Handy sicher machen und vor Angreifern schützen: So wird’s gemacht

Artem Sandler 21. Februar 2019

Es ist fest in den Köpfen der meisten Nutzer verankert: Ein Computer ist angreifbar. Er muss mit einer Antivirus-Software geschützt werden und Links in unbekannten E-Mails sind gefährlich. Anders sieht es hingegen beim Smartphone aus. Obwohl moderne Handys über einen Prozessor, einen Arbeitsspeicher, eine Festplatte, eine Internet-Anbindung und sämtliche anderen Eigenschaften eines handelsüblichen Desktop-PCs verfügen, wird der kleine Computer weiterhin oftmals lediglich als modernes Mobiltelefon angesehen und auch so behandelt. Darunter leidet vor allem die digitale Sicherheit– und das obgleich Smartphones heutzutage durchaus sogar mehr sensible Daten preisgeben können, als ihr stationäres Gegenstück, der heimische Rechner.

Kontaktdaten, Passwörter, gespeicherte Inhalte, Zugangsdaten zum Online-Banking und Standortdaten. Diese und viele weitere Informationen können Spionage-Apps auf dem Smartphone auslesen und an Dritte weitergeben. Sorgen scheint dies allerdings nur einem Bruchteil der Nutzer zu bereiten. Das legt zumindest eine Ende 2018 veröffentlichte repräsentative Umfrage des Digitalverbands Bitkom nahe. Demnach verwenden nur 40 Prozent der Befragten ein Virenschutzprogramm auf dem Handy. Und das, obwohl jeder dritte Smartphone-Nutzer ab 16 Jahren (35 Prozent) innerhalb eines Zeitraums von zwölf Monaten Opfer von Malware wurde, wie dieselbe Statistik zeigt.

Malware-Risiko minimieren und Sicherheitslücken schließen

Der Durchschnitt der mit einem Virus infizierten Geräte ist besorgniserregend. Dennoch gibt es auch gute Neuigkeiten, denn das

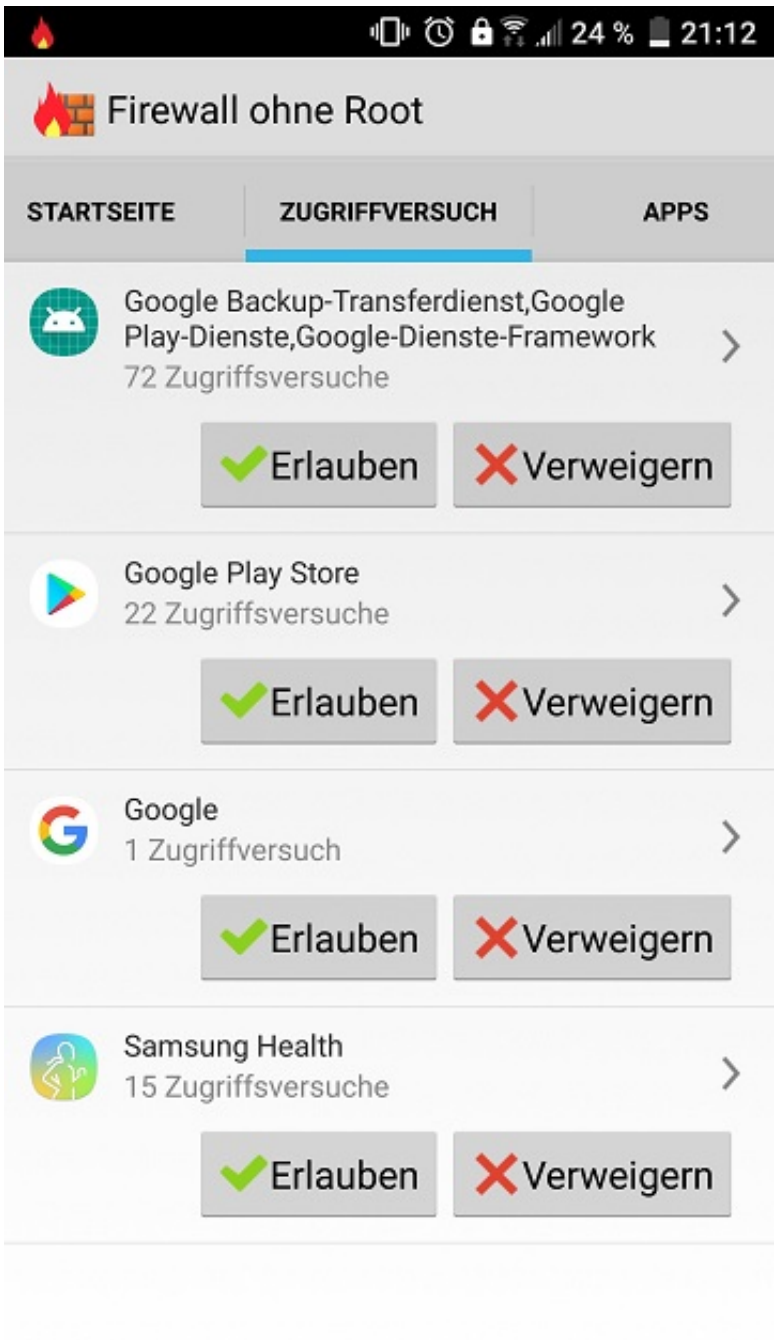
Ergebnis der Statistik kann ohne großen Aufwand deutlich verbessert werden. Was genau hierfür getan werden muss und worauf Nutzer allgemein achten sollten, um die Sicherheit ihres Smartphones zu erhöhen, zeigt der folgende Ratgeber.

