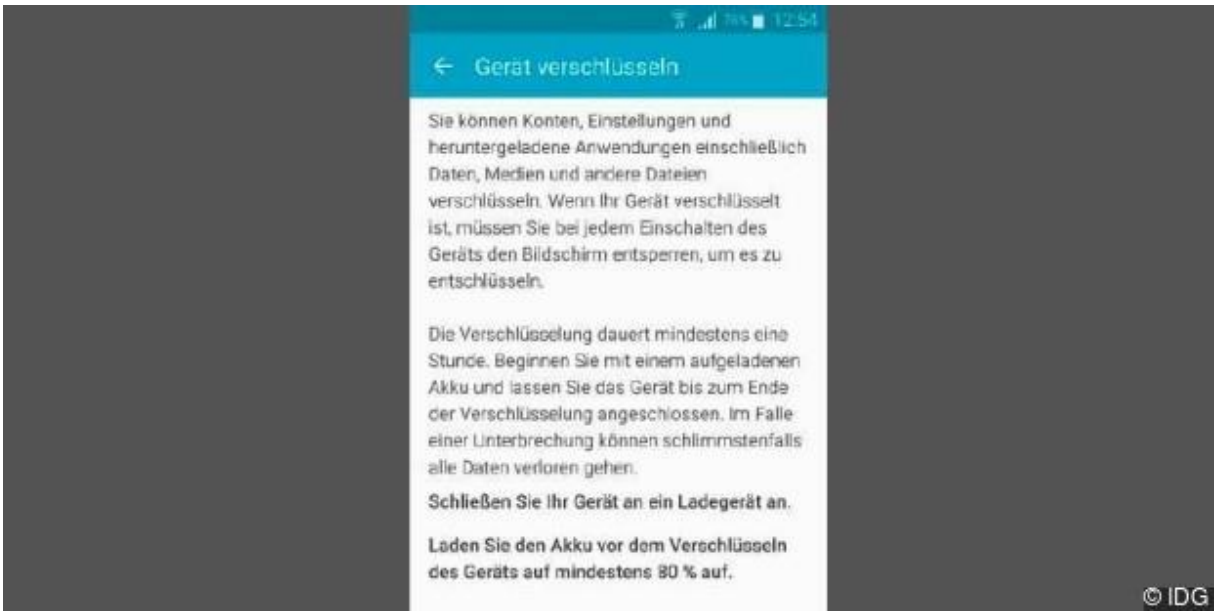
Android verschlüsseln – Anrufe_ Mails und Co absichern

Schützen Sie Ihre sensiblen Daten, damit diese nicht in falsche Hände geraden! Wir zeigen Ihnen, wie das am einfachsten geht und worauf Sie achten müssen.

In diesem Artikel verraten wir Ihnen, wie Sie endlich Ihr Android-Smartphone nutzen können, ohne sich um Ihre Daten, um Ihre private Kommunikation oder wegen Virenbefalls Sorgen machen zu müssen. So erklären wir Ihnen, wie Sie nicht nur Ihr komplettes Smartphone und einzelne Dateien, sondern auch Ihre gesamte Kommunikation wie Mails, Telefonate und Chats verschlüsseln können. Darüber hinaus verraten wir Ihnen, welche Regeln Sie befolgen sollten, um Ihr Smartphone vor Virenbefall zu schützen, und wie Sie anonym im Internet surfen.

Smartphone und alle Daten verschlüsseln

Auf Ihrem Smartphone liegen sensible Daten wie Mails, Kontakte, Fotos, Videos, App-Daten, Downloads oder Zugangsdaten für Google und soziale Netzwerke. Um zu verhindern, dass sie in falsche Hände gelangen, sollten Sie alle privaten Daten auf Ihrem Gerät schützen. Im Folgenden finden Sie detaillierte Anleitungen, mit denen Sie komplett alles auf Ihrem Smartphone oder auch nur einzelne Dateien verschlüsseln können.

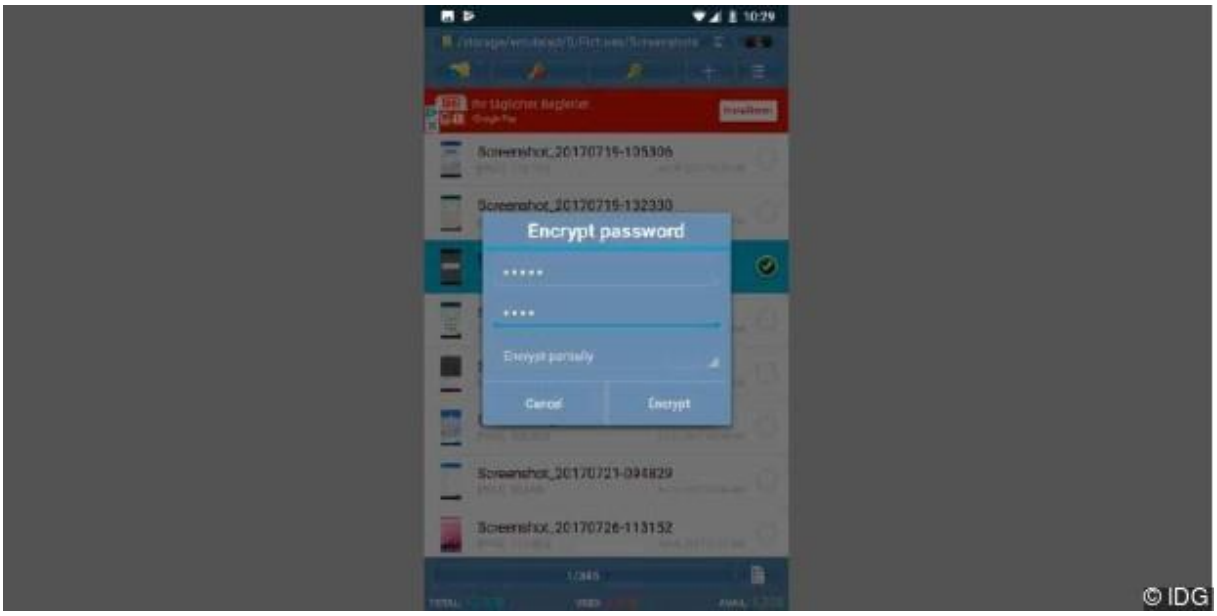


Vergrößern **Ältere Smartphones können Sie ganz einfach selbst im Nachhinein absichern.**

