10 Sicherheitstipps für das Smartphone

Von Abofalle bis Virenschutz

Ein Artikel von Autorin Jeanine Wein Referentin bei der Verbraucherzentrale Rheinland Pfalz

Ein Smartphone ist ein kleiner Computer – und genau wie dieser verschiedenen Gefahren ausgesetzt. Aus diesem Grund ist es sinnvoll, sich mit dem Thema Sicherheit bei den kleinen Alleskönnern auseinanderzusetzen. Funktionen wie beispielsweise die Bildschirmsperre können den Schutz privater Daten im Handumdrehen erhöhen. Die folgenden zehn Tipps geben Nutzerinnen und Nutzern mehr Sicherheit im Umgang mit den praktischen Alltagshelfern.

Smartphone-Schutzhülle

Als Spider-App („Spinnen-App“) bezeichnet man mittlerweile ein häufig anzutreffendes Phänomen: Risse, die sich wie ein Spinnennetz über den Smartphone-Bildschirm ziehen. Doch diese Anwendung wurde keineswegs freiwillig installiert, sie ist meist das Ergebnis eines unachtsamen Augenblicks: Das Smartphone fällt zu Boden, das Display reißt. Um Stürze etwas weniger gefährlich zu machen, kann eine Schutzhülle sinnvoll sein. Im Einzelhandel oder im Internet findet sich bestimmt ein für das eigene Gerät passendes Modell.

Datensicherung

Geht das Smartphone kaputt, kommt zum finanziellen Schaden noch ein weiterer Aspekt hinzu: verlorene Daten. Um dieser Situation vorzubeugen, empfiehlt sich eine regelmäßige Datensicherung, Backup genannt. Ob man die Dateien händisch auf einen Computer überträgt oder eine automatische Sicherung in der Cloud, einem Internetspeicher, bevorzugt, hängt von mehreren Faktoren ab. Wichtige Fragen, die man sich vor einer Entscheidung stellen sollte, werden in dem Artikel „Backup-Möglichkeiten: Datensicherung für Smartphones und Tablets“ beschrieben.

Bildschirmsperre

Zugegeben: Es ist viel bequemer, das eigene Smartphone mit einer einfachen Wischbewegung zu entsperren. Allerdings ist das auch sehr unsicher. Denn gelangt das Gerät in falsche Hände, ist nicht nur der Weg zu allen auf dem Gerät gespeicherten Daten frei: Unbefugte können beispielsweise über die Telefonfunktion Kosten verursachen (beispielsweise mit Anrufen auf Sonderrufnummer oder ins Ausland). Im schlechtesten Fall gibt es auf diesem Weg auch Zugriff auf Nutzerkonten frei, die auf dem Gerät gespeichert sind, und es können im Namen der oder des Betroffenen Mails verschickt oder Bahnkarten gebucht werden. „Was die Haustür für das Haus, ist die Bildschirmsperre für Smartphones“, heißt es auf der Website mobilsicher.de. Hier lässt sich auch nachlesen, mit welchen Methoden man die „Haustür“ am Smartphone am besten absperrt.
Nicht zu verwechseln mit der Bildschirmsperre ist die SIM-PIN. Sofern eine SIM-Karte im Gerät eingelegt ist, wird zusätzlich eine PIN abgefragt – diese schützt jedoch lediglich die SIM-Karte, diese wird aber nur beim Einschalten des Geräts (beim Hochfahren) abgefragt.

Abofallen vermeiden

Für Smartphones gibt es viele kostenlose Apps – allerdings verbergen sich in manchen davon fiese Kostenfallen: So kann ein (unbeabsichtigter) Klick auf ein Werbebanner nicht nur eine Internetseite öffnen, sondern gleichzeitig noch ein kostenpflichtiges Abo aktivieren. Die Kosten dafür tauchen als Posten eines Drittanbieters auf der Mobilfunkrechnung auf – die meisten Betroffenen erfahren meist auch erst dann von dem vermeintlichen Vertragsabschluss. Um es gar nicht so weit kommen zu lassen, empfiehlt sich eine sogenannte Drittanbietersperre. Diese lässt sich über den Mobilfunkanbieter kostenlos einrichten. Wie genau man die Sperre einrichtet, was man beachten sollte und was man tun kann, wenn man bereits in die Falle getappt ist, lässt sich auf der Seite der Verbraucherzentralen nachlesen.

