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 3
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 10
10. Datenverschlüsselung 10
11. Verkaufen, Verschenken & Verborgen 11
12. Smartphone-Finder: finden oder sperren 11
13. Das kindersichere Smartphone 12

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
Inhaltliche Verantwortung: Daniela Drobna
Endgerät: Blackberry Q10
BS: Blackberry 10.2.1.537
Blackberry ist eine eingetragene Marke von Blackberry Limited.

Gefördert durch die Europäische Union – Safer Internet Projekt

Wien, Februar 2014

ispa Internet Service Providers Austria

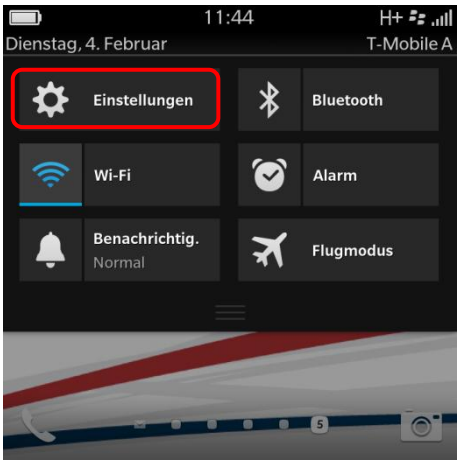
95% aller Österreicherinnen und Österreicher nutzen ein Mobiltelefon. Davon besitzt die Hälfte ein Smartphone, die Tendenz ist stetig steigend. Durch die höhere Verbreitung und das ständig wachsende Angebot an Nutzungsmöglichkeiten wird das Smartphone immer mehr zu einem personalisierten Gerät mit hoch 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 Fall eines Verlustes oder Diebstahls hilfreich sind.

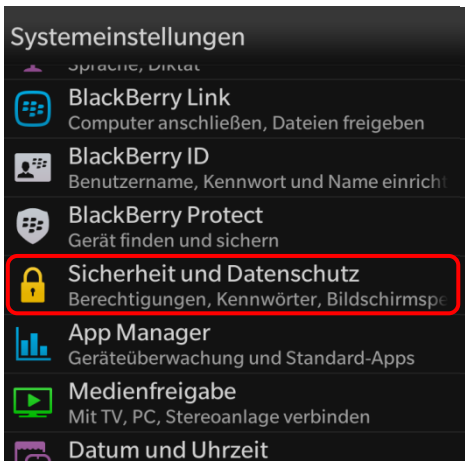
1. Doppelt hält besser: Passwortschutz am Smartphone

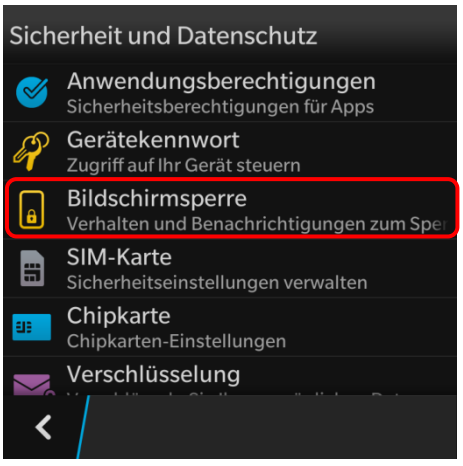
Mittlerweile gibt es bei jedem Smartphone die Möglichkeit das Gerät mittels Passwort zu schützen. Die meisten Smartphones bieten hier zwei Sicherheitsfunktionen an: einmal die PIN-Abfrage beim Einschalten des Gerätes (SIM-Kartensperre oder PIN-Eingabe) und als zusätzliche Option die Passwortabfrage bei 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 dreht sich der Bildschirm nach einiger Zeit automatisch ab, kann aber auch durch das Betätigen der Ein/Aus-Taste aktiviert werden. Die Bildschirmsperre kann nicht mit einem Kennwort versehen werden.