Smartphone: Viele aktuelle Android-Smartphones sind mittlerweile mit einer Verschlüsselung ab Werk ausgestattet. Allerdings verfügen gerade ältere Geräte noch nicht über dieses Sicherheitsfeature. Wenn Sie ein Smartphone besitzen, das mindestens mit dem Betriebssystem Android 3.0 ausgestattet ist, können Sie die Kodierung selbst nachträglich aktivieren. Öffnen Sie hierfür die Einstellungen auf Ihrem Gerät, und gehen Sie zum Punkt

„Sicherheit“. Hier finden Sie die Option „Telefon verschlüsseln“. Falls diese Option fehlt und Ihr Smartphone mit Android 5.0 oder einer höheren Version ausgestattet ist, können Sie davon ausgehen, dass der Hersteller das Gerät ebenfalls ab Werk verschlüsselt hat. Um die Verschlüsselung zu starten, muss der Akku mindestens zu 80 Prozent geladen sein. Beachten Sie außerdem, dass die Verschlüsselung ebenfalls recht viel Zeit in Anspruch nimmt. So kann der Vorgang durchaus mehrere Stunden dauern.

Bevor Sie Ihre Daten verschlüsseln, sollten Sie ein Backup erstellen, das Sie aber nicht im internen Speicher des Smartphones ablegen. Das erledigen Sie mit den Verwaltungsprogrammen der Hersteller selbst wie „Samsung Smart Switch“, oder Sie nutzen eine Drittanbieter-Software wie den „ My Phone Explorer “, der mit den meisten Smartphones kompatibel ist. Beachten Sie, dass der Verschlüsselungsvorgang bis zu eine Stunde dauern kann. Wenn Ihnen das zu lang ist, können Sie auch die Option „Schnelle Verschlüsselung“ wählen, bei der nur der auf dem Smartphone belegte Speicherplatz verschlüsselt wird. Außerdem verlangt der Androide die Eingabe einer numerischen PIN oder eines Passworts, damit Sie die Daten zum einen schützen und zum anderen auch wieder entschlüsseln können. Bei jeder Smartphone-Aktivierung nach der Verschlüsselung müssen Sie das Kennwort eingeben. Falls Sie die Verschlüsselung aufheben wollen, weil Sie etwa Performance-Probleme feststellen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Dabei werden sämtliche auf dem Handy befindlichen Daten gelöscht. Deshalb sollten Sie zuvor auf keinen Fall das Backup vergessen!

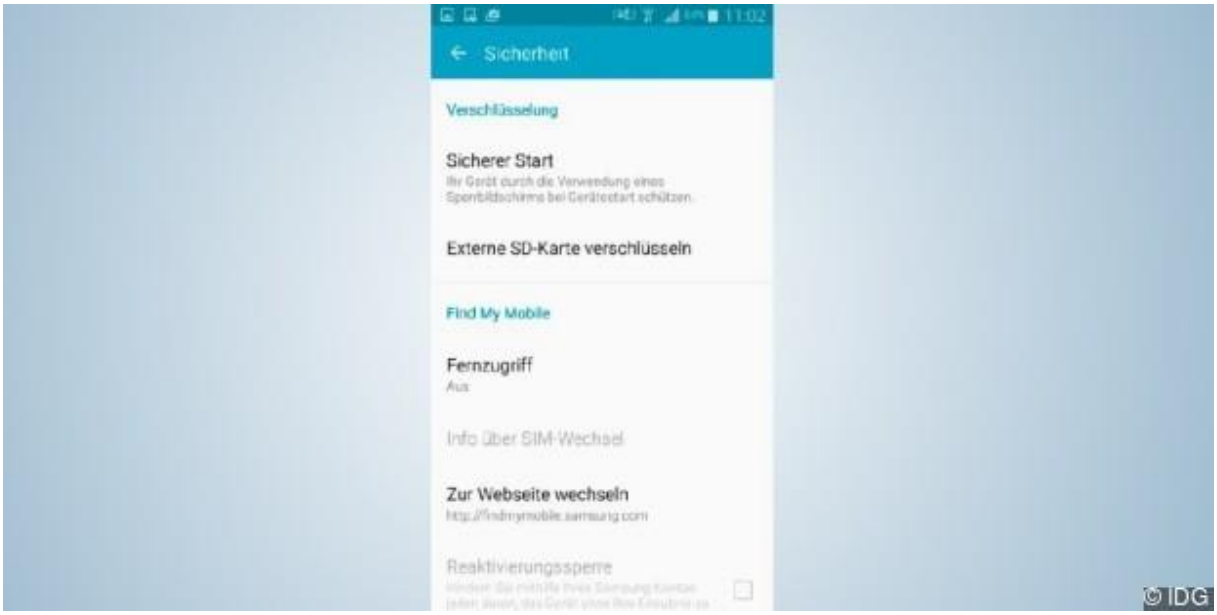


Vergrößern Mit File Protector lassen sich einzelne Dateien auf Ihrem Smartphone verschlüsseln.

Einzelne Dateien verschlüsseln: Wollen Sie nicht Ihr komplettes Smartphone, sondern nur einzelne Dateien darauf verschlüsseln, dann können Sie unter anderem die englischsprachige App File Protector Full Version verwenden. Sie ist im Grunde wie ein Dateimanager aufgebaut. Sie haben also Zugriff auf sämtliche Daten, die sich in Ihrem Telefonspeicher befinden. Wählen Sie die gewünschte Datei aus, indem Sie auf den kleinen Kreis rechts neben dem Dateinamen tippen, und berühren Sie anschließend das rote Schlosssymbol in der Menüleiste am oberen Bildschirmrand. Die App fordert Sie nun dazu auf, ein Passwort festzulegen und dieses anschließend nochmals einzugeben. Bestätigen Sie die Aktion anschließend über die Schaltfläche „Encrypt“. Die Anwendung verschlüsselt nun die ausgewählte Datei. Falls es sich bei der Datei um ein Bild handelt, erscheint nun kein

Vorschaubild in der Anzeige, sondern nur noch ein Icon mit einem roten Schlosssymbol. Um die Datei wieder öffnen zu können, wählen Sie wieder die entsprechende Datei aus und tippen dann oben auf das grüne Schlosssymbol. Geben Sie das vorher festgelegte Passwort ein, und entschlüsseln Sie die Datei über „Decrypt“. Neben einzelnen Dateien können Sie auch mehrere Daten oder gleich ganze Ordner kodieren.

