iKnow

kompakt

Christian Immler

Smartphone Security

Maximale Sicherheit für Ihr Android-Smartphone

DATA BECKER

Folgen Sie uns auf Facebook und Twitter:

www.facebook.com/databecker
www.twitter.com/data_becker

Besuchen Sie unseren Internetauftritt:

www.databecker.de

Wichtiger Hinweis

Die Nutzung des Onlineangebots steht nur dem erst-registrierenden Käufer dieses Buches zur Verfügung, setzt den Erwerb und Besitz des Buches durch den registrierten Käufer voraus und ist nicht übertragbar.

Die DATA BECKER GmbH & Co. KG behält sich somit auch alle Rechte auf Vervielfältigung, Vermietung, Verleih sowie eine öffentliche Zugänglichmachung dieser Werkkopie und/oder anderer Kopien dieses Werks einschließlich der Wiedergabe an elektronischen Leseplätzen in öffentlichen Bibliotheken, Museen und Archiven ausdrücklich vor. Solche Nutzungshandlungen sind ohne eine auf Antrag im Einzelfall in Textform erteilte ausdrückliche vorherige Zustimmung untersagt.

Die in diesem Buch wiedergegebenen Verfahren und Programme werden ohne Rücksicht auf die Patentlage mitgeteilt. Sie sind für Amateur- und Lehrzwecke bestimmt.

Alle technischen Angaben und Programme in diesem Buch wurden von den Autoren mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. DATA BECKER sieht sich deshalb gezwungen, darauf hinzuweisen, dass weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernommen werden kann. Für die Mitteilung eventueller Fehler sind die Autoren jederzeit dankbar.

Wir weisen darauf hin, dass die im Buch verwendeten Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Inhalt

Die besten Tipps für mehr Android-Sicherheit

Liebe Leserin, lieber Leser,

Android-Smartphones enthalten heute jede Menge persönlich wichtige Daten, die nicht unbedingt in fremde Hände geraten sollten – sei es durch bösartige Software oder unbefugte Personen.

Da wundert es nicht, dass diese Geräte genauso wie PCs zum Ziel von Internetkriminellen, Spionen und Werbetreibenden geworden sind, die die Benutzer aushorchen wollen.

Nicht zuletzt sind Smartphones auch beliebte Diebesgüter, die sich auf Schwarzmärkten schnell zu Geld machen lassen.

Diese E-Book zeigt Ihnen, wie Sie sich diesen Bedrohungen widersetzen und in Sicherheit Spaß mit dem Android-Smartphone haben werden.

Christian Immler

Fünf Sofortmaßnahmen zur Absicherung des Smartphones

1. Handy mit SIM-Karten-PIN sperren

Jedes Handy wird üblicherweise durch die PIN der SIM-Karte geschützt und lässt sich nur einschalten, nachdem diese PIN eingegeben wurde. Auf Android-Smartphones lässt sich die PIN-Eingabe auf Wunsch auch abschalten.

Jede SIM-Karte wird durch zwei verschiedene PINs (Persönliche Identifikationsnummern) geschützt. Diese PINs sind abhängig von der SIM-Karte und nicht vom Telefon, sie werden vom Mobilfunknetzbetreiber mit der SIM-Karte geliefert. Die PIN1 wird beim Einschalten des Telefons gebraucht. Die PIN2 wird im Wesentlichen nur zur Freischaltung spezieller kostenpflichtiger Dienste benötigt. Beide PINs können vom Benutzer geändert werden.

1. Um die PIN1 (häufig einfach nur als PIN bezeichnet) zu ändern, tippen Sie in den Einstellungen auf der Seite *Optionen* auf *Sicherheit*. Über den Punkt *SIM-PIN Optionen* ändern Sie die PIN. Zur Sicherheit muss zuerst die alte PIN eingegeben und die neue ein zweites Mal bestätigt werden.
2. An der gleichen Stelle können Sie festlegen, ob beim Einschalten des Smartphones die Eingabe der PIN erforderlich ist oder nicht.

Wenn man die PIN vergisst oder mehrfach falsch eingibt, sperrt sich die SIM-Karte selbstständig und kann nur noch mit der Super-PIN oder PUK (Personal Unblocking Key) wieder freigeschaltet werden. Der PUK kann vom Benutzer nicht verändert werden.

Zum Ändern der PIN2 sowie zum Entsperren einer durch mehrere Fehleingaben gesperrten PIN müssen sogenannte GSM-Codes eingegeben werden, hier gibt es keinen Menüpunkt.

Starten Sie die Telefon-App und geben Sie die Codes mit der Zifferntastatur wie eine Telefonnummer ein.

1. Um die PIN zu ändern, benötigen Sie die bisherige PIN und müssen die neue PIN aus Sicherheitsgründen zweimal eingeben:

   ```
   **04*[alte PIN]*[neue PIN]*[neue PIN]#
   ```

2. Um die PIN2 zu ändern, benötigen Sie die bisherige PIN2 und müssen die neue PIN2 aus Sicherheitsgründen ebenfalls zweimal eingeben:

   ```
   **042*[alte PIN2]*[neue PIN2]*[neue PIN2]#
   ```

3. Wurde die PIN durch Fehleingaben gesperrt, benötigen Sie den PUK, um eine neue PIN festzulegen, ohne die bisherige zu kennen:

   ```
   **05*[PUK]*[neue PIN]*[neue PIN]#
   ```

4. Wurde die PIN2 durch Fehleingaben gesperrt, benötigen Sie ebenfalls den PUK, um eine neue PIN2 festzulegen, ohne die bisherige zu kennen:

   ```
   **052*[PUK]*[neue PIN2]*[neue PIN2]#
   ```

Eine Änderung des PUK ist nicht möglich. Verlieren Sie diesen also nie. Heben Sie am besten den Originalbeleg mit den PINs an einem sicheren Ort auf. Sie brauchen den PUK nur im Notfall. Allgemein reicht immer die PIN.

2. Sperren mit System-PIN

Alle Android-Smartphones haben eine Bildschirmsperre, die verhindert, dass man versehentlich auf den Bildschirm tippt und damit irgendwelche Funktionen auf dem Handy auslöst. Diese Sperre lässt sich in der Standardeinstellung durch eine kleine Bewegung mit dem Finger auf dem Sperrbildschirm lösen.

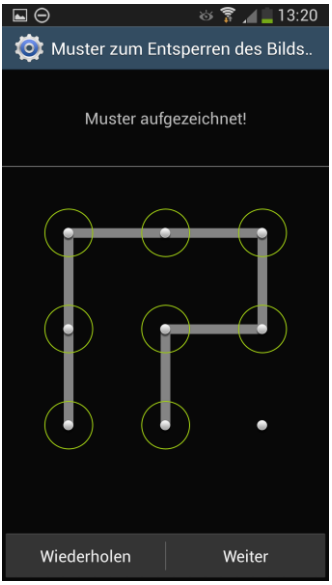
Der Sperrbildschirm dient nicht nur als Schutz vor versehentlichem Berühren, er kann auch als Zugangssperre eingesetzt werden, um Fremden die Nutzung des Smartphones zu verweigern.

1. In den Einstellungen haben Sie unter *Mein Gerät/Sperrbildschirm* verschiedene Möglichkeiten, einen Zugangsschutz einzurichten. Die Standardeinstellung wird hier als Wischen oder Streichen bezeichnet.
2. Wer es vom PC gewohnt ist, bei jedem Einschalten ein Passwort oder eine PIN einzugeben, kann dies auch auf dem Smartphone tun. Beim Festlegen der PIN oder des Passworts muss dieses zweimal eingegeben werden, um Tippfehler zu vermeiden. Auf dem Sperrbildschirm erscheint dann ein Eingabefeld.
3. Möchten Sie später wieder auf eine andere Methode der Bildschirmsperre umschalten, muss aus Sicherheitsgründen die PIN noch einmal eingegeben werden.

Unterschied zwischen PIN und Passwort

Eine PIN (Persönliche Identifikationsnummer) ist eine Zahlenkombination, ein Passwort kann aus beliebigen Zeichen bestehen. Android unterscheidet diese beiden Verfahren, um bei einer PIN-Eingabe eine Zifferntastatur mit deutlich größeren Tasten einzublenden als bei der Buchstabentastatur für die Passworteingabe.

3. Komfortabler sperren mit Fingergeste



Viel eleganter und einfacher als die Eingabe eines Passworts ist ein grafisches Sperrmuster. Hier muss man bis zu neun vorgegebene Rasterpunkte auf dem Bildschirm per Fingergeste mit einer Linie verbinden.

1. Wählen Sie in den Einstellungen für den Sperrbildschirm die Option *Muster* und zeichnen Sie mit dem Finger das gewünschte Entsperrmuster.
2. Um Fehler zu vermeiden, muss auch dieses Muster beim Einrichten zweimal gezeichnet werden.
3. Danach legen Sie noch eine Sicherungs-PIN fest, die Sie eingeben können, sollten Sie das Entsperrmuster vergessen haben.

Beim Einschalten des Smartphones erscheint dann auf dem Sperrbildschirm ein Punktraster, auf dem man das zuvor definierte Muster zeichnen muss, um die Bildschirmsperre zu lösen. Sollten Sie das Muster nicht mehr wissen oder nicht korrekt eingeben können, haben Sie noch die Möglichkeit, die zuvor festgelegte Sicherungs-PIN zum Freischalten zu verwenden.

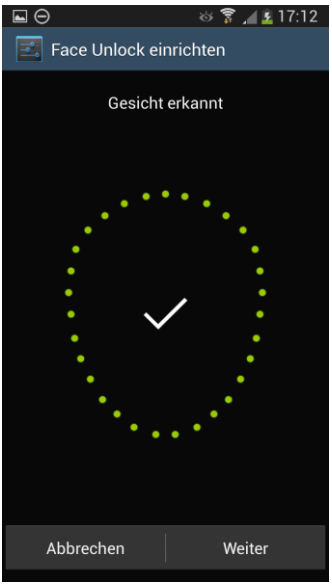
Sollten Sie einmal sowohl das Muster als auch die Sicherungs-PIN vergessen haben, ist immer noch nicht alles verloren. Nachdem mehrfach ein falsches Muster eingegeben wurde, erscheint unten rechts auf dem Sperrbildschirm ein Feld *Muster vergessen?* Tippen Sie darauf, brauchen Sie nur die Daten Ihres Google-Kontos einzugeben, und das Smartphone wird wieder entsperrt.

Notruf immer möglich

Notrufe sind immer möglich und immer kostenlos, auch wenn das Handy mit einem Sperrmuster oder einer PIN geschützt ist. Im Handy muss dazu aber eine SIM-Karte eingelegt sein. Auf dem Sperrbildschirm befindet sich dazu eine Schaltfläche *Notruf*.

4. Persönliche Sperre mit Gesichtserkennung

Viele Android-Handys lassen sich auch entsperren, indem Sie das Gerät einfach nur ansehen. Die Frontkamera erkennt ein gespeichertes Gesicht und gewährt genau dieser Person Zugriff auf das Smartphone, anderen aber nicht.



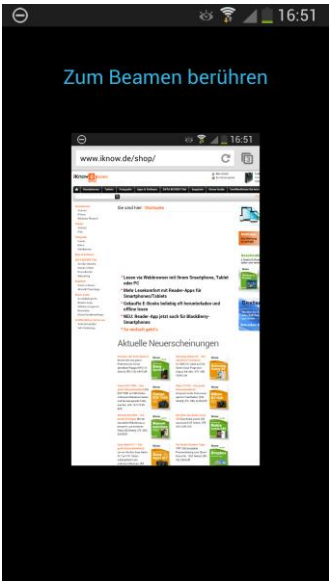
1. Wählen Sie in den Einstellungen für den Sperrbildschirm die Option *Gesichts-Entsperrung*, erscheint nach zwei Hinweisseiten das Bild der Frontkamera.
2. Halten Sie das Gerät so, dass Ihr Gesicht innerhalb des Rahmens liegt. Die Gesichtserkennung startet, was an wandernden grünen Punkten entlang des ovalen Rahmens zu erkennen ist. Wenn das Gesicht erkannt wurde, erscheint eine entsprechende Meldung.
3. Danach legen Sie noch eine alternative Entsperrmethode fest, falls später bei der Anmeldung kein Gesicht erkannt wird – ein Muster oder eine PIN.

Auf dem Sperrbildschirm erscheint jetzt beim Einschalten ein Kamerafeld. Blicken Sie dort hin, wird das Smartphone sofort entsperrt. Konnte einige Sekunden lang kein gültiges Gesicht erkannt werden, verwenden Sie die zuvor festgelegte alternative Entsperrmethode.

Gesichtserkennung noch zuverlässiger

In den Einstellungen für den Sperrbildschirm können Sie die Gesichtserkennung noch verbessern, indem Sie weitere Bilder aufnehmen, zum Beispiel mit Brille oder ohne oder bei unterschiedlichen Lichtverhältnissen. Die Anwesenheitsprüfung ist eine zusätzliche Sicherheitsfunktion. Ist diese eingeschaltet, müssen Sie während der Gesichtserkennung blinzeln. Damit wird verhindert, dass jemand Ihr Handy mit einem Foto von Ihnen entsperrt.

5. NFC-Koppelung sicherer als Bluetooth



Kleine Datenmengen wie z. B. ein Weblink, eine Visitenkarte oder eine Position in Google Maps lassen sich per NFC deutlich sicherer übertragen als per Bluetooth. Die Abkürzung NFC steht für Near Field Communication, ein Verfahren zur Datenübertragung über wenige Zentimeter und kann aufgrund der geringen Reichweite kaum ausspioniert werden. Diese Gefahr ist bei Bluetooth mit mehreren Metern Reichweite deutlich höher.

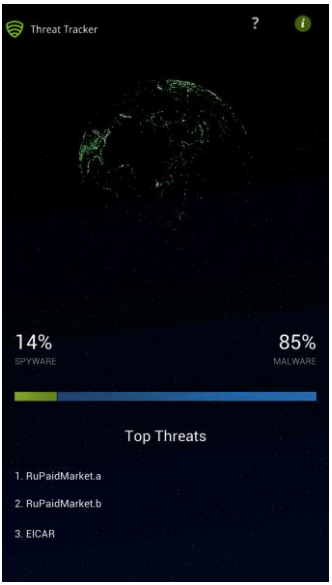
1. Schalten Sie in den Einstellungen auf der Seite *Verbindungen* den Schalter *NFC* ein, bei Samsung-Smartphones zusätzlich auch noch *S Beam*.
2. Starten Sie die App, mit der Sie Daten übertragen möchten, und lassen Sie sich dort die Daten anzeigen, die übertragen werden sollen, z. B. ein Adressbucheintrag, ein Weblink oder ein Kartenausschnitt in Google Maps.
3. Halten Sie jetzt die beiden Smartphones mit den Rückseiten gegeneinander, bis sie sich berühren. Auf dem Bildschirm erscheint *Zum Beamen berühren*. Tippen Sie auf den verkleinerten Screenshot.
4. Auf dem anderen Smartphone erscheint eine Meldung, wie die Daten angenommen werden sollen. Gibt es nur eine Möglichkeit, weil z. B. nur ein Browser installiert ist oder ein Standardbrowser eingerichtet ist, wird dieser sofort gestartet.

Verwendung von NFC im Alltag

NFC wird wegen seiner besonderen Sicherheit zum drahtlosen Bezahlen an Kassenterminals und für Zugangskontrollen verwendet. Die Deutsche Bahn nutzt dieses Verfahren für die elektronischen Fahrkarten im Touch-and-Travel-System. Zur Übertragung größerer Datenmengen ist NFC wegen seiner langsamen Übertragungsrate von nur 424 Kbit/s nicht geeignet.

Vorsicht vor bekannten Gefahren

Das sind die größten Sicherheitsprobleme



Onlinekriminelle greifen dort an, wo es sich lohnt – und das sind nicht mehr nur PCs. Daher ist es nicht verwunderlich, dass Android-Smartphones und Tablets immer stärker in den Fokus der Malware-Autoren rücken.

Die Kriminellen versenden Kurznachrichten an teure Rufnummern und haben es auf persönliche Daten der Nutzer abgesehen, z. B. Kontakte und Telefonnummern, und das Anmelden bei kostenpflichtigen Diensten. So kann ein Angriff auf dem Smartphone sehr schnell viel teurer werden als ein Virus auf dem PC.

1. Das größte Sicherheitsproblem bei Smartphones sind die Nutzer und weniger die Technik. Installieren Sie nicht ohne Nachzudenken irgendwelche Apps. Besonders kostenlose Apps, die Funktionen versprechen, die das Smartphone technisch gar nicht leisten kann, sind extrem verdächtig.
2. Auch ein zweites Problem ist eher menschlich: Phishing in E-Mails und sozialen Netzen. Auf dem Handy sind gefälschte Links schwerer zu erkennen als in einem E-Mail-Programm auf dem PC. Lesen Sie Mails noch genauer. Besonders falsche Rechtschreibung deutet auf Phishing hin.
3. Das größte Sicherheitsrisiko ist Rooting. Viele Medien versprechen unbedarften Nutzern damit Wunder. Tatsächlich öffnen Sie mit Rooting alle sicherheitskritischen Bereiche des Smartphones und machen es damit extrem anfällig für Malware.

Persönliche Daten auf dem Telefon verschlüsseln

Wer ein Android-Handy klaut, kommt auch an die darauf gespeicherten Daten. Selbst wenn das Handy über eine PIN oder ein Entsperrmuster geschützt ist, sind die Daten auf dem Handy über einen Entwicklerzugang per USB-Kabel auslesbar. Noch einfacher geht es mit den Daten auf der Speicherkarte. Diese braucht nur in einen Kartenleser am PC gesteckt zu werden.

1. Wer auf seinem Smartphone höchst vertrauliche Daten speichert, kann die für Benutzer zugänglichen Teile des Dateisystems wie auch die Speicherkarte verschlüsseln. Ohne das Passwort kommt man dann auch über externe Wege nicht an die Daten heran.
2. Verschlüsselung funktioniert nur, wenn eine Passwortsperre auf dem Handy eingerichtet ist. Das Passwort muss, da es direkt zur Verschlüsselung verwendet wird, aus mindestens sechs Zeichen bestehen, darunter mindestens eine Ziffer.
3. Die Einstellungen zur Verschlüsselung finden Sie in den Einstellungen unter *Sicherheit*. Hier können Sie den Gerätespeicher und die SD-Karte unabhängig voneinander verschlüsseln. Beachten Sie dabei die Sicherheitshinweise auf dem Bildschirm.

Nicht auf allen Smartphones

Einige Handyhersteller, wie z. B. HTC oder LG, haben die Verschlüsselungsfunktion im Betriebssystem deaktiviert. Diese Geräte lassen sich nicht verschlüsseln.