Bildschirmsperre bei BlackBerry:

Einstellungen – Sicherheit und Datenschutz – Bildschirmsperre





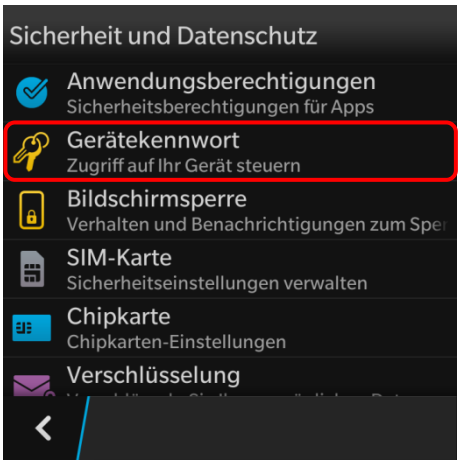


Blackberry bietet zusätzlich die Funktion der Gerätesperre, die Ihr Smartphone vor unberechtigter Verwendung schützt.
Bei der Gerätesperre haben Sie die Möglichkeit zwischen zwei Passwortarten zu wählen:

- Gerätekennwort
- Bildkennwort

Gerätekennwort bei BlackBerry:

Einstellungen – Sicherheit und Datenschutz – Gerätekennwort



Bildkennwort bei BlackBerry:

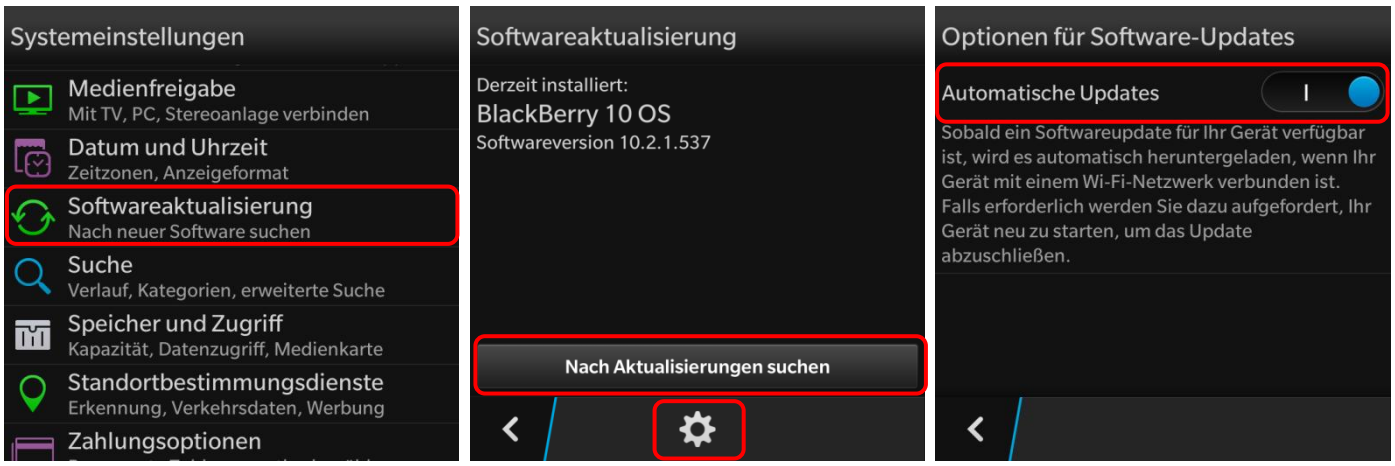
Einstellungen – Sicherheit und Datenschutz – Gerätekennwort - Bildkennwort

Beim Bildkennwort wählen Sie zuerst ein Bild aus und dann eine Zahl. Anschließend platzieren sie die Zahl an einer beliebigen Stelle des Bildes. Wenn Sie in Zukunft die Gerätesperre aufheben möchten, müssen Sie aus dem erscheinenden Zahlenraster Ihre gewählte Zahl an die zuvor gewählte Stelle ziehen.