Micro-SD mit Samsung-Geräten verschlüsseln



Vergrößern Auch die Micro-SD-Speicherkarte lässt sich verschlüsseln. Bei Samsung finden Sie diese Option in den Einstellungen unter dem Punkt „Allgemein –> Sicherheit“.

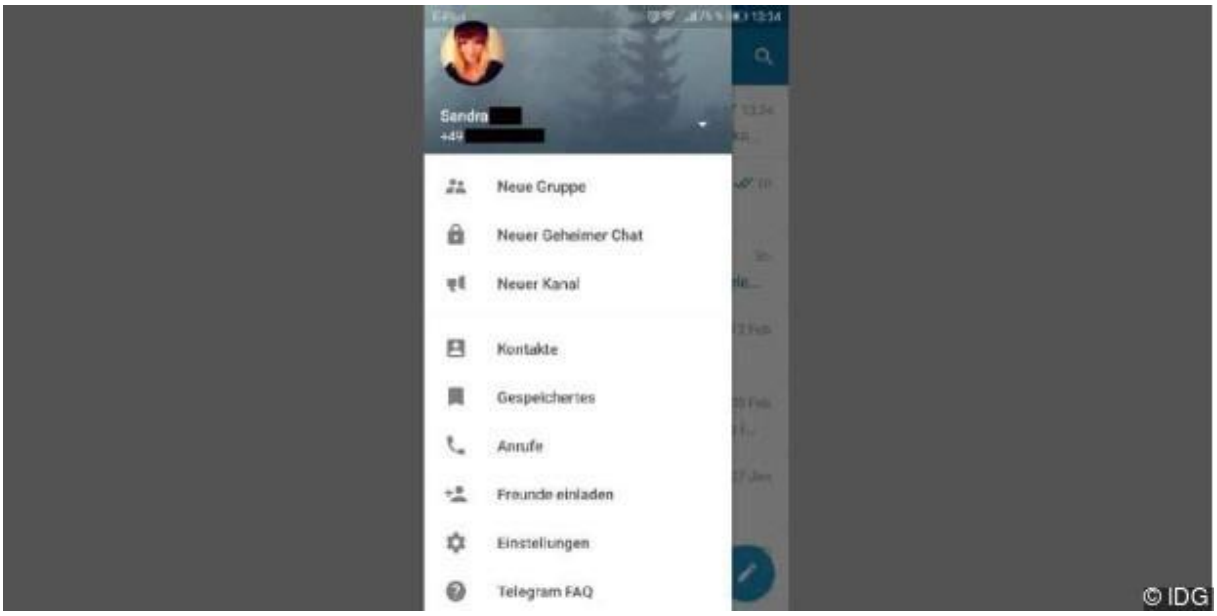
Wer seine Daten besonders sicher auf dem Smartphone verwahren möchte, der kann neben der Komplettverschlüsselung auch die Inhalte auf der Micro-SD-Karte schützen lassen. Besonders gut ist das bei Samsung-Geräten möglich, denn sie bieten die Verschlüsselungsoption in den Einstellungen unter „Allgemein –> Sicherheit –> Externe SD-Karte verschlüsseln“ an.

Um die Funktion zu nutzen, muss der Sperrbildschirm mit einem Passwort geschützt werden – andere Methoden wie eine PIN oder die Mustersperre lassen sich hier nicht nutzen. Das Passwort muss wiederum aus mindestens sechs Buchstaben und einer Zahl bestehen. Außerdem können Sie, bevor Sie den Vorgang starten, wählen, ob auch Multimediadateien verschlüsselt werden sollen. Nun folgen diverse Bestätigungen und eine Passworteingabe, bis die Verschlüsselung startet. Ist sie abgeschlossen, müssen Sie für den Zugriff auf die Micro-SD-Karte jedes Mal das zuvor festgelegte Passwort eingeben. Aber: In den Einstellungen lässt sich der Schutz auch wieder deaktivieren.

Der Nachteil: Da Lockscreen-Passwort und Verschlüsselungspasswort übereinstimmen, schützt die Verschlüsselung vor allem dann, wenn sich die Karte außerhalb des Smartphones befindet, also wenn ein potenzieller Datendieb sich per Kartenleser Zugriff verschaffen will.