Vorsicht bei Bluetooth-Übertragungen

Bluetooth bietet die Möglichkeit, Daten direkt zwischen zwei Geräten, Smartphones, Tablets oder auch einfachen Handys und PCs zu übertragen, ohne dass eine Internetverbindung nötig ist. Allerdings kann Bluetooth auch leicht missbraucht werden, um bösartige Inhalte auf fremde Smartphones zu installieren. Daher haben die Bluetooth-Spezifikation selbst und auch das Android-Betriebssystem diverse Sicherheitsmechanismen eingebaut.

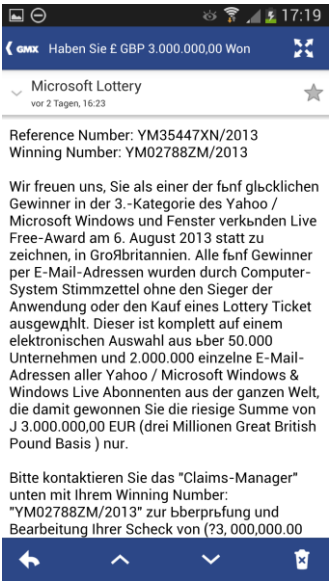
1. Bluetooth muss auf beiden Geräten eingeschaltet sein. Das Gerät, das die Daten empfangen soll, muss auf sichtbar geschaltet sein, damit das sendende Gerät es finden kann.
2. Schalten Sie in den Einstellungen unter *Netzwerke* bzw. *Verbindungen* Bluetooth ein und auf sichtbar. Aus Sicherheitsgründen schaltet Android nach zwei Minuten automatisch wieder auf unsichtbar. In dieser Zeit sollten sich die Geräte gefunden haben.
3. Bevor eine Datei übertragen werden kann, erscheint auf dem empfangenden Gerät eine Sicherheitsabfrage. Beantworten Sie diese nur, wenn Sie den Absender und die Datei kennen.

Auf den meisten Smartphones können Sie Bluetooth über ein Symbol in der heruntergezogenen Benachrichtigungsleiste direkt ein- und ausschalten, ohne den Umweg über die Einstellungen. Auf Samsung-Smartphones erreichen Sie die Bluetooth-Einstellungen einfach über langes Antippen des Bluetooth-Symbols in der Benachrichtigungsleiste.

Stromfresser Bluetooth

Bluetooth benötigt sehr viel Strom. Lassen Sie es am besten immer ausgeschaltet und schalten Sie es nur ein, wenn Sie es wirklich brauchen. Solange Bluetooth ausgeschaltet ist, sind Sie auch keinem diesbezüglichen Sicherheitsrisiko ausgesetzt.

Phishing bei E-Mails und sozialen Netzen



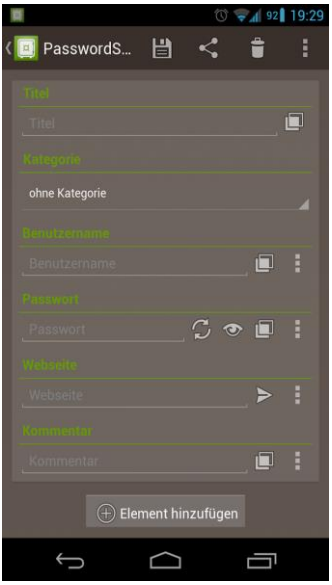
Phishing ist eine kriminelle Methode, mit der Betrüger versuchen, an Passwörter und private Daten zu kommen. Dabei werden keine technischen Mittel eingesetzt, um Passwörter zu knacken, sondern man versucht, Benutzer geschickt zu überzeugen, ihre Passwörter freiwillig herauszugeben. Dazu bauen die Betrüger eigene Webseiten, die im Design echten Banken, Onlineshops oder sozialen Netzwerken sehr nahekommen.

Die Trickbetrüger verschicken Massenmails, in denen sie sich als Vertreter einer Bank oder eines Onlinediensts ausgeben. Über einen Link in der E-Mail sollen die Benutzer auf eine Webseite gehen und dort ihre Benutzerdaten, Kontoinformationen, Passwörter und TANs eingeben. Diese werden natürlich nicht an die wirklichen Banken oder Onlineshops, sondern an den Betrüger übermittelt, der sie zu seinen Zwecken benutzt.

Bei etwas genauerem Hinsehen sind die Phishing-Mails und die betreffenden Webseiten leicht zu entlarven:

- Phishing-Mails sind immer in relativ schlechtem Deutsch formuliert. Kein professionelles Unternehmen würde derartige Texte verfassen.
- Üblicherweise wird eine anonyme oder gar keine Anrede verwendet. Professionelle Anbieter sprechen ihre Kunden mit Namen an.
- Weder eine Bank noch PayPal oder eBay fordern ihre Kunden auf, Zugangsdaten preiszugeben.
- Drohende Formulierungen zum Ablaufen einer zeitlichen Frist oder einer Kontensperrung werden von professionellen Anbietern nicht verwendet.

Passwörter sicher auf dem Handy



Das Smartphone hat man immer dabei, deshalb nutzen viele es auch gerne als Notizzettel für Passwörter für die zahlreichen Onlinedienste, die man im Alltag nutzt. Dagegen ist prinzipiell auch nichts einzuwenden, solange man seine Passwörter nicht einfach unverschlüsselt in eine Notiz schreibt. Jeder, der das Smartphone in die Hand bekommt, kann dann die Passwörter lesen.

Verschiedene Apps ermöglichen das übersichtliche Speichern von Passwörtern auf dem Handy. Viele davon sind leider kostenpflichtig oder wenig vertrauenswürdig.

Password Safe ist eine kostenlose App, die Passwörter und weitere persönliche Zugangsdaten nach verschiedenen Kategorien verschlüsselt auf dem Handy speichert. Da die App selbst keine Internetberechtigung hat, können Daten nicht in falsche Hände geraten.

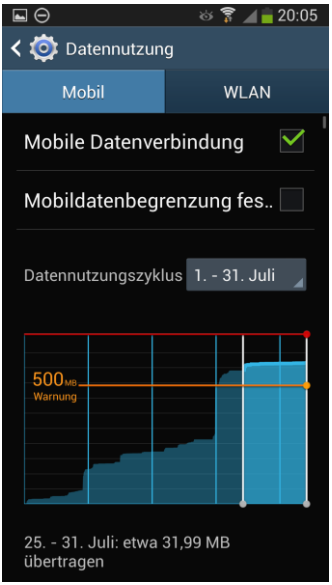
Passwort Safe verschlüsselt alle gespeicherten Daten über ein Master-Passwort nach dem AES-Verschlüsselungsstandard. Die Passwortdatenbank kann zur Datensicherung exportiert werden. Eine direkte Synchronisierung ist aufgrund fehlender Internetberechtigung nicht möglich.

Darauf sollten Sie bei der Auswahl einer Passwort-App achten

Apps zur Verwaltung von Passwörtern sind nur dann sicher, wenn sie einen bekannten Verschlüsselungsstandard wie AES nutzen. Bei herstellereigenen undokumentierten Verschlüsselungen können Gefahren lauern. Apps ohne Internetberechtigung können schon rein technisch bedingt die Passwörter nicht nach außen preisgeben. Achten Sie weiterhin auf die Möglichkeit, die verschlüsselte Passwortdatenbank für Notfälle sichern zu können.

Sicherheit vor Kosten

Sicherheit vor extremen Handyrechnungen

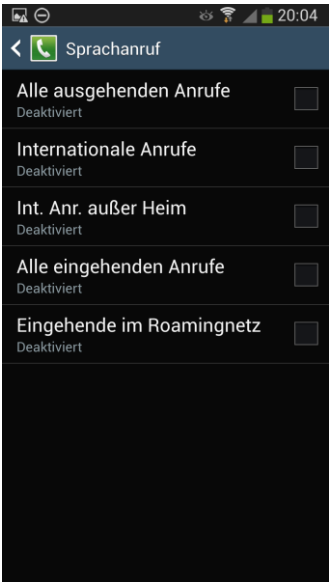


Internetnutzung wird heute in fast allen Mobilfunktarifen nach verbrauchtem Datenvolumen abgerechnet. Dazu ist es wichtig, dieses Datenvolumen zu kennen, um nicht von einer bösen Handyrechnung erschreckt zu werden.

1. Android bietet eine Anzeige der Datennutzung an, die in den Einstellungen auf der Seite *Verbindung* oder *Netzwerke* zu finden ist. Scrollen Sie nach unten, um die Apps mit dem höchsten Datenverbrauch zu sehen. Haben Sie einen Datentarif, der nach einem bestimmten Freivolumen gebremst wird, können Sie rechtzeitig abschätzen, wann diese Flatrate aufgebraucht ist.
2. Damit diese Anzeige optimal nutzbar ist, stellen Sie unter Datennutzungszyklus den Tag des Monats ein, an dem Ihr Mobilfunkanbieter das monatliche Datenvolumen der Flatrate zurücksetzt. Diesen Tag finden Sie üblicherweise auf Ihrer Mobilfunkrechnung.
3. Haben Sie einen Datentarif, der nach Verbrauch des Freivolumens auf eine volumenabhängige Abrechnung von meist 24 Cent/MByte umschaltet, schalten Sie *Mobildatenbegrenzung festlegen* ein. Damit wird die Mobilfunkdatennutzung nach Erreichen einer einstellbaren Volumengrenze abgeschaltet, um dem Benutzer die Möglichkeit zu geben, ein neues Datenpaket zu buchen oder – auf eigenes Risiko – die Begrenzung hochzusetzen und teuer weiterzusurfen. Derartige Tarife werden häufig bei sehr preisgünstigen Prepaid-Discountern eingesetzt.
4. Einige wenige Internettarife werden auch heute noch nach Zeit und nicht nach Datenvolumen abgerechnet. Da Android im Hintergrund permanent online ist, kann es hier zu sehr hohen Rechnungen kommen. Verzichten

Sie nach Möglichkeit auf solche Tarife. Wenn es nicht anders geht, schalten Sie in den Einstellungen unter *Drahtlos & Netzwerke/Mobile Netzwerke* die mobile Datenverbindung aus, immer wenn Sie sie nicht benötigen. Auf Samsung-Handys finden Sie dafür einen Schalter in der erweiterten Benachrichtigungsleiste.

Nicht nur Internet, auch Telefon kann teuer werden



Telefonieren vom Handy wird zwar immer billiger, aber auch hier lauern böse Kostenfallen in Form kostenpflichtiger Rufnummern und bei Auslandsgesprächen.

1. In den Einstellungen, die über das Menü der Telefon-App erreichbar sind, können Sie verschiedene Arten von Anrufen deaktivieren. Wählen Sie dazu in den Anrufeinstellungen nacheinander *Zusätzliche Einstellungen/Anrufsperre/Sprachanruf*.

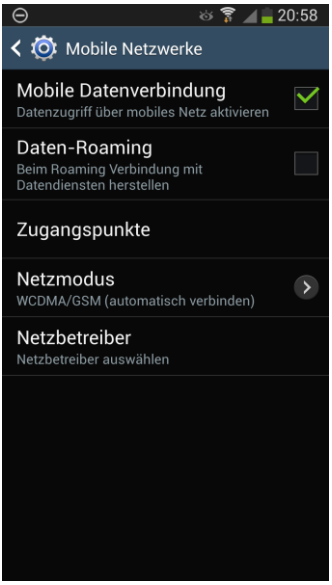
2. Wenn Sie nie ins Ausland telefonieren, deaktivieren Sie internationale Anrufe. Damit laufen Sie auch nicht Gefahr, sich durch versehentliches Tippen einer zweiten 0 am Anfang der Telefonnummer ins Ausland zu verwählen.

3. Da Anrufe an kostenpflichtige Rufnummern eine wichtige Einnahmequelle der Netzbetreiber sind, lassen sich diese eine Sperrung der sogenannten Premiumdienste bezahlen. Diese Sperrung ist deshalb auch nicht über die Einstellungen des Handys, sondern meist nur schriftlich beim jeweiligen Netzbetreiber möglich.

4. Videoanrufe über das Mobilfunknetz sind wesentlich teurer als über Apps wie Skype, die Voice over IP im Internet nutzen. Da kaum jemand die klassischen Videoanrufe überhaupt noch kennt, geschweige denn nutzt, schalten Sie diese in den Einstellungen am besten komplett aus.

Sicherheit vor Roamingkosten im Ausland

Telefonieren mit dem Handy aus dem Ausland nach Deutschland ist extrem teuer. Selbst eingehende Anrufe im Ausland müssen bezahlt werden. Noch teurer ist die Mobilfunkdatennutzung im Ausland. In Ländern außerhalb der EU kassieren viele Anbieter mehrere Euro pro MByte! Das gilt selbstverständlich auch für Hintergrundaktivitäten von Apps und Betriebssystem, auf die der Nutzer keinen Einfluss hat.



1. Schalten Sie in den Einstellungen unter *Drahtlos und Netzwerke/Mobile Netzwerke* das *Daten-Roaming* aus.
2. Schalten Sie im Roamingnetz eingehende Anrufe in den Einstellungen der Telefon-App aus. Sie sind dann im Ausland telefonisch nicht erreichbar, können aber trotzdem jederzeit selbst telefonieren.
3. Deutlich kostengünstiger als Roaming zu bezahlen ist die Nutzung einer Prepaid-Karte eines lokalen Netzbetreibers. In vielen Ländern kann man Prepaid-Karten in Supermärkten kaufen, ohne sich wie in Deutschland ausweisen zu müssen.
4. Für Internet nutzen Sie im Ausland am besten WLAN. In den meisten Ländern gibt es an öffentlichen Plätzen und in der Gastronomie offenes WLAN. Nur in Deutschland ist diese komfortable und schnelle Form mobilen Internetzugangs gesetzlich stark eingeschränkt.
5. Wer ganz sicher vor Roamingkosten sein will, schaltet sein Handy im Ausland in den Flugmodus oder nimmt einfach die SIM-Karte heraus. Bei den meisten Android-Handys lässt sich bei aktiviertem Flugmodus das WLAN nachträglich wieder einschalten. Mobilfunkverbindungen bleiben deaktiviert.

Die EU-Roamingrichtlinie

Die EU-Roamingrichtlinie begrenzt den Preis pro MByte bei 1 KByte Taktung ab Juli 2013 auf 70 Cent/MByte (83,3 Cent/MByte inkl. MwSt). Ab 50 Euro (59,50 Euro inkl. MwSt) müssen die Netzbetreiber innerhalb der EU die Verbindung trennen und den Nutzer per SMS informieren. Einige Anbieter legen im Kleingedruckten der Verträge aber fest, dass der Nutzer keine solche Information wünscht.

Die Länder des Europäischen Wirtschaftsraums EWR (engl.: EEA), die keine EU-Mitglieder sind: Island, Liechtenstein und Norwegen werden tariflich wie EU-Länder behandelt. Allerdings gilt hier die Höchstgrenze gemäß der EU-Roamingrichtlinie nicht.

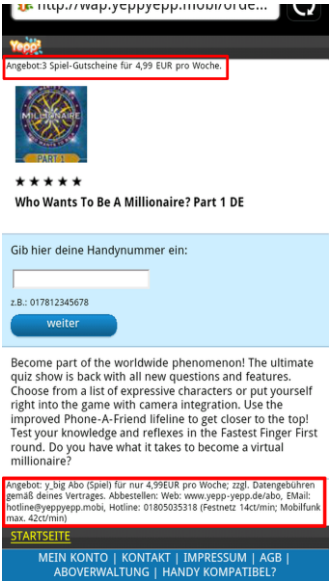
Die EU-Roamingrichtlinie enthält einen ursprünglich als Ausnahmeregelung geplanten Satz:

„In dem Fall, dass sich der Kunde für die in Absatz 3 Unterabsatz 1 genannte Funktion entscheidet, finden die Anforderungen nach Absatz 3 keine Anwendung, wenn der Betreiber eines besuchten Netzes in dem besuchten Land außerhalb der Union es nicht zulässt, dass der Roaminganbieter das Nutzerverhalten seines Kunden in Echtzeit überwacht. In einem solchen Fall wird dem Kunden bei seiner Einreise in ein solches Land mit einer SMS ohne unnötige Verzögerung und kostenlos mitgeteilt, dass die Informationen über den bisherigen Nutzungsumfang und die Garantiefunktion, wonach ein angegebener Höchstbetrag nicht überschritten wird, nicht zur Verfügung stehen."

o2 macht aus dieser Ausnahme eine Regel und schickt allen Kunden, die in einem Land der Zonen 3 oder 4 (außerhalb EU bzw. EWR) ihr Handy einschalten, eine SMS, dass der Datenverbrauch ohne Höchstgrenze abgerechnet wird. Angeblich stellen die ausländischen Roamingpartner die Daten nicht in Echtzeit zur Verfügung. Bei Telekom und Vodafone funktioniert die von der EU vorgeschriebene Kostenbegrenzung in allen Ländern der Welt.

Vorsicht vor Abzock-Apps

Viele auf den ersten Blick kostenlose Apps haben einen finanziellen Hintergrund für den Entwickler. Innerhalb der Apps lassen sich mehr oder weniger wichtige Funktionen nur kostenpflichtig freischalten.



Das Verfahren an sich ist legal und von Google im Play Store sogar erwünscht, da Google bei jedem In-App-Kauf mitverdient und kostenlose Apps deutlich häufiger heruntergeladen werden als kostenpflichtige.

Einige unseriöse Apps nutzen solche In-App-Käufe allerdings für Abos, die über die Telefonrechnung am Google Play Store vorbei abgerechnet werden. Damit sind auch Käuferschutz und Stornierungsmöglichkeit von Käufen über Google Play hinfällig. Kunden haben oft nur sehr mühsam die Möglichkeit, solche Abos zu kündigen. Vielen fallen sie auf der Handyrechnung nicht einmal auf.

1. Geben Sie in kostenlosen Apps, vor allem in Spielen, nie Ihre Handynummer ein.
2. Achten Sie bei allen Käufen außerhalb seriöser App-Shops genau darauf, ob es sich beim Kauf um ein Abo handelt. Die Hinweise sind oft sehr versteckt. In der Abbildung wurden sie nachträglich gekennzeichnet.
3. Laden Sie Apps nie über Werbebanner herunter, sondern immer nur über seriöse App-Shops. Hinter Werbebannern verbergen sich sehr häufig unseriöse Anbieter.
4. Kaufen Sie nichts per Premium-SMS. Hier haben Sie keinerlei Möglichkeit, über einen Zahlungsanbieter Ihr Geld zurückzubekommen, wenn Sie in eine Abofalle getappt sein sollten.

