicherkarte bei Android:

Einstellungen – Speicher – Speicherverschlüsselung

Möchten Sie Ihre Daten noch effektiver vor Missbrauch schützen, können Sie eine Datenverschlüsselung für alle Ihre Smartphone-Inhalte überlegen. Diese Option wird z.B. von Samsung-Smartphones unterstützt. Wird das Telefon 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.

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.

Auf Werkzustand zurücksetzen bei Android:

Einstellungen – Speicher – Auf Werkzustand zurück

Auf Werkzustand zurücksetzen beim iPhone:
Einstellungen – Allgemein – Zurücksetzen

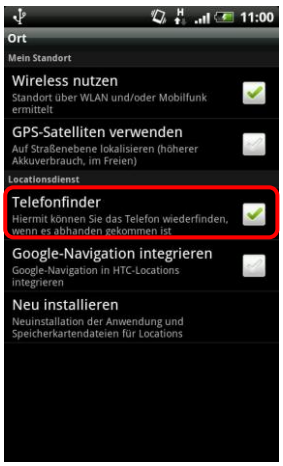
Um die Weitergabe Ihrer persönlichen Daten zu verhindern sollten Sie alle vorhandenen Speicher löschen, also nicht nur den internen Handyspeicher, sondern auch den externen (die Micro-SD-Karte). Hierfür reicht es nicht diese einfach nur zu löschen oder das Smartphone auf die Werkseinstellungen zurückzusetzen,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

12. Smartphone-Finder: finden oder sperren

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 „Find my iPhone"-Funktion integriert. Ist die Funktion auf dem Gerät aktiviert, ist die (ungefähre) Position des Smartphones über die iCloud einsehbar. Auch bei Android gibt es eine äquivalente Funktion, z.B. bei HTC Smartphones heißt diese „Telefonfinder". Ist diese aktiviert, kann über das Sense-Konto bei HTC das Smartphone lokalisiert werden.
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 bei Android (HTC):

Einstellungen – Ort – Telefonfinder



13. 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. 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.

Achtung: Bedenken Sie, dass bei iPhones 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.