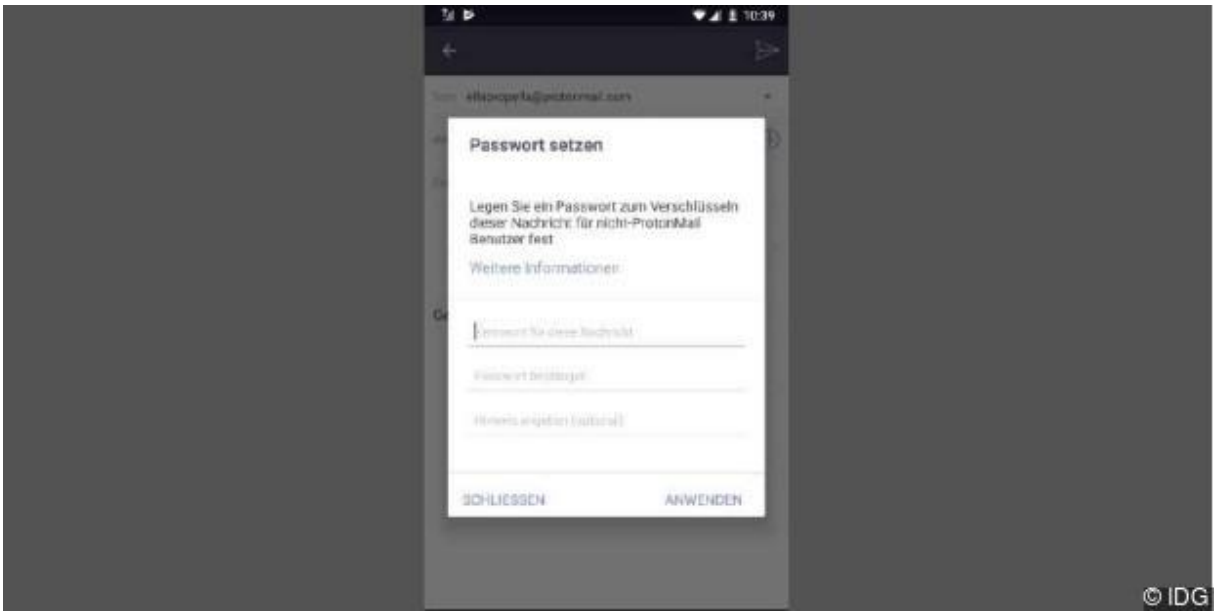
Verschlüsselt kommunizieren

Damit Ihre privaten Unterhaltungen auch privat bleiben, sollten Sie verschlüsselt mit Ihrem Smartphone kommunizieren. Hierfür bietet der Google Play Store verschlüsselte und kostenlose Chatprogramme, Mailclients und sogar Telefon-Apps, die das Risiko für Angriffe minimieren.



Vergrößern Um mit Telegram verschlüsselt zu chatten, müssen Sie vorab die Option „Gemeiner Chat“ aktivieren.

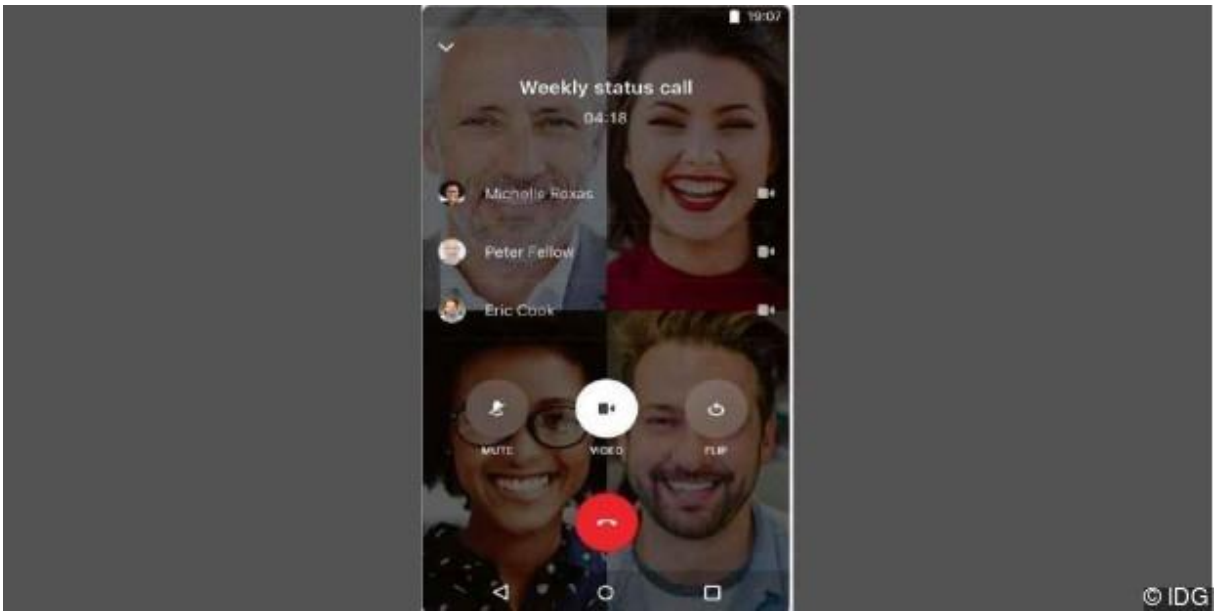
Verschlüsselt chatten: Der Verschlüsselungsmessenger Telegram verschlüsselt den Chat Ende-zu-Ende, der Gesprächsverlauf wird dabei nicht auf dem Server gespeichert – allerdings nur, wenn Sie die Option „Sicherer Chat“ gewählt haben. Hier löscht das Programm den Chatverlauf automatisch von beiden Geräten nach einem von Ihnen festgelegten Verfallsdatum. Für den Zugang zur App sind sogar zwei Beschränkungen möglich. So lässt sich einerseits ein vierstelliger PIN-Code zum Entsperren der Chats einrichten und andererseits ein zusätzliches Passwort festlegen. Damit können Sie sicher sein, dass Unbefugte, die Ihr Smartphone in die Hände bekommen, nicht auf Ihre privaten Unterhaltungen zugreifen können. Der Quellcode von Telegram ist öffentlich zugänglich. Die Sicherheit der Verschlüsselung lässt sich also jederzeit von Experten überprüfen.



Vergrößern Auch an Kontakte, die nicht „Proton Mail“ nutzen, lassen sich verschlüsselte Nachrichten versenden.

Verschlüsselte Mails unter Android versenden: Prinzipiell kann jeder die E-Mails anderer Personen im Web abfangen. Das große Problem: Die Mails werden im Klartext über eine weitestgehend offene Leitung übertragen. Eine Alternative ist der Dienst Proton Mail . Der Mailclient nimmt Ihnen die Sorge um die Sicherheit Ihrer elektronischen Post und macht Nachrichten per Ende-zu-Ende-Verschlüsselung für Unbefugte unantastbar. Um eine verschlüsselte Mail zu senden, installieren Sie die App auf Ihrem Smartphone und erstellen sich ein neues „Proton Mail“-Konto. Legen Sie ein sicheres Passwort fest, und wiederholen Sie die Eingabe anschließend erneut. In puncto Verschlüsselung können Sie zwischen den Optionen „Hohe Sicherheit (2048 bit)“ sowie „Extreme Sicherheit (4096 bit)“ wählen. Schließen Sie die Einrichtung ab, und tippen Sie oben rechts auf das Stiftsymbol, um eine neue Mail zu erstellen. Nun haben Sie zwei Möglichkeiten. Um eine Nachricht an einen anderen „Proton Mail“-User zu schicken, brauchen Sie keine weiteren Schritte für die Verschlüsselung einzuleiten. Sollten Sie eine codierte Nachricht an einen Kontakt ohne „Proton Mail“-Konto schicken wollen, tippen Sie innerhalb des E-Mail-Formulars auf das kleine Schloss. Hier können Sie nun ein Passwort sowie einen optionalen Hinweis zur Entschlüsselung der Nachricht festlegen. Bestätigen Sie anschließend die Eingabe über „Anwenden“. Ihr Gesprächspartner muss das Passwort dann eingeben, um Ihre Nachricht lesen zu können.