Komfortable Technik, aber sicher

Das Smartphone als sicherer WLAN-Hotspot

Moderne Smartphones liefern zumindest in Großstädten mit guter HSDPA-Versorgung Datenübertragungsraten, die mit DSL über Telefonkabel durchaus mithalten können. Da bietet es sich an, unterwegs das Handy als mobilen Internetzugang für das Notebook zu nutzen. Allgemein wird dieses Verfahren als Tethering bezeichnet, abgeleitet von dem englischen Wort für „anbinden“. Android-Smartphones können als mobile WLAN-Hotspots konfiguriert werden. Sie können sich dann je nach Smartphone mit maximal drei bis zehn Geräten per WLAN am Smartphone anmelden und dessen Mobilfunkverbindung als Internetzugang nutzen. Allerdings können nur Mobilfunkverbindungen auf diese Weise freigegeben werden. Ist das Smartphone selbst per WLAN im Internet, kann es nicht gleichzeitig als WLAN-Hotspot laufen.

1. Wählen Sie in den Einstellungen unter *Drahtlos und Netzwerke* die Option *Weitere Einstellungen* und dann *Tethering und mobiler Hotspot*.

2. Schalten Sie hier den Schalter *Mobiler WLAN-Hotspot* ein. Ein blaues Symbol in der Statusleiste zeigt den aktiven WLAN-Hotspot an. Er wird sofort auf den anderen Geräten als verfügbar angezeigt. Bedenken Sie jedoch, dass die Reichweite bei Weitem nicht so groß ist wie die eines klassischen WLAN-Routers. Außerdem verbraucht die Nutzung als WLAN-Hotspot sehr viel Strom aus dem Handyakku. Schließen Sie am besten das Handy die ganze Zeit ans Ladegerät an und beenden Sie den WLAN-Hotspot, sobald Sie ihn nicht mehr benötigen.

3. Tippen Sie auf die Zeile *Mobiler WLAN-Hotspot*, kommen Sie in einen Konfigurationsdialog, der den Namen des Hotspots *AndroidAP* sowie einen zufällig generierten Schlüssel anzeigt, der auf den Geräten eingegeben werden muss. Als Verschlüsselungsverfahren wird standardmäßig WPA 2 PSK verwendet.

4. Der Konfigurationsbildschirm zeigt an, wenn sich ein anderes Gerät per WLAN mit dem mobilen Hotspot verbindet.

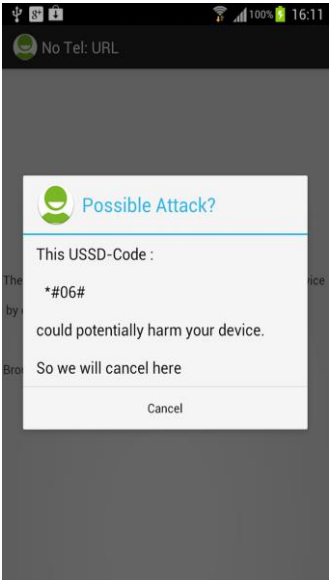
5. Über die Schaltfläche *Konfigurieren* ändern Sie den Namen des mobilen Hotspots, das Verschlüsselungsverfahren, das Passwort und auch den WLAN-Kanal, falls es Probleme mit der Standardeinstellung geben sollte.

6. Möchten Sie Geräte verbinden, die die angebotenen Verschlüsselungsverfahren nicht unterstützen, können Sie auch einen offenen WLAN-Hotspot einrichten. In solchen Fällen sollten Sie aus Sicherheitsgründen den Zugang zum Hotspot auf bestimmte eigene Geräte beschränken. Tippen Sie dazu oben auf die Zeile *Allen Geräten Verbindung erlauben* und schalten Sie auf *Nur zugelassene Geräte* um. Tragen Sie jetzt über die Schaltfläche *Zugelassene Geräte* unten links die MAC-Adressen der Geräte ein, die den mobilen Hotspot nutzen dürfen.

Tethering und Datenflatrates

Bei den meisten günstigen Flatratetarifen für Smartphones wird nach wenigen hundert MByte – zum Handysurfen in einem Monat absolut ausreichend – auf unattraktive GPRS-Geschwindigkeit abgebremst. Per Tethering mit dem Notebook kann man dieses Datenvolumen schon nach wenigen Stunden erreichen. Für den Rest des Monats hat man keinen Spaß mehr an der Flatrate. Die teureren Datenflatrates für Surfsticks beinhalten deutlich mehr Übertragungsvolumen. Natürlich spricht nichts dagegen, eine solche SIM-Karte in ein Smartphone zu stecken und dieses für das Tethering zu nutzen. Allerdings haben die typischen Notebook-Surftarife meist höchst unattraktive Preise beim Telefonieren.

Die USSD-Sicherheitslücke beim Telefonieren



Mit speziell präparierten Webseiten ist es theoretisch möglich, einen USSD-Steuerungscode in das Handy einzuschleusen und dort auch unbemerkt auszuführen, der die Daten des Handys löscht oder die SIM-Karte im Mobilfunknetz sperrt. Das gleiche funktioniert auch über QR-Codes, die direkt auf einen solchen Code verweisen. Diese Sicherheitslücke betrifft nur Telefone bestimmter Hersteller, unter anderem Samsung und HTC. Einige andere Geräte lassen sich per USSD-Code zwar nicht komplett zurücksetzen, können aber andere unerwünschte Funktionen ausführen.

NeTelURL ist eine kleine App, die USSD-Codes abfängt, anstatt aus dem Browser heraus direkt die Telefon-App zu starten.

Die App braucht nicht gestartet zu werden, sondern öffnet automatisch ein Pop-up-Fenster, wenn aus dem Browser heraus ein Telefonlink im Format *tel:.* geöffnet wird. Wird eine Telefonnummer abgefangen, besteht die Möglichkeit, diese Nummer nach Kontrolle direkt aus der App zu wählen.

Aktuelle Android-Versionen sind nicht betroffen

Dieses Problem bestand nur bis zur Android-Version 4.0.x und wurde von den meisten Geräteherstellern durch kleine Patches behoben. Die aktuellen Android-Versionen 4.2.x sowie das ganz neue Android 4.3 sind nicht betroffen.

Offene Ports finden

Wer sein Haus vor Einbrechern schützen will, schließt nicht nur die Eingangstür, sondern auch alle Fenster, Kellertüren und Nebeneingänge. Im Vergleich zu einem Computer entspricht dessen IP-Adresse der Hausanschrift, verschiedene Ports stellen die unterschiedlichen Eingänge zum Haus dar. Im TCP/IP-Protokoll sind mehrere Tausend solcher Ports definiert, die für unterschiedliche Übertragungsprotokolle genutzt werden. PCs, die Serverdienste zur Verfügung stellen, müssen diverse Ports geöffnet halten, die dann allerdings von Angreifern genutzt werden können. Im Gegensatz dazu braucht ein Smartphone keine geöffneten Ports, da hier üblicherweise keine Dienste laufen, die von außen erreichbar sein müssen.

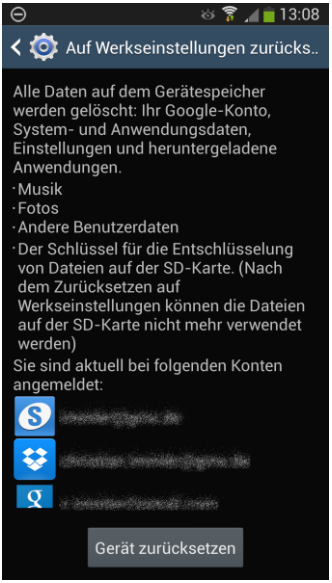
Der Landesbeauftragte für den Datenschutz des Landes Niedersachsen bietet in Zusammenarbeit mit Heise Security auf der Webseite www.heise.de/security/dienste/portscan einen unabhängigen Test an, mit dem Sie die Sicherheitseinstellungen Ihres PCs oder Smartphones jederzeit selbst überprüfen können. Dieser Test gilt als einer der besten derartigen Tests und wird von zahlreichen Datenschutzbehörden und anderen öffentlichen Einrichtungen regelmäßig eingesetzt. Auf einem Smartphone sollten alle Ports grün angezeigt werden.

Portscan bei WLAN-Verbindung

Führen Sie den Portscan über eine WLAN-Verbindung durch, werden die Ports auf Ihrer IP-Adresse im DSL-Netzwerk gescannt. Sollte auf einem Ihrer PCs oder auf dem Router ein Webserver laufen, wird der entsprechende Port rot angezeigt, was aber für das Smartphone kein Sicherheitsrisiko darstellt.

Smartphone vor Verkauf komplett zurücksetzen

Genauso, wie Sie auf einem PC die Festplatte formatieren, bevor Sie ihn verkaufen oder verschenken, sollten Sie auch auf einem Smartphone alle persönlichen Daten beseitigen. Am einfachsten setzen Sie es dazu auf die Werkseinstellungen zurück. Dabei werden alle persönlichen Daten und installierten Apps im Gerätespeicher gelöscht.



1. Wählen Sie in den Einstellungen unter *Konten* bzw. *Nutzer* die Option *Sichern und Zurücksetzen* und dann *Auf Werkseinstellungen zurücksetzen*.
2. Jetzt sehen Sie noch einmal eine Übersicht aller Konten, an denen Sie mit dem Smartphone angemeldet sind. Die Verbindungen zu diesen Konten werden gelöscht, die Konten selbst sowie die dort gespeicherten Daten bleiben in der Cloud erhalten.
3. Sollten Sie eine verschlüsselte Speicherkarte verwenden, wird der Schlüssel dazu ebenfalls gelöscht. Die Speicherkarte ist ohne diesen Schlüssel nicht mehr nutzbar.
4. Tippen Sie ganz unten auf *Gerät zurücksetzen*, um das Smartphone wirklich auf die Werkseinstellungen zurückzusetzen.

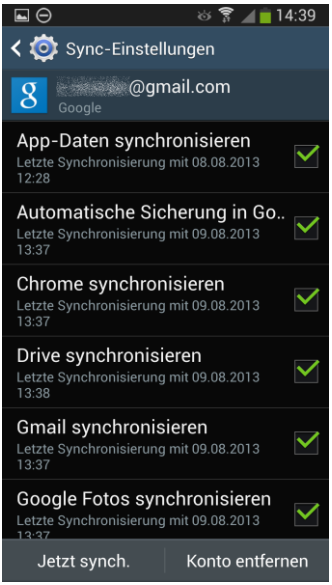
Speicherkarte formatieren

Beim Zurücksetzen auf die Werkseinstellungen bleiben die Daten auf der Speicherkarte erhalten. Wenn Sie die Speicherkarte des Handys mit verkaufen, kopieren Sie sich vorher Ihre Daten mit einem Kartenleser auf dem PC und formatieren die Speicherkarte dort neu. Auch Android bietet eine Formatierungsfunktion für Speicherkarten. Scrollen Sie in den Einstellungen unter *Speicher* ganz nach unten und tippen Sie auf *SD-Karte formatieren*.

Sicherheit vor Datenverlust

Datensicherung im Google-Konto

Mit einem Google-Konto können persönliche Daten wie Adressbuch oder Terminkalender beim Wechsel auf ein neues Smartphone leicht von einem Gerät auf ein anderes übernommen werden. Die Zeiten, als man Telefonnummern auf jedem neuen Handy wieder neu eintragen oder mühsam per SIM-Karte übertragen musste, sind lange vorbei.

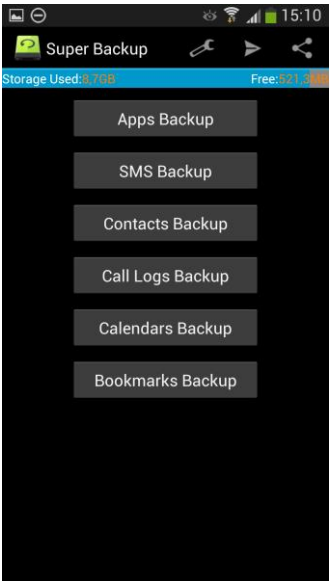


Viele Funktionen eines Android-Smartphones können theoretisch auch ohne Google-Konto genutzt werden. Zur Verwendung von Google Mail und Google Play ist ein Google-Konto zwingend erforderlich. Weiterhin lassen sich Einstellungen und Apps sowie Verlauf und Lesezeichen des Chrome-Browsers im Google-Konto sichern.

1. **Bei der Ersteinrichtung** eines Android-Smartphones wird man gefragt, ob ein vorhandenes Google-Konto auf dem Gerät genutzt oder ein neues angelegt werden soll.
2. Die Frage *Dieses Telefon über mein Google-Konto sichern* sollten Sie mit ***Ja*** beantworten. So werden Ihre Apps und Einstellungen im Google-Konto gesichert und lassen sich im Notfall oder bei einem Hard-Reset leicht wiederherstellen.
3. Tippen Sie in den Einstellungen unter *Konten* auf *Google* und wählen auf dem nächsten Bildschirm das Google-Konto, können Sie detailliert festlegen, welche Daten des Smartphones mit dem Google-Konto synchronisiert werden sollen. Bei jeder Datenkategorie steht das Datum der letzten Synchronisation dabei. Einige Daten werden nur synchronisiert, wenn sich etwas geändert hat.

Datensicherung mit Apps

Android speichert zwar Daten im Google-Konto, aber leider nicht alle. SMS, Anrufprotokolle und installierte Apps werden leider nicht gesichert. Wer seine Kontaktdaten aus einer älteren PC-Software wie z. B. Outlook übernommen hat, hat diese lokal auf dem Smartphone und nicht im Google-Konto gespeichert. Alle solche Daten können nur mit externen Apps gesichert werden.



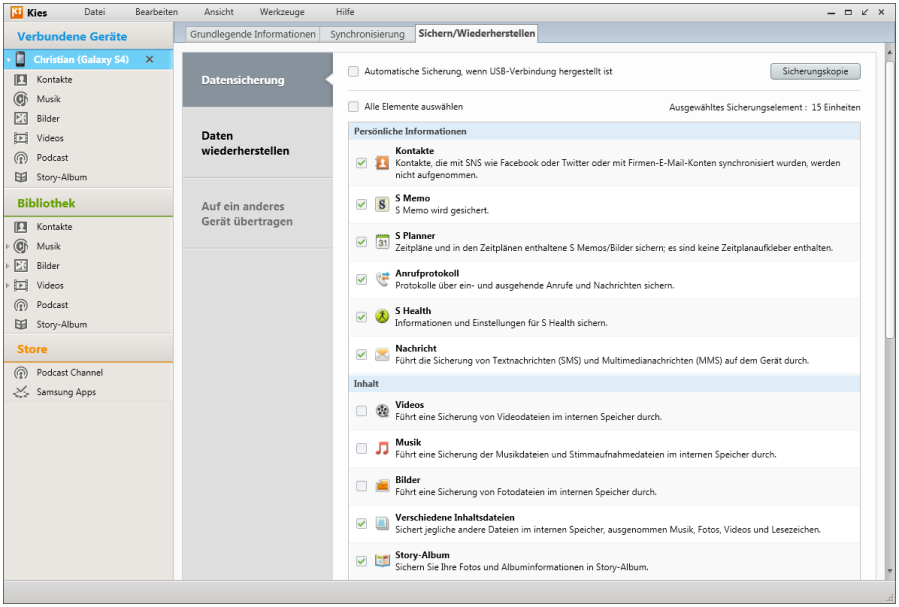
Die meisten kostenlosen Backup-Apps sind eingeschränkt und bieten die volle Funktionalität erst nach Kauf der Vollversion.

Mit **Super Backup** werden kostenlos alle wichtigen Daten auf die Speicherkarte gesichert.

1. Da die meisten Android-Smartphones ein internes Speicherlaufwerk besitzen, das sich aber zur Datensicherung nicht eignet, da es im Fall eines Totalausfalls oder Hard Resets mit ausfällt, tippen Sie als Erstes auf das Schraubenschlüsselsymbol und wählen unter *Backup Path* die Speicherkarte als Sicherungsziel..
2. In den *Schedule Settings* legen Sie die Intervalle zur automatischen Sicherung von SMS, Kontakten und Anrufprotokollen fest. Hier können Sie die gesicherten Daten automatisch als GMail sichern, um sie bei einem Verlust des Handys wiederherstellen zu können.
3. Apps können bei der Installation automatisch gesichert werden.
4. Zusätzlich zur automatischen Sicherung haben Sie im Hauptmenü jederzeit die Möglichkeit, ausgewählte Apps, SMS, Kontakte, Anrufprotokolle, Kalendereinträge und Lesezeichen manuell zu sichern.

Datensicherung auf dem PC

Was dem Android-Betriebssystem fehlt, ist eine Möglichkeit zur kompletten Datensicherung auf dem PC. Hier ist man auf zusätzliche Software der Gerätehersteller angewiesen. Die großen Hersteller wie Samsung, HTC oder Huawei liefern solche Windows-Programme mit. Am Beispiel von Samsung Kies zeigen wir, wie eine Datensicherung auf dem PC funktioniert.



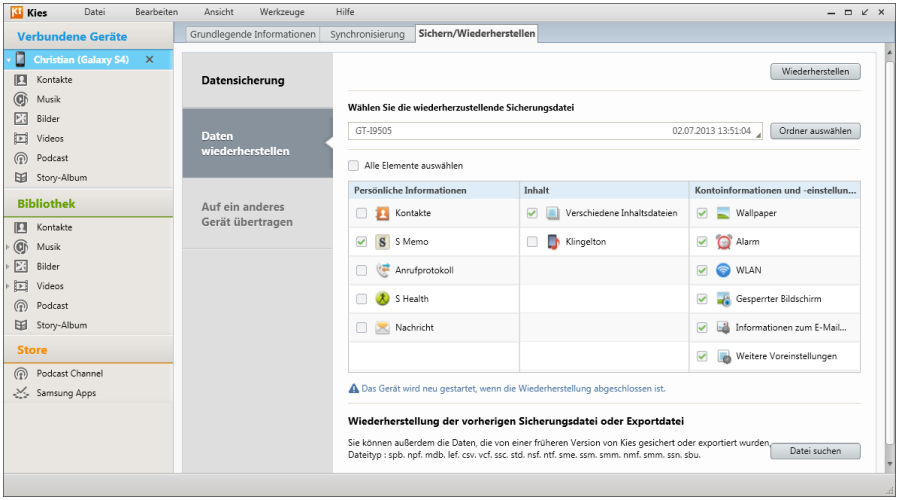
Die Kies-Software ermöglicht, persönliche Informationen, Kontakte, Termine, Notizen, Anrufprotokolle und SMS sowie auch sämtliche Einstellungen zu Klingeltönen, Startbildschirm und E-Mail-Konten auf dem PC zu sichern.