Schutz vor Schadsoftware, digitalem Datenklau und Spionage

Tipp 1: Virenschutz: Antivirus- und Firewall-Software

Eine der effektivsten und zugleich einfachsten Möglichkeiten das eigene Smartphone vor Viren zu schützen, stellt eine Antivirus-App dar. Diese bieten beispielsweise einen Virenscanner, mit dem Dateien und Anwendungen auf dem Handy durchleuchtet und auf Schadsoftware überprüft werden. Der Virenscanner gehört zur Grundausstattung und ist somit bei sämtlicher Antivirus-Software vorhanden. Wer zudem über das nötige Kleingeld verfügt, kann auch eine kostenpflichtige Antiviren-Software mit integriertem Echtzeitschutz kaufen. Dieser erkennt Viren wie Spionage-Apps in Echtzeit und leitet sofortige Gegenmaßnahmen ein.

Eine weitere Sicherheits-Funktion, die in wenigen Sekunden als App auf dem Smartphone landen kann, ist die Firewall. Sie überwacht die Netzwerkaktivitäten aller Anwendungen und kann eine Verbindung bei Bedarf auch unterbinden. Der Nutzer erhält dabei die Kontrolle über den Datenfluss seines Smartphones. Dabei darf man allerdings nicht vergessen, dass eine solche Firewall zunächst manuell Eingaben erfordert. Ansonsten blockiert diese unter Umständen sämtliche vorhandenen Anwendungen – unabhängig davon ob Spionage-Apps, Schadprogramme oder schlicht der WhatsApp-Messenger.



Tipp 2: Sicherheit in öffentlichen WLAN-Netzwerken

Egal ob im Café, im Einkaufzentrum oder im Hotel – öffentliche WLAN-Netzwerke sind bequem, oftmals kostenlos und helfen dabei, das im Tarif enthaltene Datenvolumen zu schonen. Das Problem daran: Man ist anfällig für Cyberkriminelle, die den eigenen Datenverkehr ausspionieren können. Online-Banking in öffentlichen Netzen ist darum ein absolutes Tabu. Auch Datenverbindungen, die nicht per HTTPS-Zertifikat (erkennbar an der URL) geschützt sind, sollten möglichst gemieden werden. Wer sich zusätzlich absichern will, sollte zudem auf ein Virtual Private Network (VPN) zurückgreifen. Diese leiten die eigene Verbindung ins Netz über einen VPN-

Server, verändern dabei die IP-Adresse und erhöht so die Anonymität im weltweiten Datennetz.

Zusätzlich werden die übertragenen Informationen – abhängig vom VPN-Anbieter – verschlüsselt. Das erschwert die Arbeit für ungebetene Zuschauer ungemein. Nutzer müssen hier allerdings darauf achten, welchen VPN-Anbieter sie wählen. Denn die angebotenen Dienstleistungen und das Schutzniveau unterscheiden sich teilweise sehr stark voneinander. Die Meisten kostenfreien VPNs bieten beispielsweise weniger Schutz beziehungsweise speichern einige Daten sogar selbst.