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 – Softwareaktualisierung



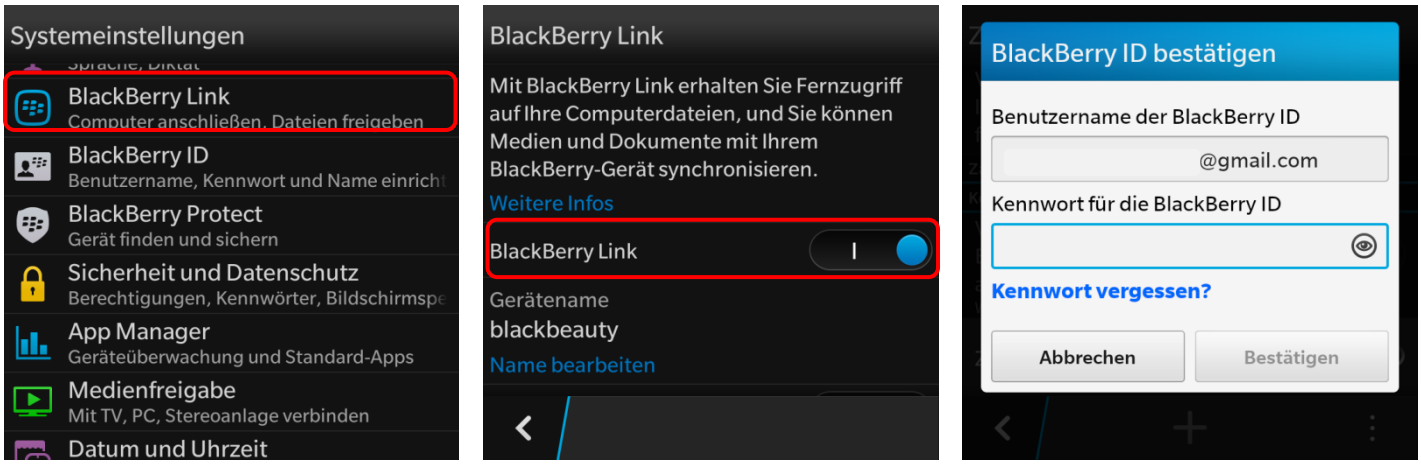
3. Synchronisierung & Backups

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

BlackBerry bietet mit der Funktion „BlackBerry Link" die Möglichkeit das Smartphone mit dem Pc zu synchronisieren. Hier können Dateien von Ihrem Smartphone auf den Computer übertragen und gesichert werden. Somit können Sie Ihre Inhalte einfach verwalten, teilen und im Bedarfsfall auch wiederherstellen. Um diese Funktion nutzen zu können, müssen Sie sich mit Ihrer BlackBerry ID anmelden und BlackBerry Link auch auf Ihrem Pc installieren.

Synchronisierung von Smartphone und PC:

Einstellungen – BlackBerry Link
(Verbinden Sie vorher das Smartphone per USB-Kabel mit dem Pc)



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), von Blackberry (BlackBerry World: http://appworld.blackberry.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 BlackBerry 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 BlackBerry komplett sperren.

Sperre unbekannter Quellen:

Einstellungen – App Manager – Installieren von Apps

Testen Sie Ihre Apps zuerst!

Ein weiterer Vorteil des Kaufes über die offiziellen Stores ist, dass Sie in den meisten Fällen ein Rückgaberecht haben. Bei der BlackBerry World haben Sie leider nicht die Möglichkeit der App-Rückgabe, können aber viele Anwendungen für einen begrenzten Zeitraum kostenlos testen. Die Probezeit und die Einschränkungen aller Funktionen können je nach App-Entwickler unterschiedlich ausfallen. Somit können Sie sich erst nach Ablauf dieser Testphase für den Kauf der Anwendung entscheiden.