1. Markieren Sie in der Kies-Software auf der Registerkarte *Sichern/Wiederherstellen* alle Datentypen, die gesichert werden sollen. Wählen Sie nicht einfach *Alle Elemente auswählen*, da in diesem Fall auch alle Fotos, Musik und Videos aus dem internen Speicherlaufwerk gesichert würden. Hier kommen schnell ein paar GByte und einiges an Sicherungszeit zusammen. Diese Daten haben Sie aber bestimmt schon anderweitig auf dem PC.

2. Unter *Anwendungen* können Sie wählen, ob Daten installierter Apps ebenfalls gesichert werden sollen. Auch hier kommen schnell mehrere Hundert MByte zusammen. Wählen Sie sorgfältig aus, welche App-Daten Sie wirklich brauchen und welche sich bei einer Neuinstallation zum Beispiel aus einem Onlinebenutzerkonto wiederherstellen lassen.

3. Ein Klick auf *Sicherungskopie* rechts oben sichert die ausgewählten Daten in einem Verzeichnis im eigenen Windows-Benutzerprofil. Der Verzeichnisname wird in der Kies-Software angezeigt, wenn man ganz nach unten scrollt.

4. Zur Wiederherstellung im Notfall wählen Sie im Bereich *Daten wiederherstellen* die gewünschte Sicherungsdatei aus und kreuzen die Datentypen an, die aus dieser Sicherung wiederhergestellt werden sollen.

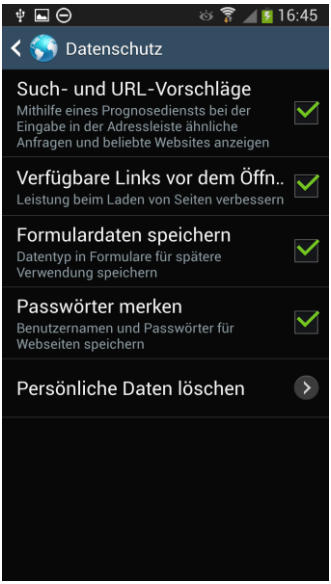


Nicht alle Daten werden gesichert

Selbst bei Auswahl aller Optionen werden nicht alle Daten des Smartphones gesichert. Kontakte, die aus einem Facebook-, Twitter- oder Exchange-Konto auf dem Smartphone angezeigt werden, werden nicht gesichert, da sie schreibgeschützt sind und somit auch nicht wiederhergestellt werden könnten. Daten von der externen Speicherkarte werden ebenfalls nicht gesichert. Diese können aber einfach auf den PC kopiert werden. Die Speicherkarte wird als Laufwerk im Windows-Explorer angezeigt.

Datenschutz und Vertraulichkeit beim Surfen

Schutz vor Browserspionage

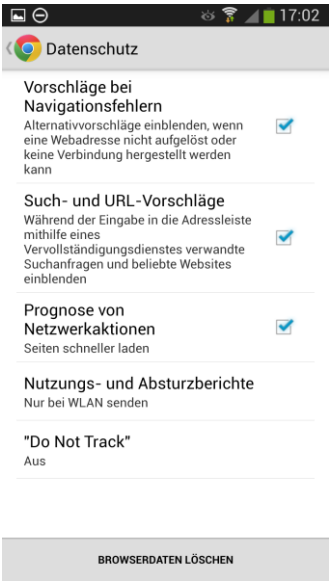


Ähnlich wie bei Desktopbrowsern bietet auch der Android-Browser diverse Sicherheitseinstellungen, die zwischen Surfkomfort und persönlichem Sicherheitsbedürfnis optimiert werden können. Besonders beim Besuch zweifelhafter Webseiten sollten Sie diese Einstellungen beachten, die Sie im Menü des Browsers unter *Einstellungen/Datenschutz* sowie auf einigen Geräten auch unter *Einstellungen/Inhaltseinstellungen* finden.

1. Lassen Sie die Sicherheitswarnungen immer eingeschaltet. Der Browser warnt vor gefährlichen Webseiten. Wurde eine Seite z. B. wegen gefährlicher Skripte von Google als bedenklich eingestuft, warnt der Browser, diese Seite nicht zu besuchen, und zeigt sie nicht automatisch an.
2. Cookies sind kleine Dateien, in denen der Browser Benutzerdaten lokal speichert. Viele Webshops benutzen Cookies, um einen Benutzer, der einmal angemeldet war, beim nächsten Besuch wiederzuerkennen. Wer Bedenken in Bezug auf den Datenschutz hat, kann Cookies im Browser deaktivieren. Einige Webseiten werden dann aber nicht mehr problemlos funktionieren, oder es gehen bestimmte Komfortfunktionen verloren.
3. Wem die Eingabe von Benutzernamen und Passwörtern auf Dauer zu lästig ist, kann dem Browser erlauben, diese Daten zu speichern und automatisch einzugeben. Natürlich hat dann jeder, der Zugriff auf das Smartphone hat, auch Zugriff auf die persönlichen Anmeldedaten auf den zuvor besuchten Webseiten. Wird das Smartphone von mehreren Personen genutzt, schalten Sie das Speichern von Passwörtern ab.

Spionageschutz auch in Google Chrome

Der schnelle und komfortable Browser Google Chrome ist auf immer mehr Android-Smartphones bereits vorinstalliert. Auch hier finden Sie in den Einstellungen diverse Möglichkeiten, den Datenschutz auf Kosten des Surfkomforts zu erhöhen.



1. Die automatischen Suchvorschläge sowie die Vorschläge bei falsch eingetippten Internetadressen sind sehr praktisch, geben Google allerdings Hinweise auf persönliche Interessen. Wer das nicht möchte, kann in den Einstellungen von Chrome unter *Datenschutz* auf diese Vorschläge verzichten.

2. Der Schalter *Prognose von Netzwerkaktionen* lädt Seiten schneller, indem das typische Nutzungsverhalten vieler Benutzer ausgewertet wird. Wer mit seinem Verhalten nicht dazu beitragen möchte, kann auf diese Funktion verzichten, was allerdings zu langsamerem Seitenaufbau und mehr Datenverbrauch führt, da uninteressante Teile der Webseiten früher als nötig geladen werden.

3. Google Chrome sendet standardmäßig nur über WLAN Nutzungs- und Absturzberichte an Google. Wer hier Datenschutzbedenken hat, kann auch diese abschalten.

4. Wie im Android-Standardbrowser lassen sich auf der Startseite der Chrome-Einstellungen das Speichern von Passwörtern sowie das automatische Ausfüllen von Formularen abschalten.

5. Bei Bedenken können Sie unter *Inhaltseinstellungen* das Speichern und Lesen von Cookies ausschalten. Auf der gleichen Seite blockieren Sie auch Pop-ups, die auf fast allen Webseiten nur für Werbung verwendet werden.

Verhindern, dass andere wissen, wo man sich aufhält

Jedes Smartphone ist auf der Welt eindeutig lokalisierbar. Dies hat deutliche Vorteile. So kann z. B. eine Google-Suche vorrangig Suchergebnisse in der eigenen Umgebung finden – sehr hilfreich, wenn man Restaurants, Läden oder Geldautomaten sucht. Manche Benutzer möchten zumindest das Gefühl haben, sich vor Google verstecken zu können und verzichten dabei auf die lokalen Suchergebnisse. Ohne Standortzugriff können Sie das Handy bei Diebstahl oder Verlust auch nicht orten.

1. Versucht eine Webseite, den eigenen Standort abzufragen, zeigt der Browser eine entsprechende Meldung an. Hier können Sie den Standortzugriff zulassen oder ablehnen. Die Antwort wird für zukünftige Zugriffe gespeichert.

2. Die Daten, die Webseiten auf diese Weise gespeichert haben, sehen Sie im Standardbrowser und in Chrome unter *Einstellungen/Inhaltseinstellungen/Website-Einstellungen* und können sie dort einzeln löschen.

3. Möchten Sie auf lokale Suchergebnisse ganz verzichten und Ihren Standort ansatzweise geheim halten, schalten Sie in den Einstellungen des Browsers unter *Inhaltseinstellungen* den Standortzugriff ab.

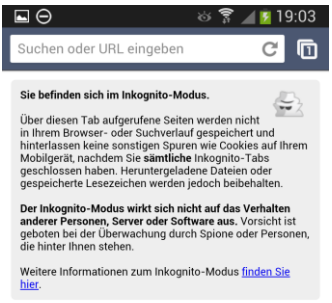
4. Apps von Drittentwicklern, die über Systemfunktionen auf den Standort zugreifen, sind von der Einstellung nicht betroffen. Um diesen Apps den Zugriff zu verwehren, schalten Sie in den Einstellungen über *Optionen/Standortdienste* den Standortzugriff aus. Hier legen Sie auch fest, ob GPS und/oder WLAN zur Standortbestimmung verwendet werden darf.

GPS ausschalten

Wer seinen Standort verbergen möchte, schaltet am besten das GPS über die erweiterte Benachrichtigungsleiste aus und spart damit noch Strom.

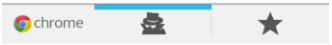
Besuchte Webseiten vor neugierigen Blicken verstecken

Die Verlaufsliste im Browser und bei der Suche wie auch gespeicherte Cookies können anderen Nutzern des gleichen Gerätes Hinweise auf zuletzt besuchte Webseiten geben.



Der Android-Standardbrowser wie auch Google Chrome bieten einen anonymen Modus, der keinerlei Spuren besuchter Webseiten auf dem Gerät hinterlässt. Allerdings können Sie auch selbst die in diesem Modus besuchten Webseiten in der Verlaufsliste nicht wiederfinden, wenn Sie keine Lesezeichen gespeichert haben.

1. Im Standardbrowser öffnen Sie einen neuen anonymen Tab über den Menüpunkt *Anonymer Modus*. Diese Tabs werden mit einer hellgrauen Titelleiste zur Unterscheidung angezeigt.



2. In Google Chrome wählen Sie im Menü *Neuer Inkognito-Tab*. Diese Tabs erscheinen mit dunkler Titelleiste und werden auch nicht mit anderen Geräten, die Chrome nutzen, synchronisiert.

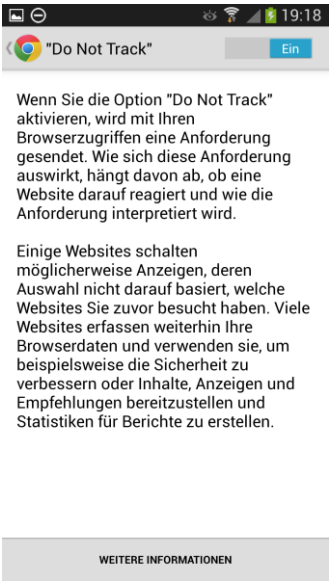
Der anonyme Modus verbirgt die Daten nur gegenüber Nutzern des gleichen Geräts. Webserver können die Benutzerdaten gleichermaßen wie in normalen Browsertabs auswerten.

Daten löschen

Erst nach dem Schließen aller Inkognito-Tabs werden alle Daten zum Browser- und Suchverlauf aus diesen Tabs sowie auch die Cookies gelöscht. Heruntergeladene Dateien und Lesezeichen bleiben erhalten.

Verfolgungsschutz Do not track

Möchten Sie nicht nur selbst auf dem PC keine Spuren hinterlassen, sondern auch für die Anbieter unerkannt bleiben, können Sie mit dem Tracking-Schutz im Chrome-Browser Inhalte bestimmter Drittanbieter blockieren. Der Standardbrowser bietet diese Möglichkeit nicht.



Viele Webseiten beziehen heute Informationen aus mehreren Quellen, nicht nur vom eigentlichen Seitenbetreiber, sondern auch von Dritten. Vielfach handelt es sich dabei um Werbung oder um Statistikmodule, die das Surfverhalten der Besucher beobachten.

Der Tracking-Schutz weist den jeweiligen Webserver an, Skripte von Drittanbietern auf Webseiten, die das eigene Surfverhalten ausspionieren, zu blockieren. Dabei werden nur „heimliche“ Aufrufe blockiert. Klicken Sie eine der betreffenden Webseiten direkt an, können Sie sie ganz normal besuchen. Tracking-Schutz ist also kein Webfilter. Die Technik basiert auf der Kooperation der Werbeanbieter, deren Skripte die vom Browser zurückgemeldeten Benutzerwünsche respektieren müssen. Wenn ein Webserver die DNT-Einstellung des Browsers ignoriert, ist der Tracking-Schutz wirkungslos.

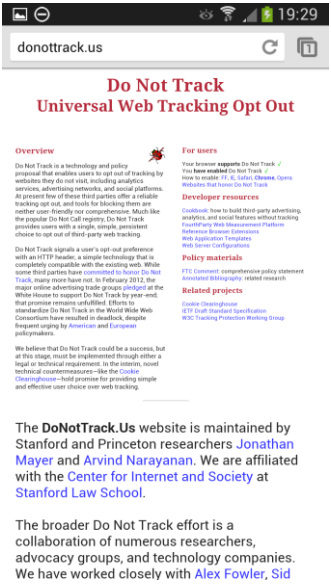
Der Tracking-Schutz wird in den Einstellungen des Chrome-Browsers unter *Datenschutz/Do Not Track* eingeschaltet.

Tracking-Schutz überprüfen

Verständlicherweise wollen Sie, wenn Sie den Tracking-Schutz aktiviert haben, auch wissen, ob dieser auch wirklich funktioniert. Die Webseite http://www.donottrack.us bietet einen einfachen Onlinetest an, der prüft, ob ein Browser DNT überhaupt unterstützt und ob diese Funktion eingeschaltet ist. Hier finden Sie auch Hinweise, wie der Tracking-Schutz in unterstützten Browsern aktiviert werden kann.

DNT – ein Politikum im Internet

Das Verfolgen von Benutzeraktivitäten, um personalisierte Inhalte anzuzeigen, ist an sich eine nützliche Technologie, die nur von den Medien immer häufiger in schlechtes Licht gerückt wird, da sie von Werbetreibenden gern missbraucht wird.



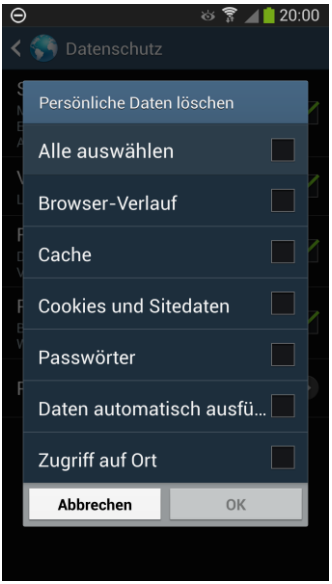
Als Microsoft mit der Release Preview von Windows 8 den Tracking-Schutz standardmäßig aktivierte, nahm die beim W3C (World Wide Web Consortium) für dieses Thema zuständige Arbeitsgruppe öffentlich Stellung: Ein Nutzer soll selbst entscheiden, ob er Tracking wünscht oder nicht. Ein Browser dürfe standardmäßig keinen Do-Not-Track-Header (DNT) übertragen. Wenn Browser standardmäßig einen DNT-Header senden, werden Werbeanbieter ganz schnell dazu übergehen, dies nicht mehr zu beachten. Webseiten mit offensichtlich illegalen Spionageinteressen werden den Tracking-Schutz ohnehin ignorieren.

Die Digital Advertising Alliance (DAA), die Interessenvertretung der Werbetreibenden, will DNT generell nur akzeptieren, wenn es nicht voreingestellt ist. Andernfalls könnten sich Anbieter von Werbung entscheiden, die DNT-Header einfach zu ignorieren.

Nach Aussage des W3C steht es Microsoft natürlich frei, den Internet Explorer auch weiterhin einen DNT-Header senden zu lassen. Das entspräche aber nicht dem W3C-Standard. Sollte Microsoft dennoch behaupten, W3C-konform zu arbeiten, sei das dann ein Fall für die Aufsichtsbehörden. Google lässt in Chrome den DNT-Header standardmäßig ausgeschaltet, bis der Benutzer ihn einschaltet.

Surfspuren beseitigen

Manchmal kommt der Zeitpunkt, wo man die Spuren seines Surfens auf dem Smartphone beseitigen möchte, wenn man es z. B. zeitweilig in fremde Hände gibt. Der Android-Standardbrowser und auch Google Chrome bieten komfortable Funktionen, die eigenen Surfspuren zu beseitigen.



1. Im Standardbrowser wählen Sie im Menü *Einstellungen/Datenschutz/Persönliche Daten löschen*. Hier können Sie die zu löschenden Daten auswählen.
2. Im Chrome-Browser wählen Sie im Menü *Einstellungen/Datenschutz* und tippen dann ganz unten auf *Browserdaten löschen*. Auch hier besteht die Auswahl der zu löschenden Daten.

Um zu verhindern, dass andere Benutzer des Smartphones sehen, welche Webseiten Sie besuchten, löschen Sie den *Browser-Verlauf*. Die Listen *Meist besucht* sowie *Verlauf* sind dann leer. Lesezeichen bleiben bestehen.

Regelmäßiges Löschen des Caches bringt deutliche Performancegewinne. Allerdings muss danach jede Webseite und vor allem jede Grafik, auch Logos, die sich nie ändern, und Ähnliches wieder komplett neu heruntergeladen werden. Der Browsercache kann Hinweise auf besuchte Webseiten und heruntergeladene Dateien geben, was manche Nutzer als Sicherheitsrisiko sehen.

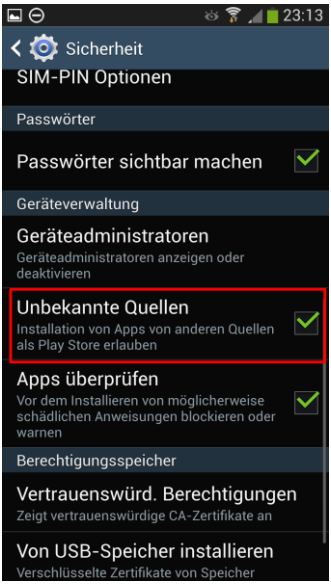
Löscht man Cookies und Sitedaten, verhält sich der Browser gegenüber einer Webseite so, wie wenn diese noch nie besucht worden wäre.

Nach dem Löschen von *Passwörtern* und *Daten automatisch ausfüllen* müssen alle Anmeldedaten auf Webseiten neu eingegeben werden.

Zugriff auf Ort enthält Beschränkungen für bestimmte Webseiten, was den Standortzugriff betrifft. Nach dem Löschen dieser Daten fragt jede Webseite erneut, ob sie auf Standortdaten zugreifen darf.