Tipp 3: Regelmäßige Sicherheits-Updates durchführen

Sowohl bei Apples iPhones als auch bei Android-Geräten verteilen Hersteller in unregelmäßigen Abständen sogenannte Sicherheits-Updates. Diese schließen unterschiedliche Sicherheitslücken und verbessern den Virenschutz. Dabei existieren jedoch größere Unterschiede, die abhängig vom gewählten Betriebssystem und Hersteller auftreten. Während Apple seine iPhones regelmäßig und über einen langen Zeitraum mit Sicherheitsaktualisierungen versorgt, sieht es bei Android-Smartphones gänzlich anders aus. Zwar veröffentlicht das Unternehmen hinter Android, Alphabet beziehungsweise Google, monatliche Sicherheitspatches. Diese müssen allerdings zunächst von jedem Hersteller an die Nutzeroberfläche des betreffenden Modells angepasst werden. Das kostet seinerseits sowohl Zeit als auch Geld, sodass günstigere Geräte unbekannter Hersteller nur sehr selten regelmäßige Updates erhalten. Bei etablierten Herstellern von Android-Smartphones wie Huawei oder Samsung sieht die Sache besser aus. Doch auch hier werden die Sicherheitsaktualisierungen meist nach zwei bis spätestens drei Jahren eingestellt. In dieser Kategorie haben iPhone-Nutzer klar die Nase vorne.

Weiterhin sollten Nutzer beim Kauf – ob gebraucht oder im Handel – darauf achten, wann das jeweilige Smartphone auf dem Markt erschienen ist. Denn der meist zweijährige Update-Zeitraum beginnt nicht mit dem Kauf des Handys, sondern mit dessen Veröffentlichung. Eine klare Regel existier hier allerdings natürlich nicht – zumindest noch nicht. Aktuell beabsichtigt die EU eine Regulierung einzuführen, die Hersteller künftig per Gesetz dazu verpflichtet, Aktualisierungen für ihre elektronischen Produkte zu verbreiten.

Tipp 4: Keine Anwendungen aus unbekannten Quellen zulassen

Ein weiterer Punkt, der vor allem Android-Nutzer betrifft, ist das Installieren von Apps aus unbekannten Quellen. Dabei wird eine Anwendungs-APK (Android Package) schlicht aus dem Internet (beispielsweise mithilfe eines Browsers) heruntergeladen und manuell auf dem Smartphone installiert. Auf

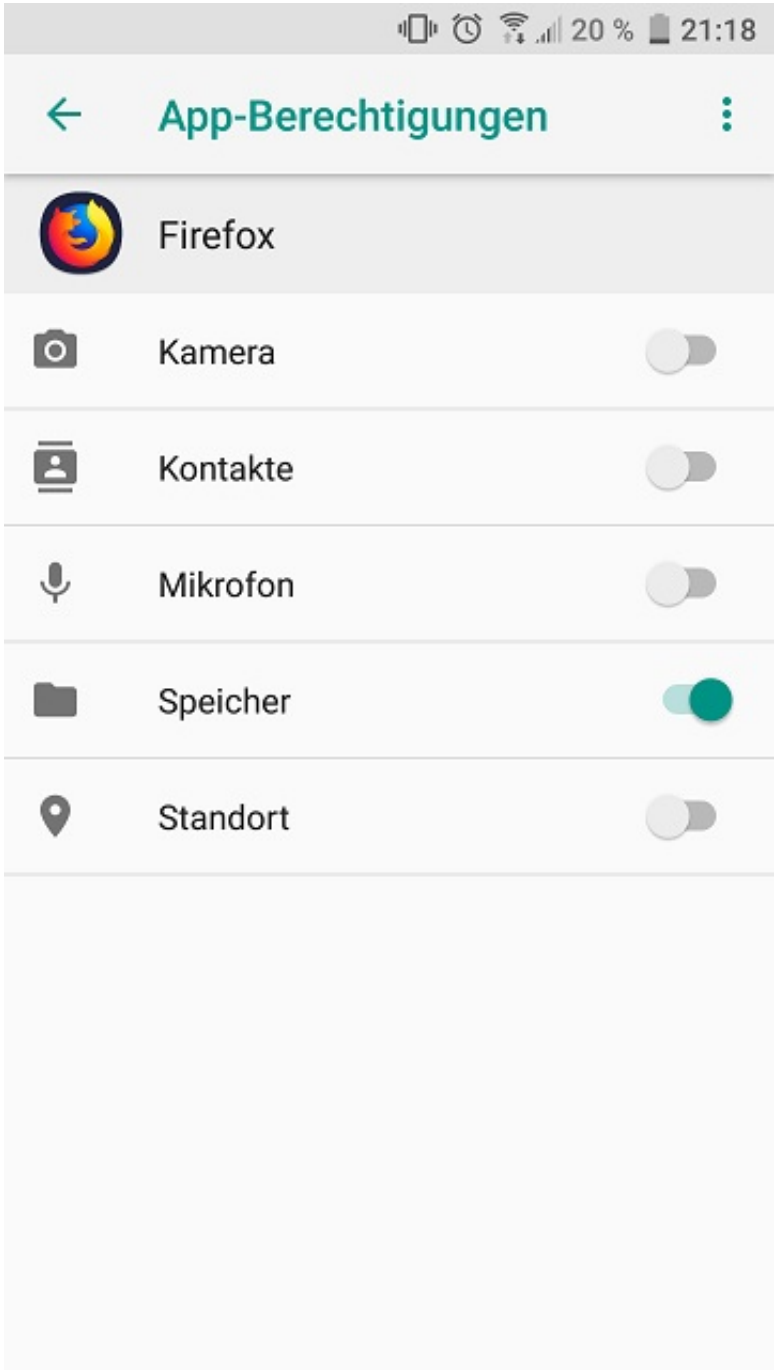
diese Weise kann die Kontrolle des Play Stores umgangen werden. Für den Nutzer bietet sich so die Möglichkeit, das Handy nach Belieben zu personalisieren. Zumindest, wenn der Entwickler der App sowie die Website, auf der der Installer heruntergeladen wird, vertrauenswürdig sind.