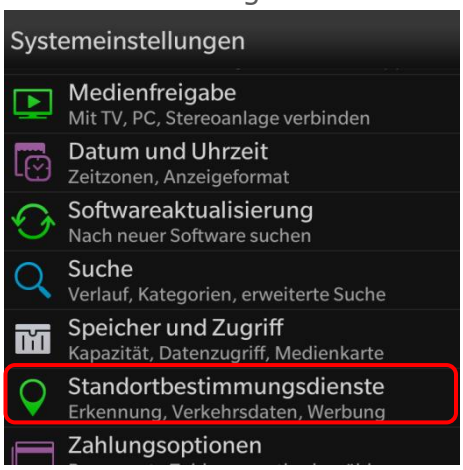
Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

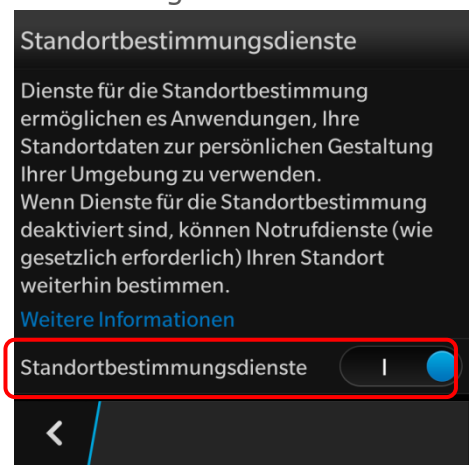
Vor der endgültigen Installation einer App müssen Sie deren Zugriffsberechtigungen zustimmen. Seien Sie hier vorsichtig und stimmen Sie Berechtigungen nur dann zu, wenn diese notwendig erscheinen. Bösartige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen,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

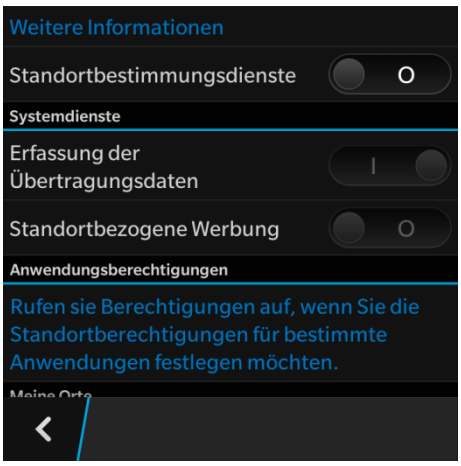
Wählen Sie ganz bewusst aus, welche Daten Sie welcher App zur Verfügung stellen wollen. Beispielsweise können Sie vorsehen, dass GPS-Daten Programmen wie einem Navigationssystem oder Routenplaner vorbehalten bleiben. Warum sollten Sie einer App Zugriff zu Daten gestatten, wofür staatliche Einrichtungen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

Deaktivierung von GPS-Daten-Übermittlung:

Einstellungen – Standortbestimmungsdienste



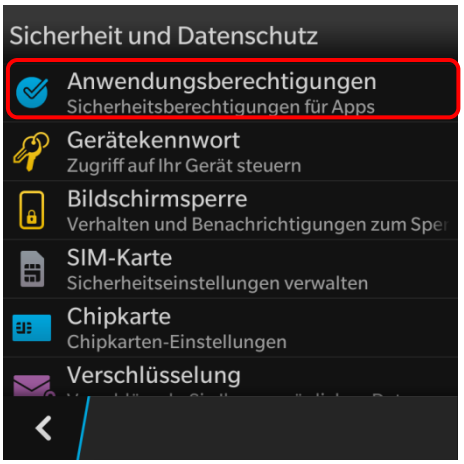


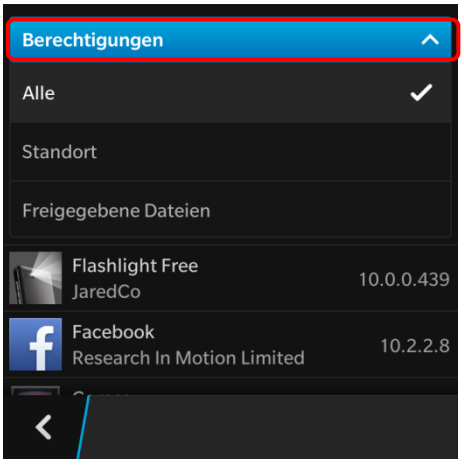


Achtung: Bei BlackBerry gibt es einen gesonderten Menüpunkt für die App-Berechtigungen! Auch wenn Sie die allgemeinen Standortbestimmungsdienste deaktiviert haben, kann es dennoch sein, dass einzelne Anwendungen Zugriff auf Ihren Standort haben (da Sie der App die Zugriffsrechte hierfür beim Download gegeben haben). Sie können diese Berechtigungen aber auch deaktivieren.