So findet man gefährliche Apps

App-Download aus vertrauenswürdigen Quellen



Der Google Play Store ist die bekannteste Quelle zum Download von Apps, es gibt aber auch noch andere, die teilweise Apps anbieten, die bei Google Play nicht lieferbar sind. Einige Entwickler, besonders aus der Open-Source-Szene, bieten ihre Apps zusätzlich auch über ihre eigenen Webseiten oder unabhängige Downloadportale an.

Apps werden außerhalb des Google Play Store meist als APK-Dateien zum Download angeboten. Diese können direkt über den Browser oder auch aus einem Dateianhang einer E-Mail auf dem Smartphone installiert werden.

Je nach Einstellung des Smartphones können bei der ersten Installation einer APK-Datei und auch schon beim Download Hinweise erscheinen, dass Installationen aus unbekannten Quellen nicht zulässig sind. Direkt aus dieser Meldung heraus besteht Zugriff auf die zugehörige Systemeinstellung, mit der man die Installation aus anderen Quellen als dem Play Store zulassen kann. Schalten Sie den Schalter *Unbekannte Quellen* ein, um die Installation von Apps aus APK-Dateien oder anderen App-Shops zuzulassen.

Samsung bietet einen eigenen App-Shop an, der auf den Samsung-Galaxy-Smartphones über eine eigene App vorinstalliert ist. Samsung stellt in der Kategorie *Apps für Galaxy* spezielle Apps aus Eigenentwicklung oder von Partnern vor, die eigens für Samsung-Galaxy-Smartphones angepasst wurden und in dieser Form nicht über den Google Play Store zu haben sind.

Amazon bietet einen eigenen App-Shop für Android-Apps an, der mit einer kostenlosen App jeden Tag beworben wird. Der Download der kostenlosen Apps funktioniert wie ein Kauf, man bekommt dabei auch eine Kaufbestätigung von Amazon per E-Mail. Dieser App-Shop läuft über eine eigene App, die zunächst auf dem Smartphone installiert werden muss.

F-Droid ist ein besonderer App-Shop, in dem es nichts zu kaufen gibt. Hier gibt es ausschließlich Open-Source-Software, darunter einige interessante Systemtools, die es nicht in den Google Play Store geschafft haben. Im Gegensatz zu anderen App-Shops bietet F-Droid bei vielen Apps verschiedene Versionen an. So kann man auch ältere Versionen testen. In den Einstellungen lässt sich festlegen, ob Apps, die unerwünschte Eigenschaften haben, wie z. B. Werbung oder Benutzerverfolgung, in den Listen angezeigt werden dürfen oder nicht. Standardmäßig werden alle derartigen Apps ausgeblendet, dazu gehören auch solche, die aus Open-Source-Sicht unerwünschte nicht freie Komponenten oder Netzwerkdienste nutzen.

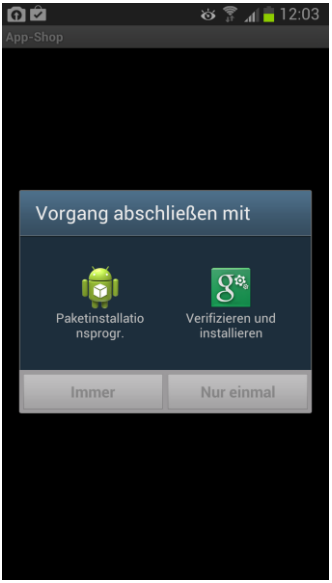
Der App Shop von **pdassi** kann mit einer speziellen App aufgerufen werden oder auch einfach im Browser auf dem Smartphone. Man kann auch vom PC aus einkaufen und bekommt die Downloadlinks der Apps dann als E-Mail aufs Handy zugeschickt

Warnungen sind Marketing für Google Play Store

Die Installation einer App aus einer APK-Datei oder aus einer anderen vertrauenswürdigen Quelle ist technisch gleichermaßen sicher wie aus dem Google Play Store. Mit Warnungen innerhalb des Betriebssystems macht Google Marketing für seinen Play Store. Auch dort haben es Entwickler immer wieder geschafft, bösartige Software zu verbreiten. Letztendlich ist jeder selbst dafür verantwortlich, welche Apps er installiert. Diese Verantwortung kann einem kein App-Shop-Betreiber abnehmen, egal ob Google Play oder ein anderer. Apps aus unbekannten Downloadseiten oder gar über einen Werbebanner zu installieren ist mehr als leichtsinnig.

Kann man der Google-App-Prüfung vertrauen?

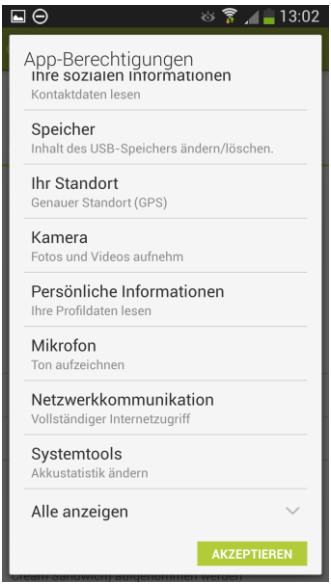
Android bietet im Gegensatz zu den beiden anderen großen mobilen Plattformen iOS und Windows Phone Entwicklern die Möglichkeit, Apps auch auf anderen Wegen als über den offiziellen Store zu verteilen. Da dies von einigen Medien als Sicherheitsrisiko angeprangert wurde, bietet Google seit Android 4.2 eine eigene App-Überprüfung für Apps, die Apps aus anderen Quellen als Google Play überprüft und bestätigt, wenn sie als gefahrlos eingestuft wurden. Diese Prüfung geht weitgehend nach den gleichen Sicherheitskriterien vor, wie die Aufnahme einer App in den Google Play Store. Trotzdem sollte man bei der Installation unbekannter Apps seinen gesunden Menschenverstand nutzen.



1. Schalten Sie in den Google-Einstellungen den Schalter *Apps bestätigen* ein.
2. Um Apps aus anderen Quellen installieren zu können, muss in den Android-Einstellungen unter *Sicherheit* der Schalter *Unbekannte Quellen* eingeschaltet sein.
3. Wenn Sie jetzt eine App aus einer anderen Quelle als Google Play installieren, erscheint die abgebildete Abfrage. Tippen Sie hier auf *Verifizieren und installieren*. Dabei werden Protokollinformationen, mit der App verbundene URLs und allgemeine Informationen über das Gerät wie die Geräte-ID, Version des Betriebssystems und die IP-Adresse an Google gesendet. Dies funktioniert nur bei einer Internetverbindung.
4. Nach erfolgreicher Prüfung wird die App installiert. Bei als schädlich bekannten Apps erscheint eine Meldung, und die Installation wird blockiert.
5. Möchten Sie in Zukunft nicht jedes Mal gefragt werden, tippen Sie in der Abfrage nach *Verifizieren und installieren* auf *Immer*. Damit werden alle Apps vor der Installation von Google überprüft.

Was bedeuten die Berechtigungen der Apps?

Zur Installation auf dem Smartphone sind nach Auswahl der App noch zwei Klicks erforderlich. Der Google Play Store zeigt an dieser Stelle, auf welche Systemkomponenten die jeweilige App zugreifen kann. Diese Berechtigungen sollte man sich in jedem Fall vor der Installation ansehen. Viele werbefinanzierte Apps fordern uneingeschränkten Internetzugriff oder gar die Berechtigung, Anrufe zu tätigen oder SMS zu verschicken. Bei Apps, wie Telefonbüchern oder Branchenverzeichnissen, ist dies zur Funktionalität wichtig, bei einfachen Spielen oder Grafikprogrammen besteht jedoch die Gefahr, dass Apps auf diesem Weg teure Verbindungen aufbauen – eine Betrugsmasche, die als Dialer schon zu Zeiten analoger Modems am PC bekannt war.



Google stuft Berechtigungen in zwei Sicherheitsstufen, *dangerous* und *normal* ein. Die Berechtigungen der Stufe *dangerous* werden direkt angezeigt, die der Stufe *normal* erst, wenn man unten auf *Alle anzeigen* tippt. 60 der insgesamt 160 in Android definierten Berechtigungen haben die Sicherheitsstufe *dangerous*. Trotz dieser Bezeichnung sind die meisten Berechtigungen für das Funktionieren einer App wirklich nötig. Achten sollten Sie vor allem auf folgende Berechtigungen:

Telefonnummern direkt anrufen – damit kann eine App beliebige Telefonnummern, auch kostenpflichtige Sonderrufnummern, anrufen, und das auch ohne dass die Telefon-App zu sehen ist.

Kurznachrichten senden – damit kann die App SMS verschicken.

Uneingeschränkter Internetzugriff – Seit das Thema App-Berechtigungen in aller Munde ist, fragt kaum noch eine App nach gezielten Internetberechtigungen, sondern verlangt immer gleich uneingeschränkten Internetzugriff, was den Blick auf die Berechtigungen schon fast wieder ad absurdum führt.

Berechtigungen installierter Apps finden

Android-Apps benötigen zum Zugriff auf sicherheitsrelevante Systemkomponenten eigene Berechtigungen, die bei der Installation der App angezeigt und vom Benutzer bestätigt werden müssen – aber wer merkt sich das schon?

Die Sicherheitslösung **G DATA AntiVirus Free** ermöglicht es, alle von installierten Apps verwendeten Berechtigungen anzuzeigen.

1. Über den Menüpunkt *Berechtigungen* zeigt G DATA AntiVirus Free eine Liste aller wichtigen Berechtigungen und wie viele Apps die jeweilige Berechtigung nutzen.

2. Tippen Sie auf eine Kategorie, um eine Liste aller Apps zu sehen, die diese Berechtigung haben. So ist im abgebildeten Beispiel völlig unklar, warum ein Python Tutorial die Berechtigung braucht, Telefonanrufe zu initiieren.

3. Da man einer App nicht ohne Weiteres eine Berechtigung entziehen kann, können verdächtige Apps direkt aus dieser Liste heraus deinstalliert werden.

Neue Funktion in Android 4.3

Bisher noch unbestätigten Berichten zufolge soll die kommende Android-Version 4.3 eine Möglichkeit beinhalten, installierten Apps einzelne Berechtigungen nachträglich wieder zu entziehen. Wie dies funktioniert, wird man erst erfahren, wenn Google diese Funktion offiziell freischaltet. Auch ist noch nicht klar, wie Apps, die nicht darauf vorbereitet sind, auf den Entzug bestimmter Berechtigungen reagieren.

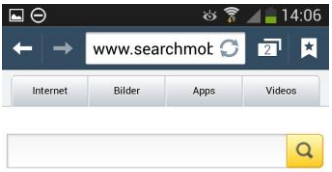
App-Berechtigungen einschränken

Offiziell ist es noch nicht möglich, aber mit einem Trick und einer speziellen App lassen sich schon in der derzeitigen Android-Version die Berechtigungen von Apps einschränken.

SRT AppGuard ermöglicht, installierten Apps einzelne Berechtigungen zu entziehen, und das sogar ohne dass das Smartphone gerootet ist. Diese App nutzt einen Umweg, der von Google nicht erwünscht ist. Daher wurde die App aus dem Google Play Store verbannt. Installieren Sie sie direkt von der Seite www.srt-appguard.com/de oder über den QR-Code.

1. SRT AppGuard fügt jeder App eine Überwachungsbibliothek hinzu, um die Rechtekonfiguration dynamisch ändern zu können. Dazu wird die App deinstalliert und anschließend neu installiert. Da AppGuard ohne Root-Recht arbeitet, muss die zu überwachende App ersetzt werden. Durch die Deinstallation gehen die gespeicherten Daten der App einmalig verloren.
2. Derzeit können folgende Berechtigungen überwacht werden: Anrufe tätigen, Kurznachrichten verschicken, Zugriffe auf Ihre Kamera, Internetzugriffe, Positionsabfragen, Zugriffe auf Ihre Kontakte, Kalender und Kurznachrichten. Dies gilt nur für Funktionen, die über die Android-API aufgerufen werden. Nutzt eine App nativen Maschinencode, lassen sich die entsprechenden Funktionen nicht überwachen.
3. Die Überwachung von vorinstallierten System-Apps ist technisch nicht möglich, da sich diese nicht deinstallieren und deshalb auch nicht ersetzen lassen.
4. Überwachte Apps, über den Google Play Store installiert, werden durch AppGuard selbst aktualisiert. Ein Update über den Google Play Store selbst ist nicht mehr möglich.

Wo lauert gefährliche und lästige Werbung?



Da nur noch sehr wenige Benutzer bereit sind, für Apps zu bezahlen, finanzieren viele Entwickler ihre Arbeit über Werbung, die in die Apps eingebaut wird.

Google selbst bietet Entwicklern die Möglichkeit, über seinen Dienst AdMob Werbung in Apps einzublenden. Diese Werbung wird noch von den meisten Nutzern akzeptiert, da sie kaum aufdringlich ist und die Nutzung außerhalb der betroffenen App nicht einschränkt. Es gibt aber deutlich aufdringlichere Werbeformen, die zusätzlich auch Informationen über Gerät oder Person sammeln.

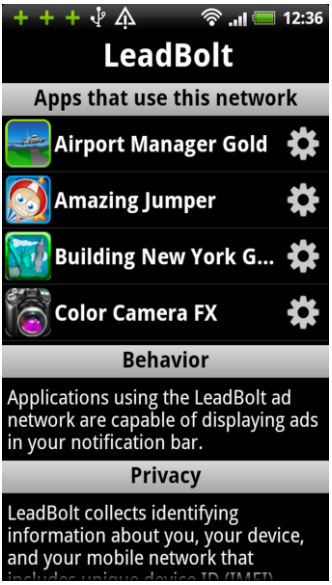
Der Werbeanbieter StartApp betreibt eine eigene Suchmaschine, über die mit gesponserten Suchergebnissen Werbeeinnahmen erzielt werden können. Der Benutzer einer werbefinanzierten App bekommt, ohne dass er von der Installation etwas merkt, ein neues Suchsymbol auf den Startbildschirm seines Handys, ein neues Lesezeichen *Web Search* sowie eine neue Startseite im Browser. Alle drei verweisen auf die Suchmaschine www.searchmobileonline.com, verbunden mit einer persönlichen App-ID, über die die Einnahmen abgerechnet werden. Viele Benutzer werden die Veränderung gar nicht wahrnehmen, da die Suchseite dem Design der Google-Suche angeglichen ist. Nachdem dieser Anbieter vor einiger Zeit schwer in die Kritik geraten ist, wurde unten auf der Suchseite ein kleiner Hinweis eingebaut, aus welcher App die Suchmaschine installiert wurde.

So wird man es los

Wen die neue Suchmaschine stört, der kann das Symbol auf dem Startbildschirm und das Lesezeichen einfach löschen und die Startseite im Browser wieder auf den Standard zurücksetzen. Allerdings werden die Änderungen bei jedem Start der werbefinanzierten App erneut vorgenommen.

Handy auf Werbenetzwerke durchsuchen

Die meisten Entwickler werbefinanzierter Apps bauen ihre Werbung nicht selbst ein, sondern nutzen eines der großen Werbenetzwerke. Hier brauchen sie nur noch einen Code einzubinden und sich dann um Anzeige und Inhalte der Werbung nicht mehr zu kümmern. Für den Benutzer kann das ein Vorteil sein – Werbung ist leichter zu finden.

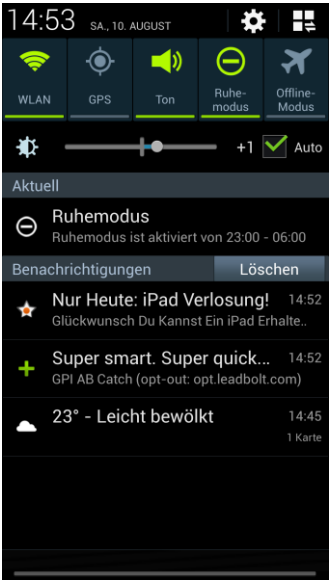


1. Die App **Lookout Ad Network Detector** prüft alle auf dem Smartphone installierten Apps auf integrierte Werbefunktionen. Dabei werden fast alle bekannten Werbenetzwerke berücksichtigt, sodass der Prüfung kaum etwas entgehen sollte. Lassen Sie den Scan einmal laufen, werden Sie sich wundern, wie viele kostenlose Apps Werbung nutzen. Das Ergebnis wird nach Funktionen klassifiziert, die die Werbenetzwerke auf dem Smartphone nutzen können.

2. In jeder der typischen Kategorien werden die für die Werbung verantwortlichen Apps aufgelistet. Dazu gibt es ausführliche Informationen über das Verhalten und die in Bezug auf Datenschutz und Sicherheit relevanten Bedenken. Einige Werbenetzwerke bieten Opt-Out-Seiten, über die man ein Smartphone schützen kann. Diese werden, falls vorhanden, angezeigt.

3. Unerwünschte Werbe-Apps kann man direkt aus diesen Listen heraus sofort deinstallieren. Nach der Deinstallation sollte man noch unerwünschte Symbole auf dem Startbildschirm sowie veränderte Lesezeichen und Suchmaschineneinträge im Browser beseitigen, da auch diese schnell wieder neue Werbe-Apps herunterladen können.

Urheber lästiger Werbe-Pop-ups finden und loswerden



Besonders lästig und penetrant sind die Werbungen von Airpush und Leadbolt. Wurde eines dieser Systeme über eine darüber finanzierte App einmal gestartet, erscheinen immer wieder Werbeanzeigen in Form von Systembenachrichtigungen in der Benachrichtigungsleiste am oberen Bildschirmrand. Zieht der Benutzer diese nach unten, erscheint die Werbeanzeige. Diese Art von Werbung wird gerne für zweifelhafte Dating- und Abodienste genutzt. Oftmals hat der Anzeigetext in der Systembenachrichtigung nichts mit der später angezeigten Werbung zu tun. Zusätzlich kann Airpush neue Symbole auf dem Startbildschirm anlegen, die auf Webseiten führen, wo weitere Werbe-Apps heruntergeladen werden.

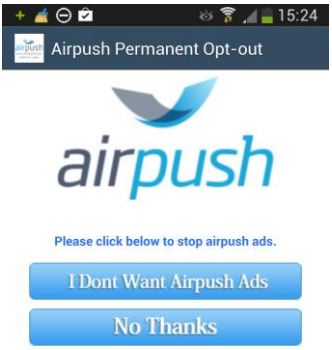
1. Tippen Sie auf Geräten mit Android 4.1 und neuer länger auf eine dieser Nachrichten in der Benachrichtigungsleiste, erscheint eine Schaltfläche *App-Info*.

