

Die Gefahren bei der Smartphone-Nutzung lauern an verschiedenen Stellen. Dabei ist der Schutz des eigenen Smartphones eigentlich nicht komplizierter als der Schutz eines stationären Computers. Die folgenden sieben Tipps helfen Ihnen, Ihre Smartphonesicherheit zu optimieren.

Tipps 1 - Smartphonesicherheit: Vorsicht vor Diebstahl

Der erste Tipp hat erst mal nichts mit einer komplizierten App oder verworrenen Einstellungen zu tun. Damit Dritte keine Möglichkeit bekommen auf Ihr Smartphone und Ihre Daten zuzugreifen, sollten Sie Ihr **Handy nie unbeaufsichtigt lassen**. Wird es Ihnen doch einmal gestohlen, können Sie Vorbereitungen dafür treffen, dass die Diebe mit Ihrem Smartphone und Ihren Daten so wenig wie möglich anfangen können. Dazu können Sie im Vorfeld eine App runterladen, die es Ihnen ermöglicht, das **Gerät aus der Ferne zu sperren**. Das funktioniert über eine SMS von einem anderen Handy oder über die Webseite des Anbieters der App. Achten Sie bei der Auswahl der App aber auf einen vertrauenswürdigen Anbieter, z.B. Avast Anti-Theft oder F-Secure Mobile Security. Wenn Sie ein Google-Konto haben oder anlegen möchten, können Sie auch hier einen Datenschutz bei Diebstahl einrichten. Bei Google ist der Dienst kostenlos. Sobald Sie Ihr Smartphone gesperrt haben, sollten Sie Ihre **SIM-Karte über den Anbieter sperren lassen**.

Tipps 2 - Displaysperre

Die zweite wichtige Hürde für einen Dieb ist eine Displaysperre. Hier gibt es zwei Möglichkeiten die **Smartphonesicherheit** zu erhöhen: eine **PIN-Sperre** oder eine **Mustersperre**. Experten raten zu einer PIN-Sperre, da Mustersperren Spuren auf dem Display hinterlassen können. Generell sollten Sie bei der Eingabe des Codes oder des Musters **auf Sichtschutz achten**, damit keine andere Person Ihren Code oder Ihr Muster sehen kann.

Eine Displaysperre kann man bei Android unter Einstellungen ⇒ Sperrbildschirm einrichten, wo man die Möglichkeit hat, beide Sperren einzurichten.

Für eine PIN-Sperre beim iPhone muss man sich unter Einstellungen ⇒ Allgemein ⇒ Code-Sperre ⇒ Code aktivieren einen vierstelligen Code ausdenken. Eine Mustersperre gibt es für das iPhone nicht.

Tipp 3 - Schnittstellen

Von den physischen Dieben kommen wir zum **Schutz vor (Daten-)Dieben** in der virtuellen Welt. Wenn man zu Hause ist, loggt man sich meistens in das eigene WLAN-Netz ein. Auch unterwegs braucht man nicht immer die mobilen Daten, weil es kostenlose WLAN-Hotspots gibt. Sobald Sie jedoch das WLAN nicht mehr benutzen, sollten Sie es auch ausschalten. Genauso verhält es sich mit Bluetooth und GPS. Das Ausschalten hat zwei Vorteile: einerseits bieten Sie weniger Angriffsfläche für Leute, die über Schnittstellen wie Bluetooth auf Ihr Smartphone zugreifen möchten, und andererseits verlängern Sie Ihre Akkulaufzeit erheblich. Wenn Sie eine dieser Schnittstellen für eine [Notfallfunktion](#) nutzen (z.B. GPS), sollten Sie diese Schnittstelle natürlich aktiviert lassen.

Tipp 4 - öffentliche Hotspots

Wenn wir schon beim WLAN sind, gleich noch eine Warnung zu öffentlichen Hotspots. Im Gegensatz zum WLAN zu Hause, das man meistens gut sichert, sind **öffentliche WLAN-Netze nicht verschlüsselt**. Das heißt für Sie, dass Sie für Ihre Smartphonesicherheit darauf achten sollten, welche Webseiten Sie besuchen. **Online Banking ist komplett tabu**. Bei anderen Webseiten sollten Sie auf das Kürzel „https“ in der Adresszeile achten. Allgemein empfiehlt sich, auf Hotspots nur durch einen VPN-Tunnel zuzugreifen. Ein VPN-Tunnel ist eine speziell abgeschirmte Verbindung. Diesen können Sie als App auf Ihrem Smartphone installieren. Dazu gehen Sie zu Google Play oder dem Apple Store, geben „VPN“ als Suchbegriff ein und installieren eine der Apps. Zu empfehlen ist z.B. Hotspot Shield.

Tipp 5 - Drittanbietersperre

Beim Surfen im Internet kann man schnell mal darauf reinfallen: **Abofallen**. Einmal aus Versehen oder aus Neugierde auf ein Werbebanner einer Abzocke-Firma getippt und auf

einmal steht auf der nächsten Telefonrechnung ein Abo, was man abgeschlossen haben soll. Um das zu vermeiden, sollten Sie eine sogenannte **Drittanbietersperre** einrichten. Diese können Sie bei Ihrem Mobilfunk-Anbieter kostenlos anfordern. Die [Verbraucherzentrale](#) zeigt Ihnen, wie es geht.