Fortnite für Android installieren: So geht's

Andernfalls kann es schnell passieren, dass man eigenständig Schadsoftware auf dem Smartphone installiert. Wenn man nicht zu 100 Prozent sicher sein kann, dass die Anwendung frei von Viren oder Spionage-Werkzeugen ist, sollte man die Android-Einstellung „Apps aus unbekannten Quellen zulassen" lieber deaktivieren. Und auch wenn die App vertrauenswürdig ist, empfiehlt es sich, die besagte Einstellung gleich nach der Installation wieder auszuschalten.

Tipp 5: App-Berechtigungen kontrollieren

Abseits von Viren können zahlreiche Nutzerdaten auch auf einem anderen, (halb-)offiziellen Weg an Dritte gelangen: über im App Store und Play Store verfügbare und dennoch unseriöse Apps. Diese erkennt man oftmals daran, dass sie mehr Berechtigungen einfordern, als sie für die eigene Funktionalität benötigen. Welche Berechtigungen das genau sind, kann man glücklicherweise sowohl unter Android (Google) als auch unter iOS (Apple) in den Einstellungen des Smartphones für jede Anwendung einzeln prüfen. Falls beispielsweise eine Taschenrechner-App Zugriff auf die Kontaktliste oder auf den Standort haben möchte, ist das ein Grund, misstrauisch zu werden. Solche Berechtigungen können einzelnen Anwendungen in den Einstellungen entzogen werden. Sie erhalten dann nur die Informationen, die sie tatsächlich benötigen.



Schutz vor Diebstahl, „physischem“ Datenklau und neugierigen Freunden

Tipp 6: Bildschirmsperre und SIM-Kartensperre

Abseits der digitalen Gefahren, die das „World Wide Web“ mit sich bringt, sollte man sein Smartphone auch vor physischen Übergriffen durch Cyberkriminelle sowie neugierige Freunde schützen. Zu den einfachsten Maßnahmen gehört hier zunächst die Bildschirmsperre. Diese stellt die erste und möglicherweise auch die wichtigste Schutzbarriere dar. Sie ist wohlbekannt und die meisten Nutzer verwenden sie. Doch auch hier gilt es

einige Dinge zu beachten, um einen guten Schutz zu gewährleisten. So ist und bleibt die Sperre per PIN-Code weiterhin die sicherste Variante. Falls die Muster-Entsperrung bevorzugt wird, empfiehlt es sich darauf zu achten, dass die Sichtbarkeit der Linien, die beim Zeichnen des Musters entstehen, ausgeschaltet ist. So minimiert sich das Risiko, dass Fremde das gewählte Muster durchschauen.