2. Tippen Sie darauf, erscheinen die jeweiligen App-Informationen. Hier können Sie der App verbieten, Benachrichtigungen anzuzeigen, oder sie auch direkt deinstallieren.

3. Vor Android 4.1 gab es diese Funktion noch nicht. Auf älteren Smartphones hilft die kostenlose App **Airpush Detector**, die Übeltäter zu finden und zu deinstallieren. Einfach nur zu verbieten, Benachrichtigungen anzuzeigen, war damals noch nicht möglich.

Werbung gezielt abmelden

Die Werbeanbieter Airpush, Leadbolt und einige weitere, die auf diese Art von Werbung aufgesprungen sind, mussten aus Datenschutzgründen eine Opt-Out-Möglichkeit anbieten, damit Nutzer die Möglichkeit haben, dieser Werbung gezielt zu widersprechen.



1. Unter www.airpush.com/optout bzw. opt.leadbolt.com können Benutzer über ihre IMEI-Nummer permanent dieser Form von Werbung widersprechen. Das angegebene Handy wird davor geschützt. Die IMEI-Nummer finden Sie in den Einstellungen unter *Info zu Gerät*.

2. Airpush bietet selbst eine App **Airpush Permanent Optout** an, um der Werbung zu widersprechen. Beim Start überträgt die App die IMEI des Smartphones an Airpush und setzt dieses dort auf eine Sperrliste, damit in Zukunft keine Werbung mehr erscheint. Danach kann die App wieder deinstalliert werden, das Handy bleibt vor Airpush-Werbung geschützt, die betreffenden Apps, die dieses Werbesystem nutzen, laufen aber weiterhin.

Kommentare im Google Play Store ignorieren

Wie in allen Onlineshops gilt auch bei Google Play, die Dümmsten schimpfen am lautesten. Bei Kommentaren, die behaupten, diese App würde nicht funktionieren, sitzt der Fehler nicht in der App, sondern wie so oft vor dem Bildschirm. Mit der App *Airpush Permanent Optout* schützt Airpush selbst absolut sicher vor seiner eigenen Werbung. Ähnliche Werbung anderer Werbeanbieter wie Leadbolt wird natürlich nicht blockiert.

Werbung im Browser abschalten

Werbung auf Webseiten nervt – besonders wenn es sich um Videos, Musik, Flash-Werbung oder Überblendungen handelt, die schwer wegzuklicken sind. Einfache Banner sind im Browser auf dem PC noch einigermaßen zu ertragen, auf dem Smartphone kosten sie aber teures Datenvolumen, das auf anderem Weg sinnvoller einzusetzen ist.

Der beliebte Werbeblocker **Adblock Plus** ist auch für Android-Smartphones erhältlich und blockiert im Browser wie auch in vielen anderen Apps die meiste unerwünschte Werbung, allerdings nur über WLAN-Verbindungen, da das Android-Sicherheitssystem den direkten Zugriff auf Mobilfunkverbindungen unterbindet. Dazu sind Root-Rechte nötig. Mehr zum Thema Rooten sowie den damit verbundenen Vorteilen, aber auch Gefahren finden Sie am Ende dieses E-Books.

1. Da Google als einer der größten Werbevermarkter im Internet Werbeblocker gar nicht gerne sieht, kann Adblock Plus nicht über den Google Play Store angeboten werden. Besuchen Sie daher zur Installation mit dem Browser auf dem Smartphone die Webseite adblockplus.org oder nutzen Sie den abgebildeten QR-Code.

2. Starten Sie Adblock Plus nach der Installation und tippen Sie auf *Konfigurieren*. Nach einer kurzen Informationsseite kommen Sie direkt zu den WLAN-Einstellungen.

3. Tippen Sie länger auf die aktuelle WLAN-Verbindung und wählen Sie *Netzwerkkonfiguration ändern*. Schalten Sie im nächsten Dialogfeld *Erweiterte Optionen anzeigen* ein und wählen Sie in der Liste *Proxy-Einstellungen* die Option *Manuell*.

4. Tragen Sie bei Proxy-Hostname *localhost* ein und bei Proxy-Port *2020*. Bestätigen Sie die Änderung mit *Speichern*. Verwenden Sie verschiedene WLAN-Verbindungen, müssen Sie jede entsprechend konfigurieren.

Adblock Plus im Firefox-Browser

Verwenden Sie auf dem Smartphone den Firefox-Browser, wird Adblock Plus dort keine Werbung blockieren. Firefox verwendet auf Android-Smartphones wie auch unter Windows eigene Proxy-Einstellungen und nutzt nicht die des Betriebssystems. Adblock Plus bietet deshalb eine eigene Firefox-Erweiterung auch für die Android-Version des Browsers an.

1. Besuchen Sie mit dem Firefox-Browser auf dem Smartphone die Webseite opt.leadbolt.com oder nutzen Sie den abgebildeten QR-Code und tippen dort auf *Für Firefox installieren*.

2. Das Sicherheitssystem von Firefox blockiert die Installation von Add-Ons auf fremden Seiten. Tippen Sie in der Meldung oben auf *Erlauben*.

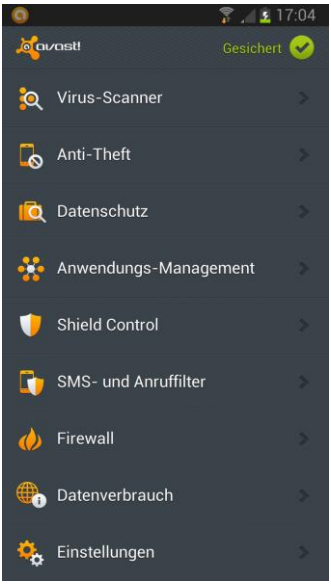
3. Der Menüpunkt *Extras/Add-Ons* in Firefox zeigt eine Liste aller installierten Erweiterungen. Tippen Sie hier auf Adblock Plus, können Sie einige Einstellungen vornehmen, wie unter anderem das gewünschte Filterabonnement auswählen.

Was ist nicht aufdringliche Werbung?

In Absprache mit großen werbefinanzierten Webseiten hat Adblock Plus einen Schalter *Einige nicht aufdringliche Werbung zulassen* eingebaut. Damit ist es möglich, bestimmte einfache Bannerwerbung, die keine Inhalte verdeckt und den Nutzer nicht mit Musik oder extrem hohem Datenvolumen belästigt, weiterhin zuzulassen. So können Benutzer Webseiten unterstützen, die nicht aufdringliche Werbung verwenden, und damit ein Zeichen gegenüber anderen Seiten setzen. Der Schalter ist automatisch aktiviert. Die meisten Nutzer verändern die Standardeinstellungen einer App nie. Standardmäßig ausgeschaltet würde diese Funktion ihren Zweck nicht erfüllen.

Braucht man Virenscanner für Android?

Sind Android-Viren nur Angstmacher?



Android-Apps laufen in gesicherten Umgebungen, sogenannten Sandboxen und haben standardmäßig keinen Zugriff auf andere Anwendungen oder deren Daten. Erst durch die bereits erwähnten Berechtigungen können bestimmte Funktionen von Apps aus der Sandbox heraus auf andere Komponenten zugreifen.

Die unbeabsichtigte Installation schädlicher Software allein durch den Besuch einer Webseite ist bei Android nicht möglich. Jede App muss bewusst installiert werden, über einen Download, aus einer E-Mail oder von der Speicherkarte. Dabei bestätigt man auch die erforderlichen Berechtigungen der App.

Tatsächlich gibt es zwar jede Menge Test-Malware aber keine wirklich in der Realität ausgebrochene Virenepidemie auf Android-Smartphones. Die Hersteller von Sicherheitssoftware erweitern daher das Funktionsspektrum ihrer Programme auf Diebstahlschutz, Datenschutz, Anruffilter, Erkennung von Werbenetzwerken und diverse weitere Features, da sich allein mit dem Scannen nicht vorhandener Viren kein Geld verdienen lässt.

Gesundes Verhalten erspart die Medizin

Auf Smartphones gilt noch mehr als auf PCs, dass ein gesunder Menschenverstand beim Umgang mit Apps, Webseiten und E-Mails deutlich mehr Sicherheit bietet als ein Virenscanner, der durch seine Hintergrundaktivität nur den Akku leer saugt, ohne einen Virus zu finden.

Der sogenannte WhatsApp-Virus

Da es auf nicht gerooteten Android-Smartphones kaum möglich ist, sich unbemerkt Malware einzufangen, gehen Malware-Autoren neuerdings andere Wege, wie der sogenannte WhatsApp-Virus Priyanka zeigt. Die Chat-App WhatsApp gehört zu den beliebtesten Apps und ist zurzeit auf jedem zweiten Android-Smartphone der Welt installiert.

Der sogenannte WhatsApp-Virus Priyanka ist kein Virus im eigentlichen Sinne, sondern eine präparierte Kontaktdatei, die auf verschiedenen Wegen zum Download angeboten wird. Diese benennt, nachdem man sie einmal aufgerufen hat, Chatgruppen und Kontakte in *Priyanka* um, einen in Indien sehr häufigen Vornamen – sogar eine frühere Miss World trug diesen Namen. Die Datei verbreitet sich nicht wie ein Virus selbstständig weiter, sondern muss bewusst versendet und geöffnet werden, daher wird sie in Deutschland nicht so schnell gefährlich, da hier fast niemand Priyanka heißt. Sollten Sie sich diese Datei doch eingefangen haben, gehen Sie folgendermaßen vor.

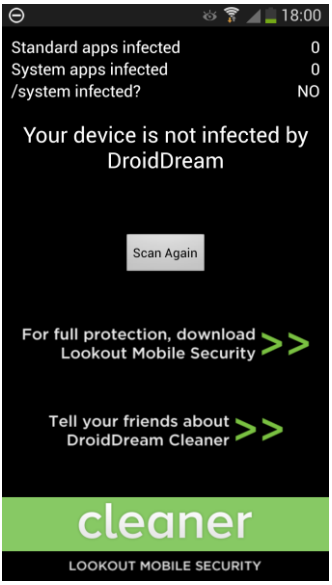
1. Schalten Sie das Smartphone auf Flugmodus, um alle Internetverbindungen zu trennen.
2. Löschen Sie den Eintrag *Priyanka* im Adressbuch, ohne ihn zu öffnen.
3. Wählen Sie in den Einstellungen unter *Anwendungsmanager* die App WhatsApp und tippen Sie auf *Stopp erzwingen*. Tippen Sie danach dort auf *Daten löschen*.
4. Bei einer Neuanmeldung mit der gleichen Handynummer stellt WhatsApp die letzten Chats sowie die Kontaktliste wieder her.

Aktualisieren Sie WhatsApp auf die neueste Version

Ab Version 2.10.768 ist WhatsApp immun gegen diese Sicherheitslücke.

DroidDream – die erste echte Malware

Im Jahr 2011 tauchte in etwa 50 Apps im Google Play Store die erste wirkliche Malware mit Namen DroidDream auf. Google reagierte schnell und entfernte die betroffenen Apps aus dem Store. Sie waren bis dahin aber schon 50.000 bis 200.000 Mal heruntergeladen worden.



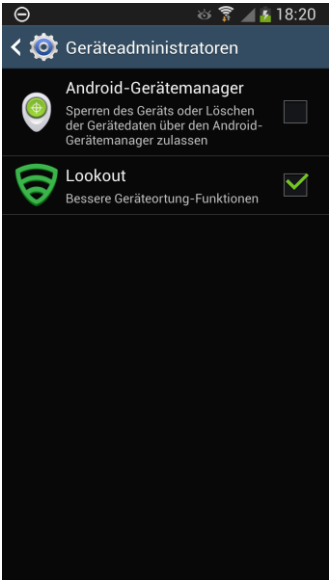
Alle betroffenen Apps stammen von Entwicklern, die sich *Kingmail2010*, *we20090202* oder *Myournet* nennen. Die meisten Apps waren Raubkopien von Apps, die gezielt wenig auf Sicherheit bedachte Nutzer ansprechen: Super Ringtone Maker, Super Sex Positions, Hot Sexy Videos, Hilton Sex Sound, Screaming Sexy Japanese Girls, Sexy Legs, Panzer Panic, Super Sexy Ringtones und Ähnliche.

DroidDream nutzt eine alte Sicherheitslücke, die nur auf Smartphones mit Android 2.2.0 und älter vorhanden war. Auf diesen Geräten konnte Google die gefährlichen Apps auch noch nicht per Fernzugriff löschen.

DroidDream enthält einen Code, der die betroffenen Smartphones rootet und anschließend unbemerkt einen Trojaner installiert, der Gerätedaten an einen Server in Kanada verschickt.

Sollten Sie noch ein Smartphone mit Android 2.2.0 oder älter verwenden und möchten sicher gehen, dass dieses nicht mit DroidDream infiziert ist, installieren Sie die App **DroidDream Cleaner**. Diese findet den Schädling und beseitigt alle gefährlichen Dateien.

Der neue Android-Trojaner Backdoor.AndroidOS.Obad.a



Im Sommer 2013 entdeckte die Firma Kaspersky, bekannter Hersteller von Virenschutzprogrammen, einen neuen Android-Trojaner *Backdoor.AndroidOS.Obad.a*, der angeblich über Downloadlinks in SMS-Nachrichten verbreitet wurde, also bewusst heruntergeladen und installiert werden muss.

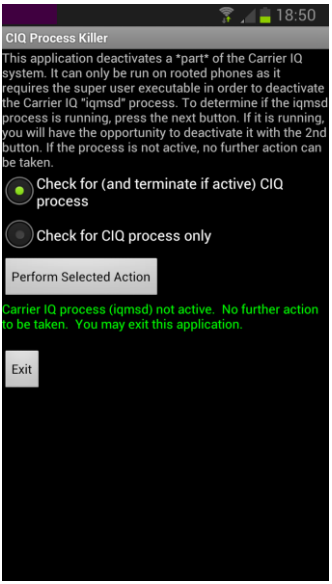
Der Trojaner, dessen Code nach Aussage von Kaspersky verschlüsselt ist, soll SMS an kostenpflichtige Rufnummern verschicken, die in der SMS-Liste nicht auftauchen. Dazu sind Geräteadministrator-Rechte notwendig.

1. Sollte eine App bei der Installation nach der Anzeige der Berechtigungen auf einem weiteren Bildschirm Geräteadministrator-Rechte anfordern, sollten Sie auf jeden Fall stutzig werden. Diese Rechte sind nur für Hintergrundaktivitäten wie z. B. Bildschirmsperren oder komplettes Löschen aller Daten notwendig.
2. In den Einstellungen unter *Sicherheit/Geräteadministratoren* sehen Sie jederzeit, welche Apps diese Berechtigungen haben, und können das Recht auch durch einfaches Ausschalten des Häkchens entfernen.
3. Sollte sich eine App über den Anwendungsmanager nicht deinstallieren lassen, liegt dies oft an Geräteadministrator-Rechten. Entfernen Sie diese, lässt sich die jeweilige App auch entfernen.

Gibt es diesen Virus wirklich?

Die Entdeckung dieses Trojaners durch Kaspersky ging durch alle Medien. Kaspersky selbst stuft die Verbreitung dieser Malware als sehr gering ein. Kein anderer Softwarehersteller hat den Trojaner erwähnt. Handelt es sich möglicherweise um einen Test, der im echten Leben – im Fachjargon der Virenjäger als Wildlife bezeichnet – gar nicht auftaucht?

Die Schnüffelsoftware Carrier IQ



Die amerikanische Softwarefirma Carrier IQ liefert an Netzbetreiber eine Software, die weit mehr als nur Qualitätskontrolle macht. Das Tool, das Handyhersteller und Netzbetreiber auf Smartphones vorinstallieren können, soll für den Service relevante Informationen auf den Geräten sammeln, um den Netzbetreibern zu helfen, ihre Mobilfunknetze zu optimieren.

Trevor Eckhart, ein unabhängiger Android-Entwickler, hat herausgefunden, dass diese ursprünglich als harmlos eingestufte Software noch weit mehr Daten ermittelt. So kann Carrier IQ, kurz als CIQ bezeichnet, Textnachrichten, besuchte Webseiten, Standortinformationen und auch gedrückte Tasten protokollieren – und das auch, wenn man nicht in einem Mobilfunknetz, sondern über WLAN im Internet ist, sogar bei https-Verbindungen. Eckhart vergleicht das Verhalten der Software mit einem Rootkit, da sie tief ins Betriebssystem eingreift und sich mit üblichen Mitteln auch nicht entfernen lässt.

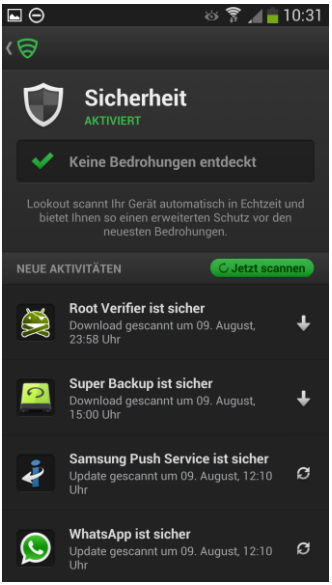
Die App **Carrier IQ Process Killer** erkennt die Carrier IQ Software, sollte diese auf dem Smartphone installiert sein, und bietet die Möglichkeit, zumindest laufende Prozesse zu beenden. Eine komplette Entfernung von Carrier IQ aus dem Betriebssystem ist mit keiner App möglich.

Bisher wurde die Carrier-IQ-App im Wesentlichen auf Geräten US-amerikanischer Mobilfunkanbieter entdeckt, aber auch die ersten deutschen Handys sollen Medienberichten zufolge damit versorgt worden sein. Carrier IQ bietet seine Tools außer für Android-Handys auch für das iPhone, BlackBerry und Nokia-Handys mit Symbian OS an, nach Herstellerangaben ist die Software auf mehr als 140 Millionen Handys installiert. Welche der erfassten Daten tatsächlich an Netzbetreiber oder den Softwarehersteller weitergegeben werden, ist nicht dokumentiert.

Tipps zu beliebten Sicherheits-Apps

Lookout Security & Antivirus Free

Lookout Security & Antivirus ist eine Sicherheitslösung für Android, die neben dem unwahrscheinlichen Virenrisiko auch vor deutlich wahrscheinlicheren Risiken schützt – und das auch in der kostenlosen Version.



Lookout überprüft jede installierte App und auch jedes Update auf mögliche Malware-Infektionen und überprüft auch im Hintergrund das Smartphone auf gefährliche Aktivitäten. Zusätzlich kann man jederzeit bei Verdacht einer Malware-Infektion das Gerät komplett überprüfen lassen.