Diebstahlschutz

Es passiert schneller, als man denkt: Im Nu ist das Smartphone weg. Ob verloren oder gestohlen, hier könnten Kosten entstehen. Aus diesem Grund ist es sinnvoll, sein Gerät gegen Diebstahl abzusichern: Neben einer Bildschirmsperre und regelmäßigen Datensicherungen (siehe oben) lassen sich auch Sicherheitsapps so einstellen, dass sie im Falle des Verlusts Fernzugriff auf das gestohlene Gerät ermöglichen, um beispielsweise alle Daten zu löschen. Die Website mobilsicher.de erklärt ausführlich, welche Maßnahmen man vorbeugend ergreifen sollte, wie man solche Sicherheitsapps richtig verwendet und was man zur Schadensbegrenzung tun kann, sollte das Smartphone bereits weg sein.

Funktionen ausschalten

Smartphones sind kleine Computer mit vielen verschiedenen Funktionen. Aber längst nicht alle werden ständig benötigt. Um potenzielle Hintertüren zu schließen und Datenspuren zu verringern, kann man nicht benutzte Funktionen wie Bluetooth, NFC und GPS/Ortungsdienste ausschalten. Wenn man die Funktionen braucht, beispielsweise für ein Autotelefon oder um sich navigieren zu lassen, kann man sie wieder aktivieren. Positiver Nebeneffekt des Ausschaltens: Vielleicht hält so auch der Akku länger durch.

Vorsicht bei App-Installationen

Kleine Anwendungen, Apps genannt, machen das Smartphone erst richtig smart. Um sie zu installieren, sollte man immer nur die Anbietershops des jeweiligen Betriebssystems nutzen. Das bedeutet in der Praxis: Auf den meisten Geräten ist bereits eine App installiert, über die man weitere Apps herunterladen kann, für Android-Geräte ist das der (Google) Play Store, bei Apple der AppStore (iTunes) und bei Windows-Smartphones heißt die Anwendung schlicht „Store“. Diese vorinstallierten Anwendungen zu nutzen, ist empfehlenswert, da hier nur Apps landen, die zumindest grundsätzlich überprüft wurden. Wie die Vergangenheit zeigte, sind schadhafte Apps aber trotzdem nicht völlig auszuschließen.
Wie man Apps beispielsweise unter dem Betriebssystem Android auf das eigene Gerät bringt, sieht man in diesem Video.

Berechtigungen prüfen

Holt man sich Apps auf das eigene Gerät, muss man der Anwendung bei der Installation erlauben, dass sie auf bestimmte Bereiche des Telefons zugreifen kann (z.B. Kontakte, Fotos etc.). Eine Navigationsapp muss beispielsweise auf die Standortinformationen des Geräts zugreifen können, um ihre Funktion auch umzusetzen. Eine Foto-App braucht Zugriff auf die Kamera. Doch nicht alle Berechtigungen, die sich die kleinen Programme geben lassen, sind auch immer unbedingt zum Funktionieren nötig. Manchmal sind die Unternehmen hinter den Apps auch schlicht neugierig. Im Idealfall schaut man schon bei der Installation auf die geforderten Berechtigungen und wägt für sich ab, ob man diese App zu den Bedingungen haben möchte. Je nach Betriebssystem(Version) lassen sich Berechtigungen auch im Nachhinein geben oder entziehen (mehr zum Thema Rechte-Verwaltung bei Android und bei iOS). Mobilsicher.de versucht, die oft schwer verständlichen Zugriffsrechte zu entschlüsseln, damit eine Einschätzung der Sinnhaftigkeit leichter wird.

Updates

Wer einen Computer nutzt, kennt sie: die Updates. Und auch Smartphone-Besitzerinnen und -Besitzer haben mit ihnen zu tun, und das ist gut so. Denn Updates aktualisieren, fügen vielleicht neue Funktionen hinzu, beheben Fehler und schließen bekanntgewordene Sicherheitslücken (mehr dazu auf mobilsicher.de). Bei Smartphones gibt es zwei Typen von Updates: die des Betriebssystems und die von Apps. Grundsätzlich gilt: Betriebssystem und Anwendungen sollte immer auf dem neusten Stand gehalten werden. Nicht benötigte Apps kann man alternativ auch deinstallieren.
Updates unterscheiden sich von Upgrades. Ein Update aktualisiert ein bestehendes System, bei einem Upgrade wird quasi die ganze Anwendung ausgetauscht – es handelt sich um ein neues System.

Virenschutz per App

Auch das Smartphone kann sich einen Schnupfen holen – Viren und andere elektronische Schädlingen gibt es mittlerweile auch für die smarten Telefone. Vor allem Geräte mit dem Betriebssystem Android sind gefährdet. Aus diesem Grund kann die Installation einer Antiviren-App sinnvoll sein.
Das Computerportal Chip listet getestete Schutzsoftware auf.

Dieser Artikel gibt den Sachstand zum Zeitpunkt der Veröffentlichung wieder. Datum: 12. Mai 2021