Tipp 6 - Virenprogramme und Sicherheitsupdates

Diesen Tipp kennen Sie vielleicht schon von Ihrem Computer. Auch Smartphones sind kleine Computer und können durch Virenprogramme und regelmäßige Sicherheitsupdates geschützt werden.

Virenprogramme: Ein Virenprogramm können Sie sich auch ganz einfach als App runterladen. Dazu gehen Sie zu Google Play und suchen nach Virenprogrammen. Die ersten, die angezeigt werden (Avira, Kaspersky, AVG, Avast) sind auch die meistgenutzten und können ruhig installiert werden. Für iPhones gibt es keine Virenprogramme, die man nachrüsten kann, da das Betriebssystem sehr verschlossen und dadurch weniger anfällig ist.

Sicherheitsupdates: Updates für die Sicherheit und für das Betriebssystem sollten immer umgehend installiert werden. Am einfachsten ist das, wenn Sie die automatische Update-Funktion einschalten. Für ein iPhone geht das über Einstellungen ⇒ iTunes & App Store ⇒ Automatische Downloads ⇒ Updates. Bei Android-Geräten sind die automatischen Updates als Standard eingestellt.

Tipp 7 - Apps

Im letzten Tipp geht es noch mal ausschließlich um Apps. Grundsätzlich gilt, dass man **Apps nur aus vertrauenswürdigen Quellen installieren** sollte, also aus Google Play und dem Apple Store. Wenn Sie den Anbieter einer App nicht kennen, suchen Sie kurz nach ihm im Internet, um herauszufinden, ob er vertrauenswürdig ist, sonst steht es schlecht mit Ihrer Smartphonesicherheit.

Deinstallieren Sie ungenutzte Apps. Jede zusätzliche App auf Ihrem Smartphone stellt eine Sicherheitslücke dar.

Zugriffsrechte von Apps

Ein letzter, aber wichtiger, Punkt sind die Zugriffsrechte von Apps. Bei **alten Android-Versionen** (bis Android 5.1) lassen sich die Zugriffsrechte leider nicht einschränken. Entweder man installiert die App mit allen verlangten Zugriffsrechten oder man verzichtet.

Ab der **Version Android 6.0** können die Zugriffsrechte angezeigt und einzeln entfernt werden. Dazu gehen Sie nach der Installation in die Einstellungen und dort in den Anwendungsmanager und wählen eine App aus. Scrollen Sie nach unten zu den Berechtigungen. Jetzt können Sie die einzelnen Berechtigungen ein- und ausschalten. Die Programme können auch später noch Zugriffsrechte anfordern, wenn sie sie für die Ausführung der App brauchen. In diesem Fall können Sie während der Benutzung der App entscheiden, ob die App die aktuell geforderten Zugriffsrechte wirklich braucht oder nicht. Überlegen Sie immer, welche Zugriffsrechte die jeweilige App wirklich benötigt.

Auf dem **iPhone** müssen Sie zum Ändern der Zugriffsrechte nur in den Einstellungen auf den Menüpunkt „Datenschutz“ gehen. Hier können Sie den Apps auch später noch einzelne Zugriffsrechte entziehen.

Bei Updates sollten Sie auch genau hingucken, welche Änderungen das Update vornehmen möchte. Es kann nämlich vorkommen, dass **ein Update auch Zugriffsberechtigungen verändern will**. Bei älteren Versionen des Android-Smartphones (bis Version 5.1) hat man leider wieder nur die Möglichkeit, das Update mit allen Änderungen anzunehmen oder auf das Update zu verzichten. Wenn man verzichtet, dann wird allerdings möglicherweise eine Sicherheitslücke nicht geschlossen, wodurch Ihr Smartphone angreifbar wird.

Ab der Version Android 6.0 können Sie die Zugriffsrechte jedoch wieder einschränken. Damit die Updates nicht automatisch ablaufen und Sie den Überblick verlieren, können Sie einstellen, dass Sie **jedes Update und seine Zugriffsberechtigungen manuell bestätigen** müssen. Dazu gehen Sie zu Google Play, tippen auf das Menü (die drei Querstreifen im Suchfeld ganz oben) und dann auf Einstellungen. Hier können Sie unter „Allgemein“ das Menü „Automatische App-Updates“ auswählen, wo Sie dann „Keine automatischen App-Updates zulassen“ auswählen. Unter Benachrichtigungen sollten Sie jetzt noch auswählen, dass Sie eine Benachrichtigung haben wollen, wenn ein neues Update verfügbar ist.

Bei einem iPhone müssen Sie in die Einstellungen gehen und dort unter „Automatische Downloads“ im Punkt „Updates“ die Regler von Apps und Updates nach links verschieben. Ab jetzt wird Ihnen im Home-Bildschirm am App-Store-Button mit einer roten Zahl

angezeigt, wie viele neue Updates verfügbar sind.