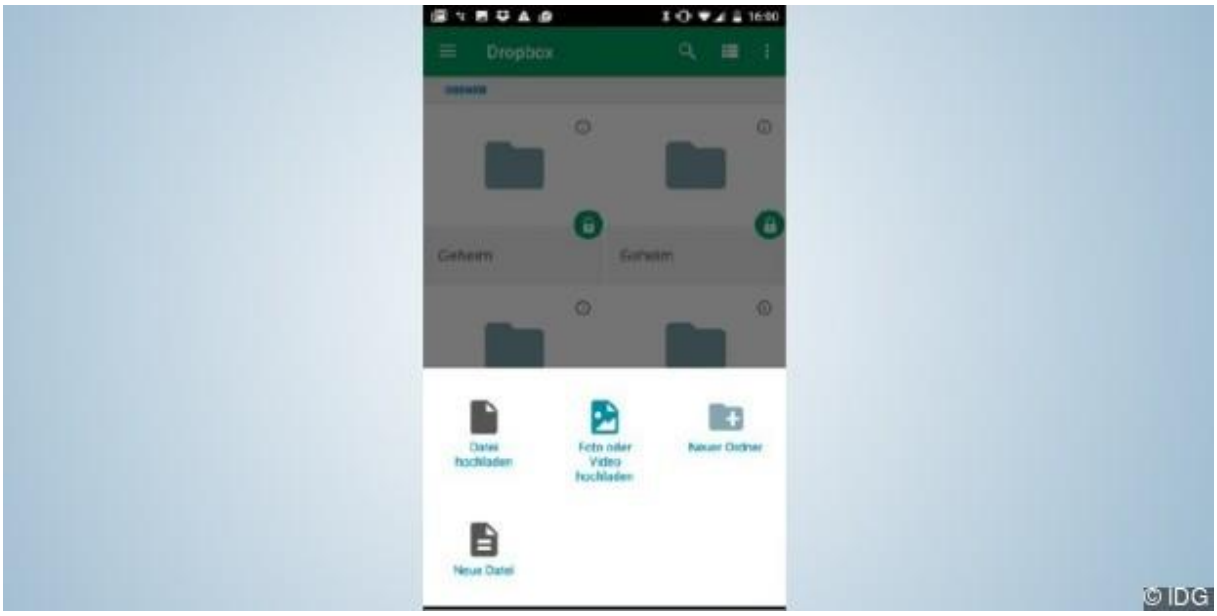
Tipp: Android-Frühjahrsputz - schnell wie am ersten Tag



Vergrößern Der verschlüsselte Messenger „Wire“ ermöglicht codierte Sprach- und Videoanrufe.

Verschlüsselt telefonieren: Sprach- und Videoanrufe lassen sich ganz einfach mit der App Wire verschlüsseln. Allerdings telefonieren Sie hier nicht über das Mobilfunknetz, sondern über VoIP (Voice over IP), sprich: das Internet. Das Chatprogramm bietet eine Ende-zu-Ende-Verschlüsselung für Video- und Sprachtelefonie sowie für das Versenden von Textnachrichten, Sprachnachrichten, GIFs, Bilder und Zeichnungen. Die Verschlüsselung beruht dabei auf einem Open-Source-Code. Praktisch: Sie können den Dienst zeitgleich auf mehreren Devices zu nutzen. Die Macher des Messengers (die Wire Swiss GmbH) sitzen in der Schweiz, die Server, über welche die Nachrichten versendet werden, befinden sich in Deutschland und Irland. Installieren Sie hierfür die kostenlose App auf Ihrem Smartphone, und erstellen Sie mithilfe Ihrer Telefonnummer oder Ihres Mailkontos ein neues Nutzerkonto. Tippen Sie in der Kontaktliste anschließend auf die Person, die Sie anrufen wollen. In dem sich nun öffnenden Chatfenster können Sie wahlweise Textnachrichten schreiben sowie Video- oder Sprachanrufe tätigen. Letztere Optionen finden Sie oben rechts. Berühren Sie hier entweder das kleine Kamera- oder das Telefonhörer-Symbol.

Dateien in der Cloud verschlüsseln



Vergrößern Laden Sie einzelne oder mehrere Dateien in den vorher erstellten verschlüsselten Ordner hoch, um sie vor fremdem Zugriff zu schützen.

Damit auch die Daten in Ihrer Dropbox, Ihrem Google Drive oder Ihrem One-Drive-Speicher vor fremdem Zugriff geschützt sind, hilft Ihnen die App „ Boxcryptor “. Mit ihrer Hilfe können Sie ganz einfach alle Dateien in der Cloud verschlüsseln. Die App ersetzt anschließend die Dropbox-App auf Ihrem Smartphone.

Um Ihre online gespeicherten Daten zu verschlüsseln, installieren Sie die kostenlose Version auf Ihrem Androiden und richten anschließend ein neues Konto beim Anbieter ein. Danach tippen Sie unten rechts auf das kleine Pluszeichen. Wählen Sie nun den gewünschten Cloudspeicher-Anbieter Ihres Vertrauens aus, und loggen Sie sich mit den jeweiligen Zugangsdaten ein. Genehmigen Sie den Zugriff von der App „Boxcryptor“ auf die in der Cloud gespeicherten Dateien. Um nun einen neuen verschlüsselten Ordner zu erstellen, tippen Sie unten rechts auf das Plussymbol und entscheiden sich für die Option „Neuer Ordner“. Geben Sie einen Namen ein, und bestätigen Sie den Vorgang mit „OK“. Berühren Sie anschließend den Ordner und dann erneut das Plussymbol. Nun lassen sich Dateien zum Ordner hinzufügen oder neue Dateien hochladen.