Moderne Geräte bieten zudem das Entsperren mithilfe biometrischer Daten an – sprich: Fingerabdrucksensor, Gesichtserkennung oder Iris-Scanner. In puncto Sicherheit unterliegen diese jedoch ebenfalls dem handelsüblichen Passwort beziehungsweise PIN-Code. Zudem müssen Benachrichtigungen von wichtigen Anwendungen, wie Mobile-Banking-Apps oder unter Umständen auch von Instant-Messaging-Diensten wie WhatsApp, auf dem Sperrbildschirm deaktiviert werden.

Ergänzend zur Bildschirmsperre sollten Nutzer auch die SIM-Karte schützen – falls die Sperre nicht sowieso bereits eingerichtet ist. Mit einer geschützten SIM-Karte lässt sich nur wenig anfangen. Auch wenn diese in ein anderes Smartphone eingesetzt wird. Die Sperre selbst kann bequem in den Einstellungen aktivieren oder deaktivieren. Falls das eigene Handy und / oder die SIM-Karte allerdings tatsächlich gestohlen werden, empfiehlt es sich dennoch zusätzlich auch den Provider zu kontaktieren.

Tipp 7: Gestohlenes oder verloren gegangenes Handy finden

Sämtliche bereits aufgeführte Maßnahmen helfen nicht viel, wenn das Smartphone unbemerkt aus der Tasche rutscht oder ein Dieb dieses in seine Finger bekommt. In diesem Fall existieren allerdings auch einige Möglichkeiten, das Problem mit etwas Glück zu lösen. So bieten sowohl iPhones als auch Android-Geräte die Möglichkeit, den Standort abzufragen, das Handy aus der Ferne zu sperren oder alle Daten zu löschen. Wie das bewerkstelligt werden kann, erläutert ein entsprechender Magazinartikel der Redaktion.

Es existieren allerdings auch einige Einschränkungen. Damit das Gerät

auffindbar ist, muss unter anderem eine Verbindung zum Internet bestehen und die Standortdienste müssen aktiviert sein. Diese Probleme lassen sich mit Anti-Diebstahl-Software wie „Cerberus“ sowie einigen Antivirus-Programmen lösen. Die Funktionsweise ist hier recht ähnlich, allerdings kann der Nutzer zusätzlich SMS-Befehle an das vermisste Handy senden und so Funktionen wie die Internetverbindung oder die Standortortung aus der Ferne einschalten – auch ohne, dass das Smartphone zuvor gerootet werden muss.