Deaktivierung des Standortzugriffs bei Apps:

Einstellungen – Sicherheit und Datenschutz – Anwendungsberechtigungen





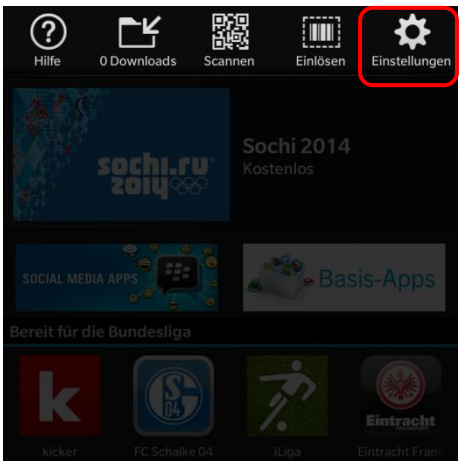
5. Virenscanner

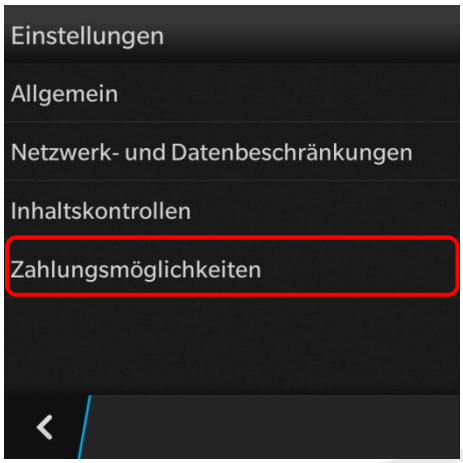
Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Online-Banking verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Smartphone nach Infektionen aller Art (Viren, Würmer und Trojaner) blockieren und beseitigen diese wenn möglich. Bei BlackBerry kann aus dem großen Pool der angebotenen Virenschutzprogramme gewählt werden, von BlackBerry selbst gibt es noch keine. 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!

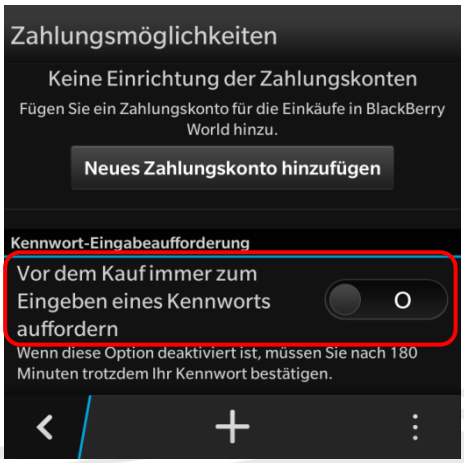
6. Kostenfalle In-App-Käufe

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.
Bei BlackBerry haben Sie die Möglichkeit den App-Kauf und den In-App-Kauf durch ein Kennwort zu sperren. Somit muss vor jedem Download oder kostenpflichtigen Kauf das selbstgewählte Kennwort eingegeben werden, unbeabsichtigte Käufe können so leicht verhindert werden.

PIN-Sperre für App-Kauf:
BlackBerry World – Einstellungen – Zahlungsmöglichkeiten – Kennwort