Um den Zugriff auf die App zu beschränken, öffnen Sie durch ein Wischen vom linken Bildschirmrand zur Mitte das Anwendungsmenü: In den Einstellungen finden Sie unter „Account“ die Option „Passwort speichern“. Deaktivieren Sie nun den Schieberegler, damit zum Starten der App immer die Eingabe des Passworts erforderlich ist. Unter „Allgemein“ können Sie zusätzlich noch die Eingabe einer vierstelligen PIN-Nummer aktivieren.

Auch interessant: Geheime Befehle für Android ausprobiert

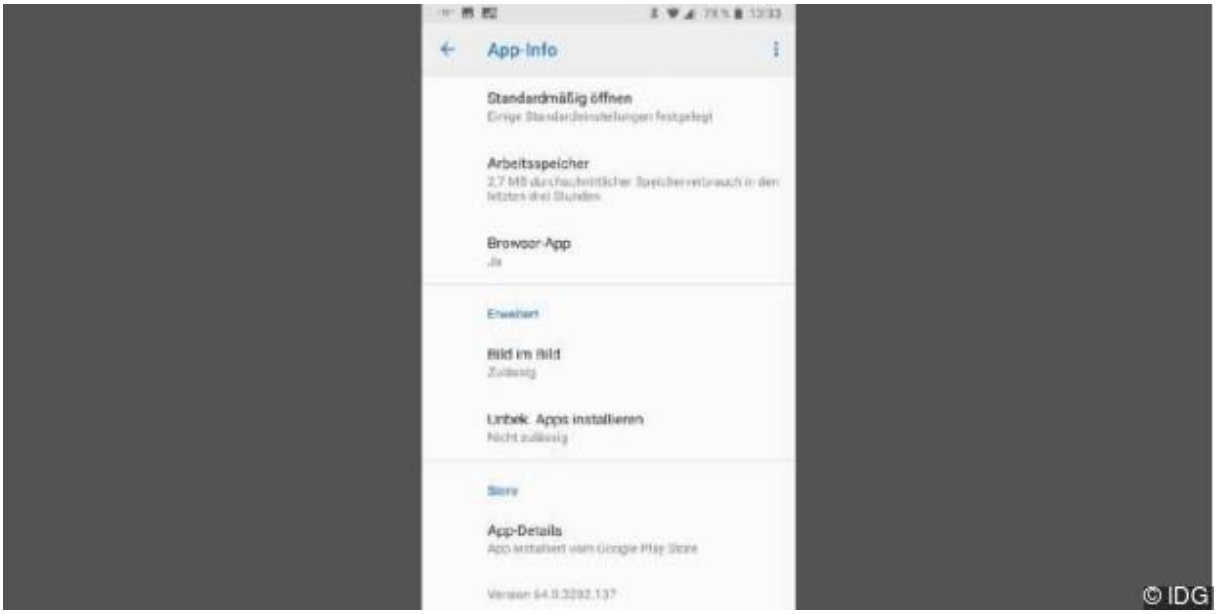
Virus-Vorsorge

Eine verseuchte App aus dubioser Quelle, ein Pornoplayer mit angeblich kostenlosen Inhalten, ein Spiel, das außergewöhnlich viele Rechte einfordert – die Möglichkeiten, sich einen Virus auf dem Smartphone einzuhandeln, sind vielfältig. Aktuell müssen Sie immer noch selbst tätig werden, damit ein Schädling Zugriff auf Ihr Smartphone erhält. Seien Sie

also grundsätzlich vorsichtig, wenn Sie auf Links klicken, Dateien herunterladen und öffnen oder einer App Berechtigungen erteilen. Zusammenfassend können wir Ihnen sieben goldene Regeln ans Herz legen:

1. Laden Sie nur im Ausnahmefall Apps aus anderen App-Stores als dem Google Play Store herunter. Deaktivieren Sie daher am besten die entsprechende Option in den Einstellungen unter „Sicherheit –> Unbekannte Quellen“. So gelangen keine Apps aus Drittanbieter-Stores mit ungewolltem Gepäck auf Ihr Mobilgerät.

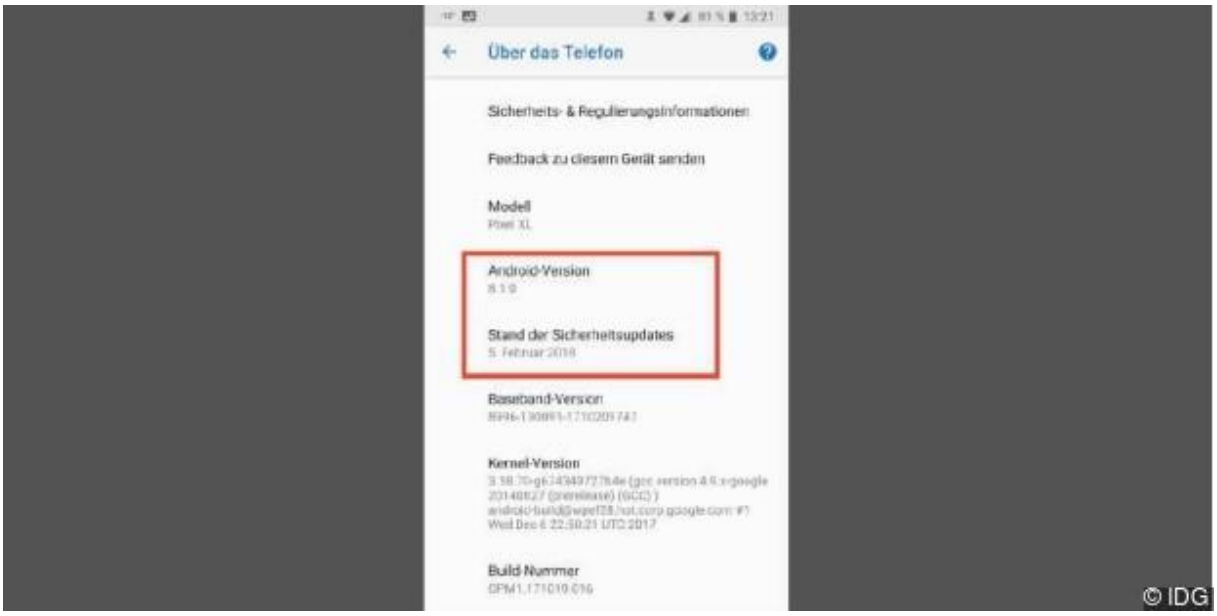
2. Doch Achtung: Diese Option ist nur bis Android 7 zu finden. Ab Android 8 können Anwender jeder App eine Installationsberechtigung erteilen.
3. Zeigen Sie ein gesundes Misstrauen gegenüber APK-Dateien. Es wird schon seinen Grund haben, dass die dazugehörige App (noch) nicht offiziell erhältlich ist. Beispielsweise haben Hacker vor dem offiziellen Release von Pokémon Go virenverseuchte APK-Dateien des Spiels in Umlauf gebracht.