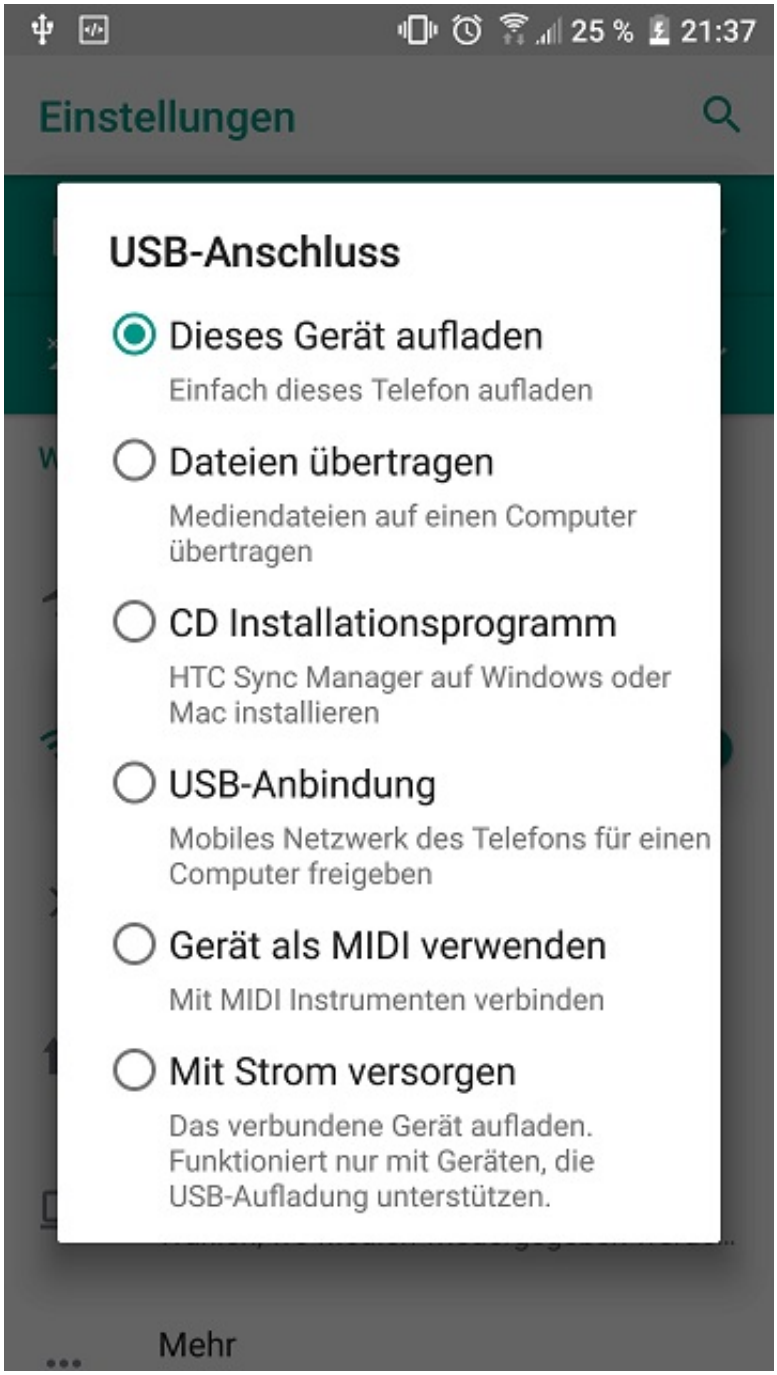
Lesetipps: Gestohlene Handys per IMEI sperren lassen

Solche Anti-Diebstahl-Apps bieten einen recht hohen Schutz, doch auch diese sind nicht ideal. So müssen solche Anwendungen, genauso wie ihre offiziellen iOS- und Android-Pendants, bereits vor dem Diebstahl eingerichtet worden sein. Zudem empfiehlt sich hier ebenfalls eine Displaysperre, denn ansonsten können Diebe die Funktionen schlicht ausschalten und somit jeglichem Fernzugriff entgegenwirken. Zu guter Letzt sollte der Besitzer schnell handeln. Denn sobald der Akku erschöpft ist, gibt es nicht mehr viel, was noch getan werden kann.

Tipp 8: Vorsicht bei USB- und Bluetooth-Verbindungen

Obwohl die Gefahr, sich Schadsoftware oder Spionage-Apps per USB-Verbindung auf das Smartphone zu holen, recht gering ist, besteht sie durchaus. Darum sollte sich das Handy im besten Fall nur mit vertrauenswürdigen Rechnern verbinden. Wer sein Gerät aufladen möchte, sollte darüber hinaus darauf achten, dass in den Einstellungen, die beim Einstecken des Kabels erscheinen, lediglich die Strom- und nicht die Datenverbindung aktiviert ist. Alternativ kann hier auch ein sogenanntes „USB-Kondom“ helfen, das als Adapter ebenfalls keine Datenverbindung zulässt. Selbiges gilt auch für Funk-Verbindungen wie beispielsweise über

Bluetooth. Damit das Smartphone wirklich geschützt ist, müssen diese ausgeschaltet bleiben, sofern sie nicht gerade benötigt werden.



Wer aufmerksam ist, bleibt geschützt

Sämtliche genannten Schutzmaßnahmen können eine große Hilfe darstellen, wenn es darum geht, ein Betriebssystem vor Viren, Malware, Spionage-Apps sowie sonstigen Gefahren zu schützten und die Smartphone-Sicherheit allgemein zu erhöhen. Das alles hilft allerdings nicht viel, wenn der Nutzer selbst nicht aufmerksam ist. Wer beispielsweise eine E-Mail von einem nigerianischen Prinzen erhält, sollte kritisch bleiben. Und

auch nicht jede URL-Adresse, die in einem WhatsApp-Kettenbrief enthalten ist, muss besucht werden. Den größten Beitrag zum Schutz eines Smartphones leistet nach wie vor der Besitzer selbst.

Smart Home: Intelligente Sicherheitssysteme zum Schutz vor Einbrechern