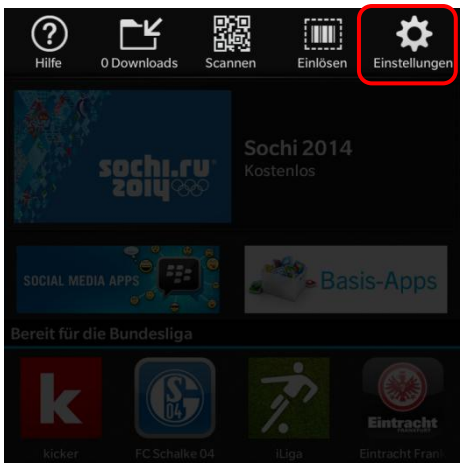


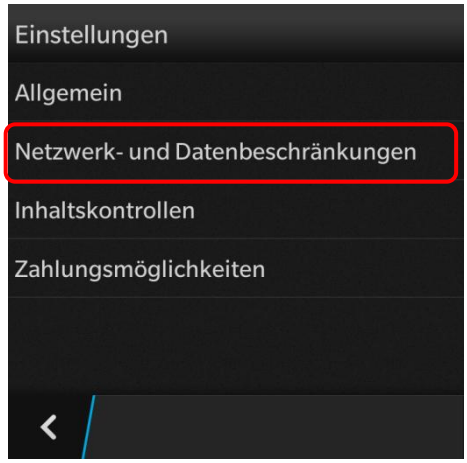
7. Kostenfalle Datentarife

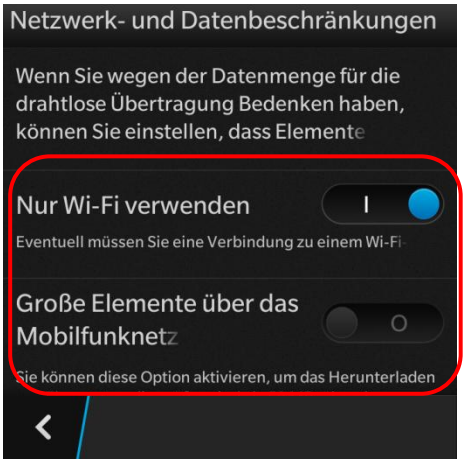
Viele Smartphone-Nutzerinnen und -Nutzer haben Handyverträge mit einem limitierten Internet-Paket, pro Monat können sie somit ein bestimmtes Datenvolumen verbrauchen. Wird dieses überschritten, wird es meistens teuer. Wenn Sie einen Datentarif mit begrenztem Internetvolumen haben, empfiehlt es sich den 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 größere Downloads manuell über verfügbare Wlan-Netzwerke durchführen. Bei BlackBerry können Sie vorsehen, dass große Elemente nicht über das Mobilfunknetz runtergeladen werden, sondern nur bei bestehender WLAN-Verbindung.

Netzwerk- und Datenbeschränkungen:

BlackBerry World – Einstellungen – Netzwerk- und Datenbeschränkungen





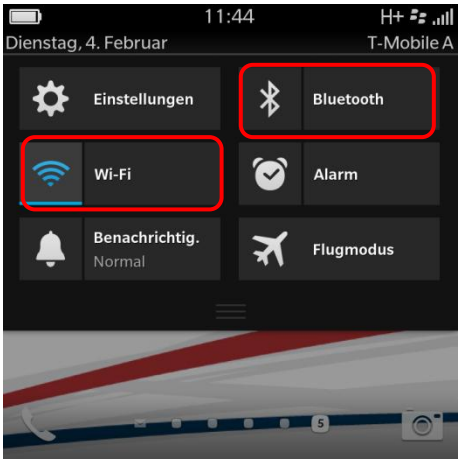


8. WLAN, Bluetooth und mobile Hotspots

„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:

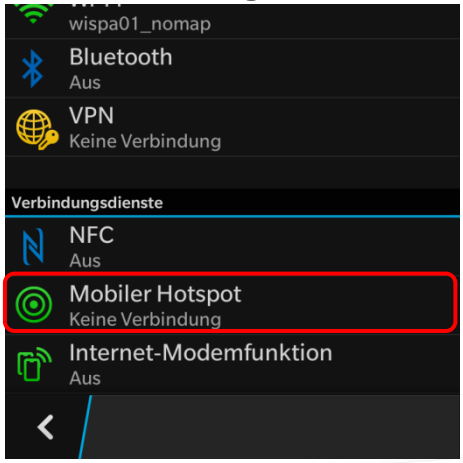
Einstellungen – Netzwerk und Verbindungen