Vergrößern Ab Android 8 gibt es keine pauschale Bestimmung für Dateien aus unbekannten Quellen mehr.

4. Klicken Sie nicht unbedacht auf Links in Mails, deren Absender Sie nicht kennen. Eventuell steckt ein Download dahinter, der automatisch startet und Ihnen eine korrumpierte App aufs Smartphone lädt. Was für Mails am PC gilt, gilt auch für Mails auf dem Mobilgerät!

5. Glauben Sie keinen Angeboten, die zu gut erscheinen, um wahr zu sein. Viele Schädlinge sind etwa in Pornoplayern versteckt. Aber: Niemand schenkt Ihnen etwas im Internet, vor allem keine Pornoangebote! Im Zweifelsfall bezahlen Sie die angeblichen Gratisinhalte mit Ihren Daten oder gar dem Zugriff auf Ihr Smartphone.



Vergrößern Achten Sie darauf, dass das Betriebssystem und das Sicherheitsupdate möglichst aktuell sind.

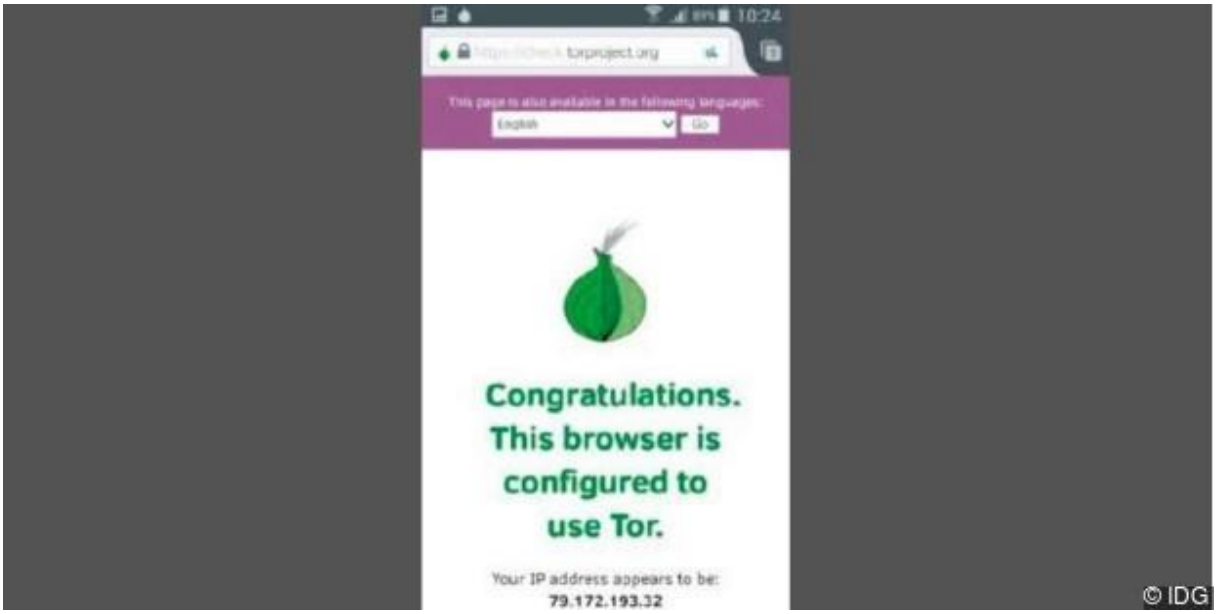
6. Software-Aktualisierungen, egal ob des Betriebssystems oder einer Applikation, sind wichtig. Denn mit jedem Update steigt die Stabilität der Anwendung, und offene Sicherheitslücken werden geschlossen. Normalerweise bekommen Sie eine Pushnachricht, sobald ein Update für Ihr Smartphone-Modell verfügbar ist. Möchten Sie jedoch auf Nummer sicher gehen, können Sie auch selbst regelmäßig überprüfen, ob eine neue Softwareversion für Ihr Smartphone verfügbar ist. Dazu gehen Sie in den Einstellungen auf „System“, „Geräteinformationen“ oder ähnlich und tippen auf „Jetzt auf Updates prüfen“ – die genaue Bezeichnung variiert je nach Hersteller. Ihr Smartphone sagt Ihnen dann, ob die Software bereits auf dem neuesten Stand ist oder ob es tatsächlich eine neue Version zum Downloaden gibt. Auch App-Entwickler aktualisieren regelmäßig ihre Anwendungen, um neue Funktionen zu integrieren. Es ist hier also auch wichtig, dass Sie diese Updates durchführen. Falls Sie die automatische Updatefunktion aktiviert haben, sollten Sie zudem dafür sorgen, dass die Updates nur per WLAN heruntergeladen werden. Sonst kann dies auf Kosten Ihres Datenvolumens gehen.