Auf der Startseite werden die letzten Aktivitäten angezeigt. In den meisten Fällen sind das nur Updates der Malware-Signaturen sowie Bestätigungen, dass installierte Apps und Updates sicher sind.

Wer sich besonderen Gefahren ausgesetzt sieht, kann das gesamte Dateisystem des Smartphones wöchentlich oder auch täglich auf Infektionen durchsuchen lassen. Bedenken Sie dabei aber, dass diese intensiven Dateisystemzugriffe viel Strom verbrauchen.

Im Hintergrund sichert Lookout die Kontakte auf dem Handy. In der kostenpflichtigen Premium-Version lassen sich noch weitere Daten wie Fotos und Anruflisten sichern sowie auch bösartige Webseiten im Browser automatisch blockieren.

Avast Mobile Security

Avast, ein bekannter Hersteller kostenloser Virenscanner für den PC, liefert eine umfassende Sicherheitslösung für Android, in der die meisten Funktionen kostenlos sind. Da das Virenrisiko bei Android vernachlässigbar ist, wurden diverse andere sicherheitsrelevante Funktionen eingebaut.

Im Bereich *Datenschutz* werden alle Apps nach Kategorien aufgelistet, die in Bezug auf Datenschutz relevante Berechtigungen nutzen, wie z. B. Position feststellen oder auf Identitätsdaten, Nachrichten oder Kontakte zugreifen. Die betreffenden Berechtigungen werden ausführlich erklärt.

Das *Web-Shield* schützt vor schädlichen Internetseiten und Phishing im Android-Standardbrowser sowie in Google Chrome. Die Funktion *SiteCorrect* korrigiert automatisch Rechtschreibfehler in Domainnamen. Betreiber bösartiger Internetseiten registrieren gerne Domains, die sich nur durch einen Buchstaben oder Dreher von populären Webseiten unterscheiden, um so Besucher auf ihre zweifelhaften Angebote zu locken.

Mit dem *SMS- und Anruffilter* können Sie für bestimmte Telefonnummern Anrufe und SMS sperren. Um Ruhe vor dem Telefon zu haben, lassen sich Zeiten festlegen, zu denen die Sperre automatisch aktiviert wird.

Weiterhin bietet Avast einen Anwendungsmanager und eine Datenverbrauchsanzeige, die weitgehend den gleichnamigen Funktionen in Android entsprechen, in einigen Bereichen aber übersichtlicher sind. So lässt sich z. B. der Datenverbrauch an einem Tag anzeigen.

Bitdefender Clueful Privacy Advisor

Clueful zeigt, wie installierte Apps Ihre persönlichen Daten nutzen oder möglicherweise missbrauchen und wie diese Ihre Privatsphäre behandeln. Dabei werden die installierten Apps mit den Informationen der permanent aktualisierten Bitdefender-Cloud-Datenbank abgeglichen.

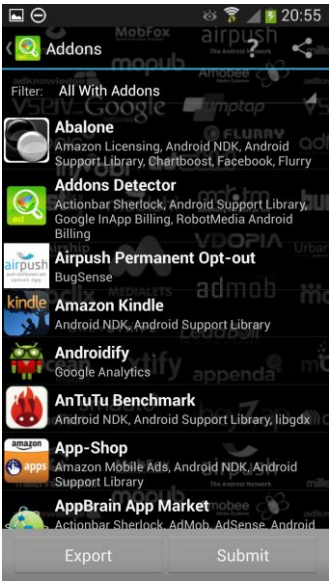
Bei der Neuinstallation einer App meldet Clueful sofort, inwieweit diese App die Privatsphäre respektiert.

Als bedenklich für die Privatsphäre gelten unter anderem Zugriff auf Kontaktdaten und Kalender, Lesen und Schreiben von SMS, Versenden von privaten Daten über das Internet, Zugriff auf Standortinformationen und auch die Verwendung aufdringlicher Werbung wie z. B. Airpush.

Aus allen ermittelten Daten der installierten Apps wird ein Privatsphäre-Faktor ermittelt, der eine grobe Auskunft darüber geben soll, wie hoch das Gefahrenpotenzial auf einem Smartphone ist.

Alle installierten Apps werden in drei Risiko-Klassen eingeordnet, die allerdings mit Vorsicht zu genießen sind. So werden Browser wegen ihres Internetzugriffs als gefährlich eingestuft und GPS-Anwendungen wegen ihres Zugriffs auf die Positionsdaten. Auch andere Sicherheits-Apps werden wegen Systemzugriffen als bedenklich angezeigt. Aber genau das sind die Aufgaben dieser Apps. Ohne die entsprechenden Berechtigungen wären sie sinnlos.

Addons Detector



Addons Detector schützt zwar weder vor Viren noch vor Diebstahl, liefert aber eine ausführliche Analyse von in installierten Apps eingebauten Add-ons.

Der Addons Detector findet nicht nur in Apps integrierte Werbenetzwerke, sondern auch noch weitere Tools, die Entwickler vom Nutzer unbemerkt in ihre Apps integrieren. Dazu gehören unter anderem Diagnose- und Analysetools, die das Benutzerverhalten ausspähen. Bei jedem Add-on wird eine ausführliche Beschreibung angezeigt, anhand derer sich jeder selbst ein Bild machen kann, inwieweit das Add-on bedenklich sein kann.

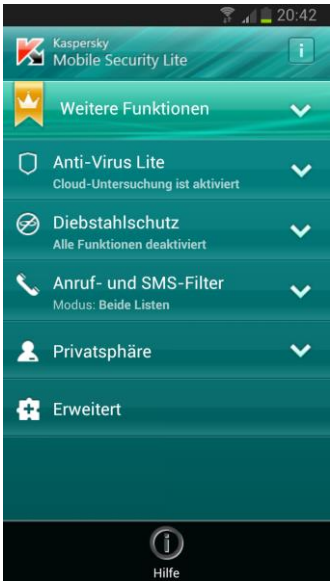
Auch Funktionen, die das Smartphone mit sozialen Netzwerken und Spielenetzwerken verbinden, werden aufgedeckt.

Die App erkennt neben den auffälligsten Werbenetzwerken Airpush und Leadbolt auch noch diverse andere, die unter Umständen bedenklich sind.

Viele Apps, die sich im Google Play Store als Freeware tarnen, enthalten versteckte Lizensierungstools, die prüfen, ob eine App legal gekauft ist oder bei Testversionen Zeitbeschränkungen setzen. Alle Apps, in denen z. B. Google InApp Billing gefunden wird, sind voraussichtlich nicht komplett kostenlos nutzbar.

Weiterhin lassen sich zu allen Apps die verwendeten Berechtigungen sehr detailliert anzeigen, sowie die Apps nach Installationsdatum sortieren, um eventuell den Übeltäter eines seltsamen Geräteverhaltens einzugrenzen.

Kaspersky Mobile Security Lite



Kaspersky liefert eine der teuersten Sicherheitslösungen für Android, die mit über 100 Euro zu den teuersten Apps im Google Play Store insgesamt gehört. Die kostenlose Version hat den Namen *Lite* verdient, enthält sie doch nur einen Bruchteil der Funktionen der Vollversion.

Neu installierte Apps werden automatisch über den Cloud-Service von Kaspersky überprüft.

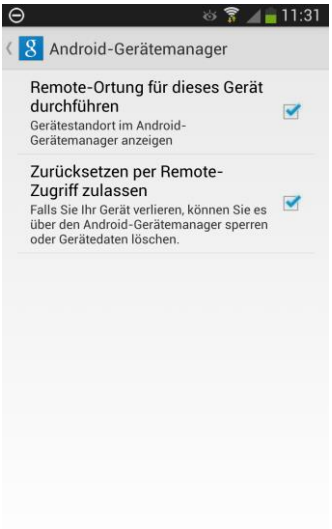
Über Anruf- und SMS-Filter können Sie schwarze und weiße Listen festlegen, die Telefonnummern enthalten, die nie bzw. immer anrufen und SMS schicken dürfen. Auf diese Weise kann man sich Ruhe vor dem Telefon verschaffen. Verwenden Sie die weiße Liste in Kombination mit der Einstellung *Kontakte erlauben*, lassen sich auch Anrufer mit unterdrückter Rufnummer automatisch wegfiltern.

Selbst die kostenlose Version enthält Funktionen zum Diebstahlschutz. Über spezielle SMS, die man von einem beliebigen Handy an das verlorene schickt, lässt sich dieses ferngesteuert blockieren und eine Nachricht für den Finder anzeigen. Außerdem ist es möglich, per SMS und Geheimcode bestimmte Ordner auf dem Smartphone ferngesteuert zu löschen oder die GPS-Koordinaten per SMS zu erhalten. Die Benachrichtigung über einen SIM-Kartenwechsel nach dem Diebstahl ist leider Nutzern der kostenpflichtigen Version vorbehalten.

Handy geklaut – was nun?

Besser vorbeugen

Wird ein Smartphone gestohlen, ist das sehr ärgerlich und kann auch teuer werden. Sie können sich einigen Ärger sparen und die Chance erhöhen, das Gerät wiederzubekommen, wenn Sie rechtzeitig Vorsorge treffen.

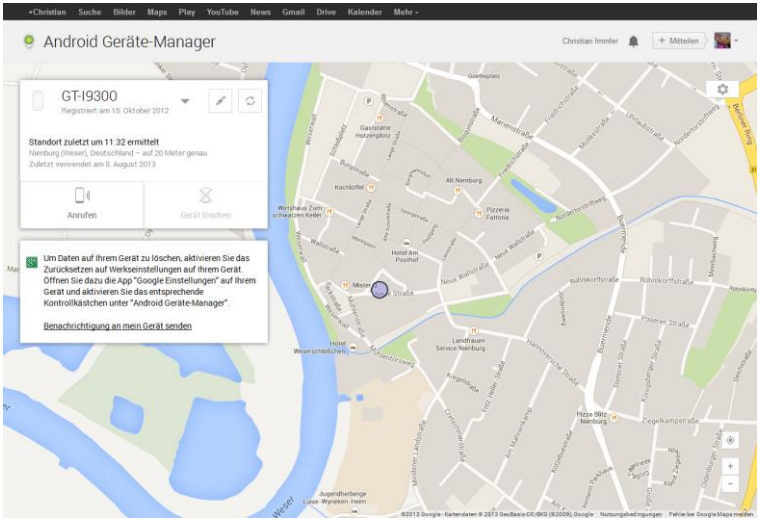


1. Schreiben Sie sich die IMEI des Smartphones auf. Diese brauchen Sie, um es im Notfall eindeutig zu identifizieren oder über den Netzbetreiber orten zu lassen. Sie finden die IMEI in den Einstellungen über *Info zu Gerät/Status*. Auf den meisten Smartphone-Verpackungen steht die IMEI außen auf einem Aufkleber. Immer mehr Gerätehersteller gehen dazu über, gleich mehrere solche Aufkleber auf der Verpackung anzubringen. Lösen Sie einen davon ab und kleben Sie sich ihn an eine Stelle, wo Sie ihn im Notfall sofort finden, z. B. in den Geldbeutel.

2. Schalten Sie in den Google-Einstellungen unter *Standort* die Optionen *Standortzugriff*, *Standortbericht* und *Standortverlauf* ein, um die Ortung über Google optimal nutzen zu können.

3. Schalten Sie unter *Android-Gerätemanager* den Schalter *Remote-Ortung* ein. Möchten Sie im äußersten Notfall das Smartphone aus der Ferne auf Werkseinstellungen zurücksetzen, wenn Sie nicht mehr davon ausgehen können, es zurückzubekommen, schalten Sie auch den Schalter *Zurücksetzen per Remote-Zugriff zulassen* ein. Dazu müssen Sie auch noch Geräteadministrator-Berechtigungen zulassen. Nach dem Zurücksetzen auf Werkseinstellungen kann das Handy über Google nicht mehr geortet werden, nur noch mithilfe der IMEI über den Netzbetreiber.

4. Schreiben Sie für ehrliche Finder Ihren Namen sowie eine Telefonnummer, auf der Sie auch ohne dieses Smartphone erreichbar sind, auf den Sperrbildschirm. Einige Gerätehersteller, wie z. B. Samsung bieten in den Einstellungen unter *Sperrbildschirm* die Möglichkeit, einen Infotext über den Besitzer auf dem Sperrbildschirm anzeigen zu lassen, auch wenn eine Bildschirmsperre aktiv ist, der Finder das Telefon also nicht in Betrieb nehmen kann. Auf Smartphones, die diese Möglichkeit nicht bieten, verwenden Sie ein persönliches Hintergrundbild für den Sperrbildschirm, in das Sie ihren Namen und Telefonnummer mit einem Bildbearbeitungsprogramm auf dem PC hineinschreiben.

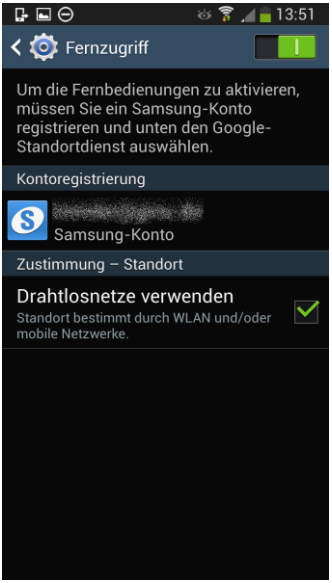


Was tun, wenn das Handy wirklich weg ist?

Auf der Seite android.com/devicemanager finden Sie nach Anmeldung mit dem persönlichen Google-Konto alle Android-Geräte, die auf dieses Google-Konto registriert sind. Mit einem Klick auf *Anrufen* können Sie das Gerät klingeln lassen, um es zu finden, wenn Sie es irgendwo in der Nähe verlegt haben. Das funktioniert auch, wenn das Handy auf lautlos gestellt ist.
Der häufig gehörte Tipp, sofort die SIM-Karte sperren zu lassen, ist bei Smartphones nicht zu empfehlen, da ohne Internetverbindung über Mobilfunk die Ortungsfunktionen nicht nutzbar sind.
Haben Sie Ihr Smartphone geortet, melden Sie den Standort sofort der Polizei zusammen mit der IMEI und der Telefonnummer der SIM-Karte, und kommen Sie nicht auf die Idee, den Täter persönlich zu besuchen.

Die Ortungsfunktion bei Samsung-Smartphones

Samsung bietet Smartphonenutzern einen eigenen Ortungsdienst für verlorene Handys, der noch mehr Funktionen als der Android Gerätemanager bietet. Hier können Sie das Smartphone orten, anrufen, sperren oder die Daten löschen.



1. Voraussetzung für die Nutzung von *Find my mobile* ist ein angemeldetes Samsung-Konto auf dem Smartphone. Geben Sie das Passwort dieses Kontos in den Einstellungen unter *Sicherheit/Fernzugriff* ein, schalten Sie oben den Fernzugriff ein und aktivieren Sie weiter unten den Google-Standortdienst.

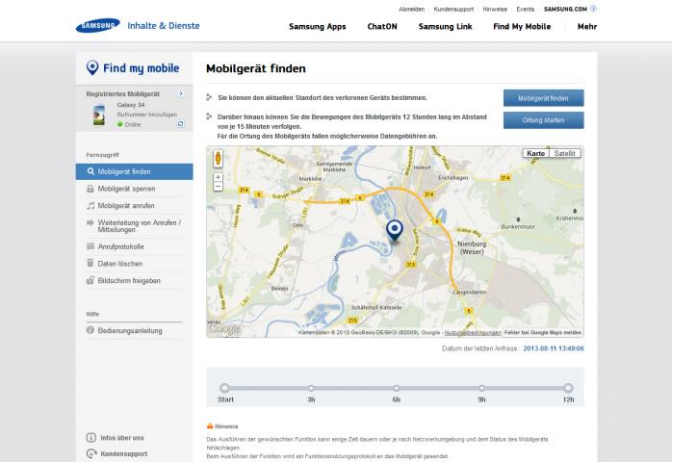
2. Wenn Sie Ihr Handy suchen, melden Sie sich auf einem PC bei findmymobile.samsung.com mit dem gleichen Samsung-Konto an und klicken auf *Mobilgerät finden*. Sie können diese Funktion auch von einem anderen Samsung-Smartphone in den Einstellungen unter *Sicherheit/Find My Mobile-Webseite* aufrufen.

3. Mit der Schaltfläche *Ortung starten* können Sie die Bewegungen des Mobilgeräts 12 Stunden lang im Abstand von je 15 Minuten verfolgen.

4. Im Bereich *Mobilgerät sperren* können Sie das Handy aus der Ferne sperren und auf dem Bildschirm eine Meldung anzeigen lassen. Hier lässt sich auch eine Telefonnummer festlegen, die vom gesperrten Handy angerufen werden kann, damit ein ehrlicher Finder sich bei Ihnen melden kann. Legen Sie weiter unten eine PIN fest, mit der Sie die Sperre Ihres Smartphones wieder aufheben können, wenn Sie es zurückbekommen haben. Dies sollte eine andere PIN sein, als sie für die SIM-Karte verwendet wird.

5. Im Bereich *Mobilgerät anrufen* können Sie das Smartphone klingeln lassen, um es zu finden, wenn Sie es irgendwo in der Nähe verlegt haben. Das funktioniert auch, wenn das Handy auf lautlos gestellt ist. Beim Klingeln kann eine beliebige Textmitteilung angezeigt werden.

6. Damit eingehende Anrufe und SMS nicht beim Dieb ankommen, tragen Sie im Bereich *Weiterleitung von Anrufen* eine Telefonnummer eines Zweithandys ein, auf das die Anrufe umgeleitet werden sollen.



7. Im Bereich *Anrufprotokolle* rufen Sie die Anrufprotokolle des Smartphones ab. Die darin enthaltenen Daten können Hinweise auf den Dieb geben. Außerdem dienen Sie als Beweismittel gegenüber dem Netzbetreiber. Profidiebe haben eigene kostenpflichtige Rufnummern, mit denen sie stundenlange Gesprächsverbindungen von gestohlenen Handys herstellen und so zusätzlich Geld in die eigene Kasse erwirtschaften. Die meisten Mobilfunkbetreiber haften erst dann für durch Diebstahl entstandene Kosten, wenn bei der Polizei eine Verlustanzeige gestellt wurde.

Samsung-Handys informieren bei SIM-Kartenwechsel

Manche Diebe tauschen die SIM-Karte in gestohlenen Handys aus, um Ortungsversuchen zu entgehen oder das Gerät trotz SIM-PIN zu nutzen. Geben Sie in den Einstellungen unter *Sicherheit/Info über SIM-Wechsel* die Nummer eines Zweithandys an, werden Sie benachrichtigt, wenn der Dieb eine andere SIM-Karte einsteckt. Da Sie dann auch die Nummer haben, kann die Polizei mithilfe des Netzbetreibers den Dieb identifizieren.