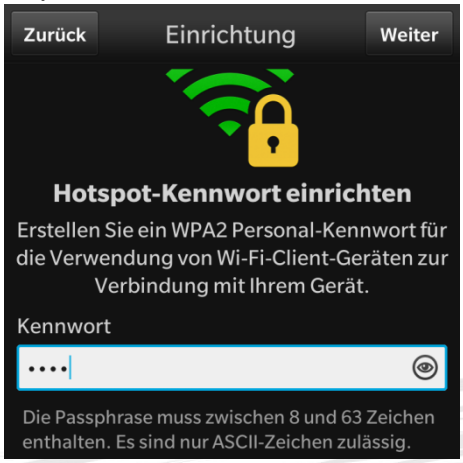


Viele Smartphones mit Datenverbindung bieten die Möglichkeit das Smartphone als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort sichern und ebenfalls nur bei Bedarf aktivieren.

Sicherheitseinstellungen für WLAN-Hotspot:

Einstellungen – Mobiler Hotspot





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.

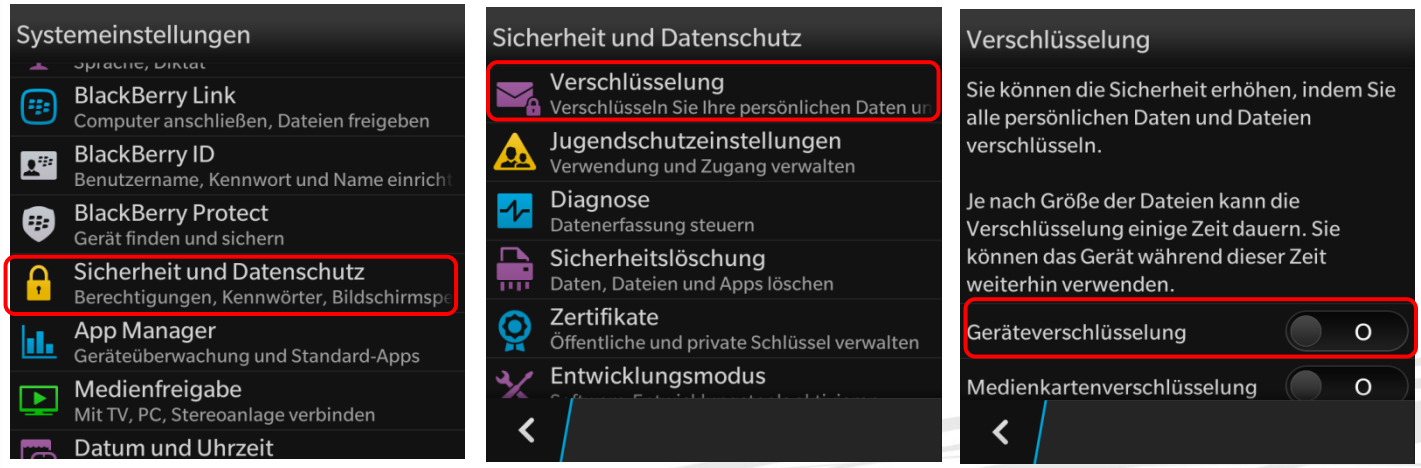
Achtung: Durch das Rooten können die Betriebssysteme der Smartphones beeinträchtigt oder sogar beschädigt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Root-Programmen oder von Schadsoftware werden. Zudem fällt das Rooten in eine rechtliche Grauzone und kann unter Umständen die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