7. Nutzen Sie eine Sicherheitssuite auf Ihrem Smartphone! Bekannte Anbieter sind etwa Avast, AVG, Avira, Bitdefender, G Data, Kaspersky und Symantec. Die zentrale Funktion einer Sicherheitssuite ist der Schutz vor Malware und Viren: Zum einen wird das Dateisystem Ihres Smartphones oder Tablets regelmäßig auf bekannte Malware gescannt, zum anderen agiert bei den meisten Lösungen ein Echtzeitscanner im Hintergrund, der neue Dateien scannt, klassifiziert und gegebenenfalls direkt löscht. Basis für die Untersuchung ist eine Datenbank, in welcher die Signaturen der Viren gespeichert sind. Wird ein solcher Virus erkannt, entfernt ihn die Software eigenständig oder lässt gleich gar keine Installation zu.

Anonym im Internet surfen

Beim Surfen im Internet hinterlassen Sie vielerlei Spuren: So speichern etwa Webdienste Informationen über Sie in Cookies. Je mehr Sie den Dienst eines Anbieters verwenden, desto exakter wird sein Bild von Ihnen. Ihr Kaufverhalten oder auch Ihre Produktrecherche wird stets mitgeschnitten und analysiert. So erhalten Sie Kaufvorschläge in Form von

Werbebannern für Produkte, die Sie auf einer anderen Seite zuvor gesucht haben. Auch beim sogenannten Dynamic Pricing kann die Datensammelwut der Webdienste nachteilig für Sie sein. So passt sich der Produktpreis der Nachfrage an. Dies kann dazu führen, dass sie am Ende einen höheren Preis bezahlen. Wenn Sie lediglich auf dem Smartphone keine Spuren hinterlassen wollen, bieten sich die Private-Browsing-Funktionen aller gängigen Internetbrowser wie beispielsweise Chrome und Firefox an. Hier ist anschließend auf dem Gerät nicht mehr nachvollziehbar, auf welchen Webseiten Sie gesurft haben. Die Vorgehensweise unterscheidet sich lediglich minimal bei den verschiedenen beliebten Browsern für Android. Bei Chrome tippen Sie oben rechts in der Suchleiste auf die drei Punkte und anschließend auf die Option „Neuer Inkognito-Tab“. Um mit Firefox anonym surfen zu können, tippen Sie zuerst rechts oben neben der Suchleiste auf die drei Punkte und berühren anschließend die Option „Neuer privater Tab“.



Vergrößern Neben „Orfox“ hat der Anbieter Guardianproject noch weitere Applikationen in petto.

Ein weiterer Verräter ist Ihre IP-Adresse. Sie wird automatisch beim Surfen genannt, damit der Server mit der Webseite weiß, wohin er seine Daten schicken soll. Das ist notwendig, aber über die IP-Adresse kann jeder zumindest Ihren ungefähren Standort herausfinden. Hier schafft der Anonymsierungsdienst „Tor“ Abhilfe: „TOR“ steht für „The Onion Router“ – Verschlüsselung nach dem Zwiebelschalenprinzip. Um seine Herkunft zu verschleiern, schickt Tor jedes Datenpaket über verschiedene, zufällig ausgewählte Rechner (Nodes), bevor es dann über einen Endknoten (Exit Node) ins offene Internet übergeben wird. Ihre IP-Spur wird also über verschiedene Anonymisierungsserver umgeleitet. Damit die Daten auf keinem der beteiligten Tor-Rechner mitgelesen werden können, sind sie verschlüsselt.

Den Dienst nutzen Sie mit der kostenlosen Proxy-App Orbot: Vermittlung mit Tor mit dem Security-Browser „Orfox“. Installieren Sie beide Anwendungen auf Ihrem Smartphone. Öffnen Sie dann Orbot, und tippen Sie in der Mitte auf den Schriftzug „Start“ auf dem Zwiebelsymbol. Warten Sie anschließend, bis das Symbol mit einem grünen Hintergrund hinterlegt ist. Tippen Sie dann weiter unten auf das Logo des „Orfox“-Browsers. Sie wechseln dann automatisch in die App und erhalten die Meldung „Congratulations. This browser is configured to use Tor“. Anschließend können sie lossurfen.

Passwort-Safes verwenden

Ein ideales Passwort besteht aus einer möglichst langen, zusammenhanglosen Kombination von Buchstaben, Ziffern und Sonderzeichen und lässt sich unmöglich erraten. Selbst ein leistungsstarker Computer würde Jahre benötigen, um alle theoretisch denkbaren Zeichenfolgen auszuprobieren. Damit selbst dann nicht allzu viel passieren kann, empfehlen Experten, ein und dasselbe Passwort niemals für den Zugang zu mehr als einem Dienst zu verwenden. Damit Sie hier nicht den Überblick verlieren, sollten Sie einen sogenannten Passwort-Safe verwenden, der Ihre Passwörter geschützt zentral und verschlüsselt speichert.

Eine gute Wahl ist hier der „ Password Safe und Repository “. Die App speichert Daten mit sehr sicherer AES-256-Verschlüsselung und hilft auch beim Erstellen guter Passwörter: Die beste Verschlüsselung ist nämlich wenig wert, wenn das Passwort kurz oder zu simpel ist. Hier können Sie die Länge festlegen und bestimmen, ob das Passwort Zahlen, Sonderzeichen, Klein- oder Großbuchstaben enthalten soll. Um eine neue Datenbank mit Ihren Passwörtern anzulegen, öffnen Sie die App, geben einen Namen für Ihre Datenbank ein und wählen die Option „Passwort“. Geben Sie nun ein neues Passwort ein, und wiederholen Sie es zur Bestätigung anschließend ein weiteres Mal. Öffnen Sie die danach neu erstellte Datenbank. Nun können Sie über das Plussymbol am unteren Bildschirmrand ein neues Passwort für unterschiedliche Einsatzszenarien generieren und abspeichern. Für die einzelnen Datenbänke können Sie ein eigenes Ablaufdatum bestimmen: Am festgelegten Tag entfernt die App dann gnadenlos alle im Datensatz abgelegten Zugangsdaten. Aus Sicherheitsgründen sind Screenshots der App nicht möglich.