Prey Anti-Diebstahl-App

Die Open-Source Software **Prey** (engl. für berauben oder erbeuten) findet gestohlene Notebooks, Tablets und Handys. Außer den Koordinaten, wo sich das Gerät befindet, bekommen Sie auch Informationen über SIM-Kartenwechsel. Und das Beste: Prey fotografiert den Dieb mit der Frontkamera des Smartphones.

1. Installieren Sie die App auf dem Smartphone und legen Sie sich ein kostenloses Benutzerkonto an.

   Aktivieren Sie bei der Installation die angefragten Geräteadministratorberechtigungen.

2. Tragen Sie im Konfigurationsbildschirm von Prey die Nummer eines Zweithandys ein. Beim Wechsel der SIM-Karte sendet Ihr Smartphone eine SMS mit der neuen Nummer an dieses Handy und aktiviert Prey automatisch.

3. Im Falle eines Verlustes schicken Sie von einem anderen Handy eine SMS mit dem Inhalt GO PREY an Ihr verlorenes Smartphone. Damit wird Prey aktiviert und sendet Statusberichte.

4. Melden Sie sich bei panel.preyproject.com mit Ihrem Prey-Benutzerkonto an, um die Berichte einzusehen.

Privatsphäre der Diebe

Straftäter genießen in Deutschland einen besonderen Schutz ihrer Privatsphäre. Die Fotos, die Prey vom Dieb gemacht hat, dürfen nicht als Fahndungsaufruf z. B. auf Facebook veröffentlicht werden. Geben Sie sie am besten der Polizei als Beweismittel zusammen mit den Standortinformationen und der aktuellen Telefonnummer des gestohlenen Gerätes.

Die Ortungsfunktion von Lookout Security & Antivirus

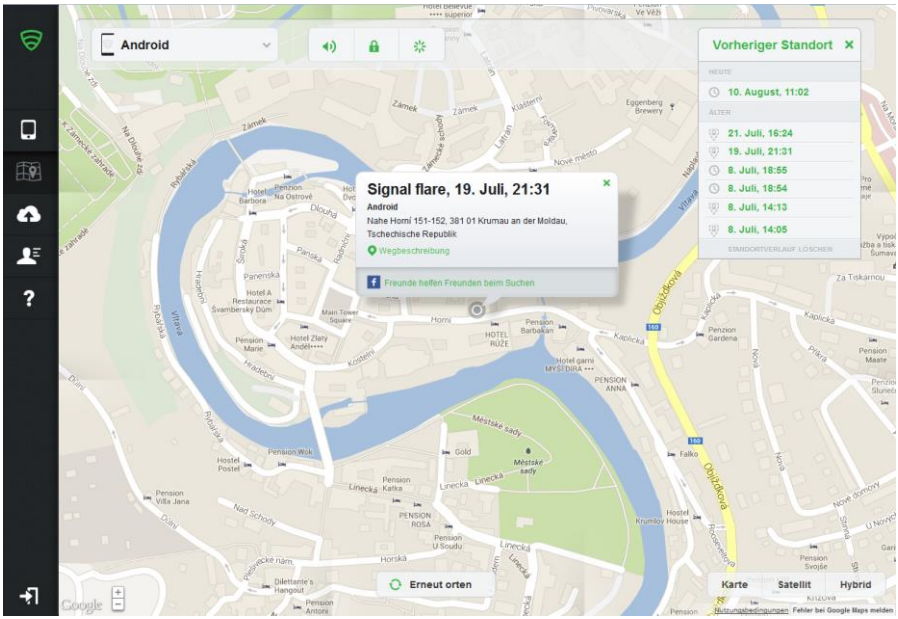
Die Sicherheitsapp **Lookout Security & Antivirus** bietet auch in der kostenlosen Version eine komfortable Ortungsfunktion für verlorene Smartphones.

1. Auf dem Startbildschirm von Lookout schalten Sie die Geräteortung ein, um den aktuellen Standort Ihres Smartphones jederzeit auf einer Landkarte anzeigen zu lassen. Dazu müssen Sie das Gerät einmal bei Lookout registrieren. Melden Sie sich später von einem PC bei www.lookout.com/de mit den gleichen Zugangsdaten an, können Sie Ihr Gerät jederzeit orten und sich auch frühere Standorte zeigen lassen.

2. Der Standort wird auf einer Google-Maps-Karte sehr genau angezeigt und der Kartenausschnitt auch per E-Mail verschickt.

3. Direkt aus dem Browser auf dem PC oder einem anderen Smartphone heraus können Sie auf dem Gerät eine sehr laute Sirene ertönen lassen, um in der Nähe verlorene Smartphones wiederzufinden oder Diebe zu erschrecken. Diese Sirene funktioniert auch, wenn das Gerät auf lautlos geschaltet ist.

4. *Signal Flare* ist ein weiterer nützlicher Schutz gegen Verlieren. Ist diese Funktion aktiviert, werden die Koordinaten des Geräts rechtzeitig gespeichert, bevor der Akku leer ist. Liegt ein Smartphone mit leerem Akku herum, kann man es nicht durch Anrufen oder über die Sirene der Ortungsfunktion wiederfinden.



5. Haben Sie Ihr Smartphone mit einem PIN-Code oder einem Sperrmuster geschützt, schalten Sie die Funktion *Lock Cam* ein. Versucht dann eine unbefugte Person dreimal, die PIN bzw. das Sperrmuster einzugeben, wird sie automatisch mit der Frontkamera fotografiert und das Bild zusammen mit dem aktuellen Gerätestandort per E-Mail an Sie verschickt.

6. Damit *Lock Cam* und andere systemnahe Funktionen genutzt werden können, braucht Lookout Security & Antivirus erweitere Berechtigungen, die als *Geräteadministrator* bezeichnet werden. Schalten Sie diese in den Einstellungen frei. Bevor die App Lookout Security & Antivirus deinstalliert werden kann, muss der Geräteadministrator deaktiviert werden.

Die Funktionen zum Sperren des Geräts und zum Löschen der persönlichen Daten aus der Ferne sind Nutzern der kostenpflichtigen Version von Lookout Security & Antivirus vorbehalten.

Plan B, wenn das Handy weg ist

Alle erwähnten Diebstahlschutz-Apps für Android-Handys müssen vorbeugend installiert werden, damit man im Notfall aus der Ferne auf die installierte App zugreifen kann. Plan B findet ein Handy, auch wenn es schon zu spät ist, noch mit hoher Wahrscheinlichkeit. Die App kann nachträglich aus der Ferne installiert werden und nutzt dazu die Funktion des Google Play Store auf dem PC, Apps von dort auf dem eigenen Smartphone zu installieren.

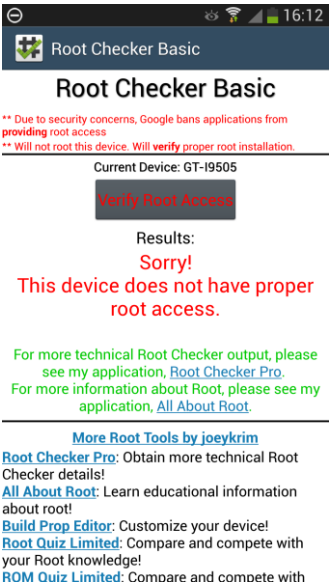
1. Suchen Sie im Webbrowser auf dem PC bei play.google.com die App **Plan B**. Dabei müssen Sie mit dem gleichen Google-Konto angemeldet sein, das auch auf dem gestohlenen Smartphone genutzt wird.
2. Installieren Sie jetzt die App vom PC auf dem gestohlenen Smartphone. Dieses muss dazu eingeschaltet sein und eine Internetverbindung haben, wovon in den meisten Fällen auszugehen ist.
3. Nachdem sich die App dort ohne Zutun des Diebes installiert hat, sendet sie automatisch eine E-Mail an Ihre Googlemail-Adresse, die den Standort enthält. Diese Mail sollten Sie möglichst sofort auf einem PC lesen und sichern, da sie auf dem Smartphone auch ankommt und ein Dieb sie dort möglicherweise gleich löscht. Wenn das Smartphone sich bewegt, werden in den nächsten 10 Minuten weitere Mails gesendet.
4. Um später, nachdem Plan B installiert ist, nochmals den Standort abzufragen, schicken Sie eine SMS mit dem Wort *locate* an das Smartphone. Plan B wird dann wieder E-Mails senden.

Einschränkung

Plan B funktioniert wegen einer technischen Einschränkung nur auf den Android-Versionen 2.0 – 2.3.4 und nicht auf aktuellen Versionen 4.x.

Sicherheitsrisiko Routing

Was bedeutet root?



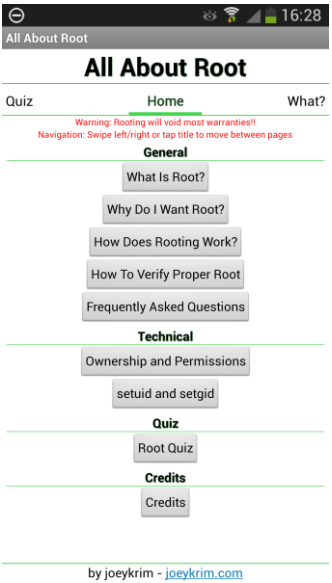
Da Android auf Linux basiert, geht es auch von einem normalerweise eingeschränkten Benutzerkonto aus, dem kritische Systemzugriffe verwehrt werden. Ein spezieller Benutzer *root* hat Zugriff auf das komplette System, was natürlich auch mit hohen Risiken verbunden ist. Android-Nutzer können mit speziellen – von den Geräteherstellern nicht autorisierten – Tools sich selbst Root-Zugriff auf ihr Handy freischalten. Im gerooteten Modus sind noch weit mehr Funktionen möglich, was auch Entwicklern einen großen Spielraum für spezielle Root-Apps bietet. So ist zum Beispiel das Übertakten des Prozessors oder die Installation nicht autorisierter sogenannter CustomROMs nur mit Root-Rechten möglich, da bestimmte Schutzmechanismen des Systems übergangen werden müssen. Gerootete Handys haben keine Sicherheitsmechanismen mehr. Sie stehen Trojanern und anderer bösartiger Software völlig offen gegenüber. Einige Trojaner rooten bei ihrer Installation das Handy, um anschließend weitere Software nachzuinstallieren.

Sind Sie sich nicht sicher, ob Ihr Smartphone gerootet ist oder nicht, hilft die kostenlose App **Root Checker Basic** weiter. Diese App überprüft das Smartphone auf mögliche Root-Zugriffe, ohne es selbst zu rooten oder irgendwelche anderen Veränderungen vorzunehmen.

Das Rooting an sich ist zwar mittlerweile weitgehend sicher, danach hat man aber volle Rechte auf dem System und kann durch Fehlbedienung oder bösartige Apps, die ohne Rootzugriff nicht laufen, sein System eventuell unwiderruflich be-

schädigen. Mit Übertaktungs-Apps lässt sich sogar die Hardware dauerhaft schädigen. Die meisten Gerätehersteller lehnen Garantieansprüche für gerootete Geräte grundsätzlich ab. Ein Android-Gerät zu rooten ist aber nicht illegal, da im Gegensatz zu Jailbreaks auf dem iPhone keine Urheberrechte verletzt und auch keine bewusst gesetzten Sperren aufgebrochen werden.

Der genaue Vorgang des Rootens ist von Smartphone zu Smartphone unterschiedlich und funktioniert nicht einmal bei allen Geräten eines Herstellers auf die gleiche Weise. Die App **All About Root** liefert ausführliche Informationen zur Technik des Rootens.



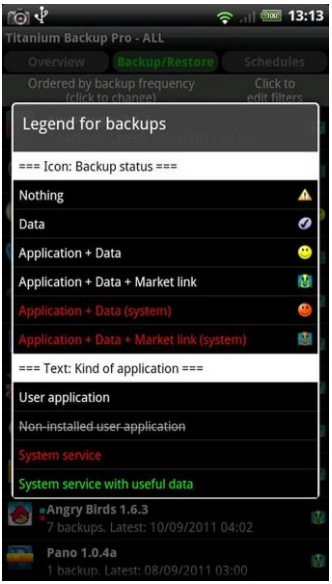
1. Zum Rooten muss sich das Smartphone im Entwicklermodus mit eingeschaltetem USB-Debugging befinden. Wie das Umschalten in den Entwicklermodus genau funktioniert, ist bei jedem Handy anders. Den Schalter für das USB-Debugging finden Sie in den Einstellungen unter *Entwickler-Optionen*.

2. Herstellerspezifische Software zur Kommunikation zwischen PC und Handy, wie z. B. Samsung Kies-Software, darf während der USB-Verbindung zum Rooten nicht laufen, auch nicht im Hintergrund. Beenden Sie mit dem Taskmanager alle diesbezüglichen Prozesse.

3. Jetzt benötigen Sie noch spezielle USB-Treiber aus dem Android SDK, das Flashing-Tool *Odin* sowie eine gepatchte Firmware-Datei passend zu Ihrem Smartphone.

4. Starten Sie dann das Smartphone im Downloadmodus. Dies funktioniert je nach Handymodell über eine bestimmte Tastenkombination, und übertragen Sie anschließend die gepatchte und mit Root-Zugriff versehene Firmware auf das Smartphone.

Backup für gerootete Geräte



Bei allen Risiken hat das Rooten aber auch Vorteile, vorausgesetzt, man weiß genau, was man tut. So ist es nur mit Root-Zugriff möglich, alle installierten Apps und auch die von diesen Apps gespeicherten Daten zu sichern.

Titanium Backup ist eine Datensicherungslösung für Android-Smartphones, die nicht nur Daten, sondern auch installierte Apps auf die Speicherkarte sichert. Das funktioniert auch mit Kauf-Apps und System-Apps.

Titanium Backup sichert im manuellen Modus auf Wunsch jede einzelne App. Deutlich komfortabler ist der automatische Modus, in dem ausgewählte Apps jedes Mal nach einem bestimmten Zeitplan – vorzugsweise nachts – neu gesichert werden, wenn in der Zwischenzeit Daten dieser Apps verändert wurden.

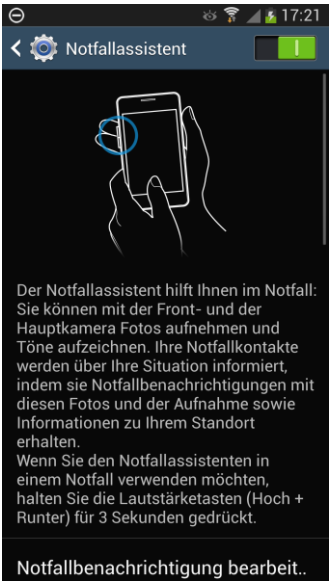
Ein komplettes Backup kann einige Zeit dauern. Lassen Sie das Smartphone während dieser Zeit am besten am Ladegerät hängen.

Titanium Backup bietet in der kostenlosen Version nur die Basisfunktionen. Die kostenpflichtige Version ermöglicht unter anderem mehrere Backups für jede App, Datensynchronisation mit Dropbox, Box oder Google Drive, Übertragung der Backups im ZIP-Format auf den PC. Dazu verwendet Titanium Backup einen eigenen Webserver. Normale Benutzer-Apps lassen sich in System-Apps konvertieren und umgekehrt, und einzelne Apps und Daten lassen sich aus Datensicherungen anderer Backupprogramme extrahieren.

Persönliche Sicherheit dank moderner Technik

Neben der technischen Sicherheit kann ein Smartphone, das man immer bei sich trägt, auch zur persönlichen Sicherheit in Notlagen behilflich sein.

Auf dem Samsung Galaxy S4 gibt es einen **Notfallassistenten** – eine Funktion, die man hoffentlich nie braucht, aber für den Notfall sicherheitshalber einmal einrichten sollte. Der Notfallassistent macht im Notfall Fotos mit der Front- und Hauptkamera, zeichnet Geräusche und Hilferufe auf und schickt diese mit einer vorher geschriebenen Nachricht per MMS an ausgewählte Personen. Das ersetzt keinen Notruf, kann aber helfen, wenn man selbst nicht in der Lage ist, den Notruf anzurufen.



1. Schalten Sie den Notfallassistent in den Einstellungen unter *Mein Gerät* ein. Hier müssen Sie bestätigen, dass Sie die Hinweise zur Verwendung gelesen haben.
2. Wählen Sie Personen aus, die im Notfall benachrichtigt werden sollen. Zum Empfang von MMS sind Handynummern erforderlich. Bei Kontakten aus dem Adressbuch muss eine Handynummer als Standardnummer gewählt sein.
3. Schalten Sie den Schalter *Notfallfotos senden* ein und schreiben Sie eine Nachricht, die im Notfall mit den Fotos verschickt werden soll.
4. Im Feld *Nachrichtenintervall* legen Sie fest, ob die Nachricht nur einmal oder wiederholt gesendet werden soll.

Im Notfall

... drücken Sie die beiden Lautstärketasten lauter und leiser gleichzeitig mindestens drei Sekunden, um die Aufzeichnung zu starten und danach die Nachricht automatisch zu senden. Das funktioniert auch, wenn der Bildschirm des Smartphones ausgeschaltet ist.

iKnow – das lohnende Portal für Self-Publisher

- Sie sind fit in Sachen Technik, PC, Smartphone oder Tablet?
- Sie würden gerne selbst eine Anleitung zu Ihrem Fahrrad-GPS oder Ihrer Lieblings-App schreiben, um anderen unterhaltsam und verständlich zu vermitteln, wie es funktioniert?
- Sie haben eine flotte Schreibe und verstehen es, das Wesentliche auf den Punkt zu bringen?

iKnow E-Books by DATA BECKER

Und Sie möchten damit Geld verdienen?

Dann kommen Sie zu uns. Wir publizieren keine Allerweltsliteratur zu Themen von A wie „Anstandsbesuche“ bis Z wie „Zucker macht glücklich“. Wir sind vielmehr die erste Adresse für E-Book-Anleitungen zu populärer Technik und Unterhaltungselektronik.
Sie profitieren von fairen Konditionen ohne Knebelverträge und einer eingeführten Marke.
Wenn unser aufstrebendes iKnow-Portal mit seinem technikaffinen Anleitungscharakter zu Ihnen passt, dann passen Sie auch zu uns!

Nutzen Sie die Chance, auf einem spezialisierten E-Book-Portal zu publizieren, und erfahren Sie mehr auf www.iknow.de unter Veröffentlichen Sie bei uns.

Oder fragen Sie einfach unverbindlich bei uns nach mit einer E-Mail an:
selfpublishing@databecker.de