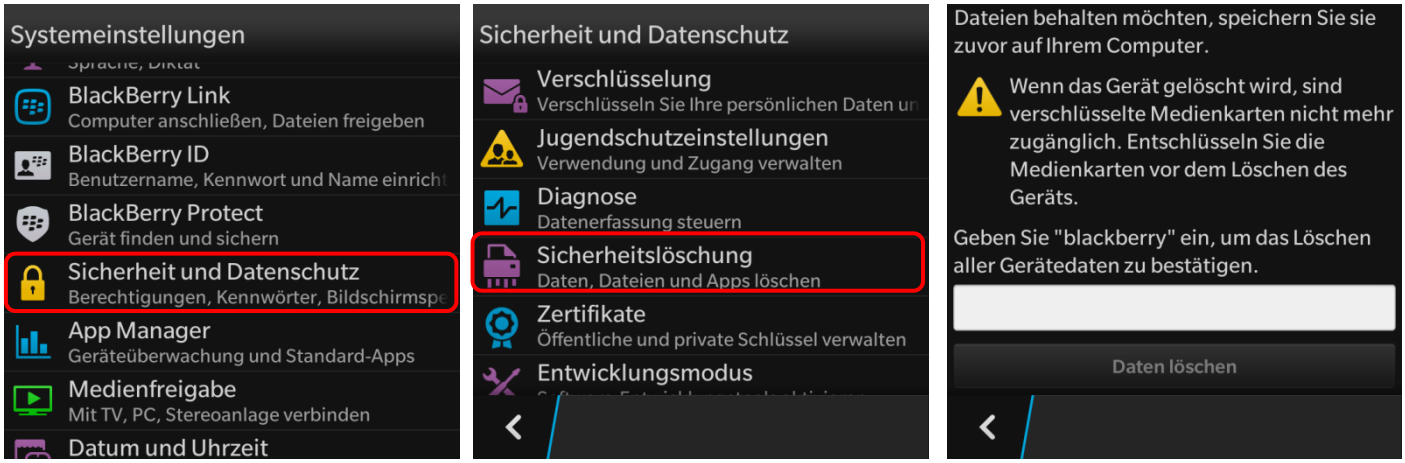
Achtung: Wird das Smartphone gelöscht, sind verschlüsselte Medienkarten nicht mehr zugänglich. Entschlüsseln Sie Medienkarte vor dem Löschen des Smartphones.

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 – Sicherheit und Datenschutz - Sicherheitslöschung



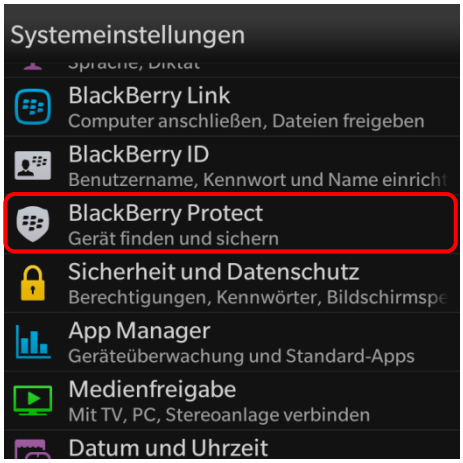
12. Smartphone-Finder: finden oder sperren

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.
Bei BlackBerry heißt diese Funktion „BlackBerry Protect". Ist diese aktiviert, kann das Smartphone über das Konto bei Samsung geortet, gesperrt oder die Daten aus der

Ferne gelöscht werden. Es gilt bei dieser Funktion zwischen Privatsphäre und Sicherheit abzuwägen: möchten Sie diese nutzen, müssen Sie die Standortbestimmung aktivieren.

Aktivierung des Telefonfinders:

Einstellungen – BlackBerry Protect



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.
Bei BlackBerry gibt es hierzu die Funktion „Jugendschutzeinstellungen". Hier können Sie nach dem Festlegen eines Kennwortes Einschränkungen für Ihr Smartphone einrichten. Sie können zum Beispiel vorsehen, dass Ihr Kind nur Anrufe und Textnachrichten von Personen aus den eingespeicherten Kontakten erhält. Ebenso können Sie bestimmte Anwendungen deaktivieren, sodass diese nicht mehr verwendet werden können. Dies reicht von App-Käufen über das Hochladen von Videos auf YouTube bis hin zur Löschung von Anwendungen.

Aktivierung der Jugendschutzeinstellungen:

Einstellungen – Sicherheit und Datenschutz – Jugendschutzeinstellungen