Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Wie sicher ist dein Smartphone?

Ratgeber zum Datenschutz

Wie sicher ist dein Smartphone?

Ratgeber zum Datenschutz

Herausgeberin:

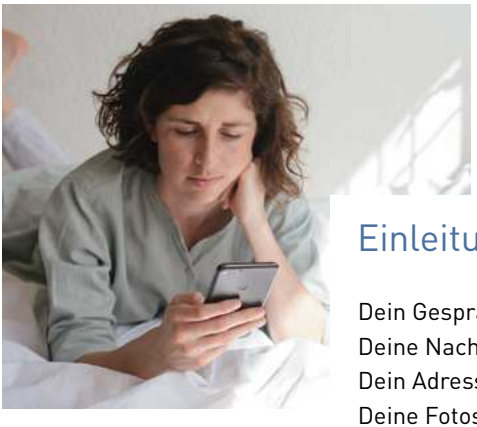
Berliner Beauftragte für
Datenschutz und Informationsfreiheit

Friedrichstr. 219
Besuchereingang: Puttkamerstr. 16-18
10969 Berlin
Telefon: 030 13889-0
Telefax: 030 2155050
E-Mail: mailbox@datenschutz-berlin.de

Gestaltung: april agentur GbR
Druck: ARNOLD group.

Stand: März 2020

Inhalt



Einleitung

Dein Gespräch!
Deine Nachrichten!
Dein Adressbuch!
Deine Fotos! Deine Musik!
Deine Daten!

Dein Smartphone hast du natürlich immer dabei. Du machst damit Fotos, spielst deine Lieblingssongs ab, streamst Musik, teilst deine Erlebnisse, verwaltest damit deine Termine und Kontakte, surfst im Internet und nutzt Apps.

Damit gilt aber auch: Je mehr Funktionen dein Smartphone hat, umso anfälliger ist es für verschiedenste Gefahren. Und selbstverständlich ist im Schadensfall letztendlich nicht dein Smartphone zu bedauern.

Im Gegenteil: Du bist es, der durch eine ausgenutzte Sicherheitslücke unter Umständen gravierende Nachteile zu erleiden hat.

Das deutsche Grundgesetz gewährt dir das Recht auf „informationelle Selbstbestimmung“. Danach hast du grundsätzlich das Recht, selbst über die Preisgabe und Verwendung deiner personenbezogenen Daten zu bestimmen. Du musst aber auch selbst auf den Schutz deiner Daten achten. Im Umgang mit Smartphones z. B. gibt es eine Reihe nützlicher Tipps, die es zu beachten gilt, wenn du verhindern willst, dass die falschen Leute an deine Anruflisten, deine Musik, deine Nachrichten, deine Fotos, eben deine persönlichen Smartphonedaten kommen können.

PERSONENBEZOGENE DATEN: Hierbei handelt es sich um alle möglichen bestimmbaren Einzelangaben zu einer konkreten Person. Also neben offensichtlich personenbezogenen Daten wie deinem Namen, deinem Geburtstag oder deiner Wohnadresse usw. sind z. B. auch deine Essgewohnheiten, dein Musikgeschmack oder der Inhalt von Telefongesprächen gemeint. Als sensitive (besonders schützenswerte) personenbezogene Daten gelten Angaben über deine Gesundheit, deine ethnische Herkunft sowie deine religiöse, politische oder sexuelle Orientierung.

Diese Tipps wird dir diese Broschüre geben: Zunächst erfährst du, wo mögliche Gefahren für deine persönlichen Daten im Umgang mit Smartphones liegen. Anschließend zeigen wir dir, wie du diesen Gefahren am besten begegnest.

1. Viren und andere Schadsoftware

Was vom PC her schon lange bestens bekannt ist, macht sich seit einiger Zeit auch verstärkt bei Smartphones breit.

VIREN, WÜRMER UND TROJANER: Das sind kleine schädliche Programme, die sich über verschiedene Wege von Smartphone zu Smartphone selbstständig verbreiten können. Gelangt ein solches Programm auf dein Smartphone, kann es dessen Funktion erheblich beeinträchtigen, deine Daten ausspionieren oder löschen und sogar hohe Kosten (z. B. durch Versenden von sogenannten Premium-SMS) verursachen.

Mit steigendem Funktionsumfang der Geräte hat auch die Gefahr der Infizierung durch Smartphone-Viren zugenommen. Wichtig ist es deshalb, dass du bestimmte Vorkehrungen triffst, um dein Smartphone gegen die neuen Gefahren immun zu machen. Mögliche Eingangstore für Viren in dein Smartphone sind der Download von Klingeltönen, Logos, Spielen, Apps sowie ungeschützte Funkschnittstellen wie Bluetooth und offene WLAN-Verbindungen (unverschlüsselte, kabellose Internetverbindungen).

Achte also darauf, dass du dir zugesandte Bilder, Songs oder Dateien nur dann annimmst, wenn du sie tatsächlich angefordert hast oder den/die Absender/in und seine/ihre Absichten wirklich kennst. Dem Empfang unaufgeforderter Daten kannst du vorbeugen, indem du die Bluetooth-Funktion deines Smartphones auf „unsichtbar" einstellst. Benutzt du die Funkschnittstellen deines Smartphones nur gelegentlich, dann ist es am besten, diese im Menü komplett abzuschalten und nur bei Bedarf wieder zu aktivieren. So behältst du immer die Kontrolle und gefährliche Programme haben keinen Zutritt. Inzwischen gibt es auch Antivirenprogramme für Smartphones mit Android-Betriebssystemen.

Tipp: **Nimm niemals ausführbare Dateien an, die sich unaufgefordert in dein Smartphone einschleichen wollen.**

2. Mobiler Datenspeicher

Viele Handys und Smartphones verfügen über einen relativ großen Speicher. Sie ersetzen damit u. a. die herkömmlichen USB-Sticks als mobile Datenspeicher. Damit gelten natürlich alle Sicherheitshinweise für USB-Sticks in Verbindung mit Computern gleichermaßen auch für dein Smartphone.

Besonders gefährlich ist hierbei die Übertragung von Computerviren von einem PC zum anderen über ein infiziertes Smartphone. Leider kommt es auch immer wieder vor, dass mobile Datenspeicher verloren gehen oder gestohlen werden. So können persönliche Daten von dir leicht in fremde Hände gelangen. Daher ist es wichtig, dass du dein Smartphone mit möglichst sicherem Passwort oder einer mindestens sechsstelligen PIN schützt, die beim Aktivieren des Geräts eingegeben werden muss, damit du dein Smartphone nutzen kannst.

Sei auch bei der Arbeit am PC gegen Virengefahren gewappnet. Achte z. B. immer darauf, dass der Computer, an den du dein Smartphone anschließt, über eine aktuelle Anti-Viren-Software verfügt. Sollte sich doch einmal ein PC-Virus in dein Smartphone eingeschlichen haben, so sorge dafür, dass dieser zuerst entfernt wird, bevor du das Gerät an die „gesunden" Rechner zu Hause oder bei deinen Freundinnen und Freunden anschließt.

SIM-SPERRUNG: Für den Fall, dass du dein Smartphone verloren hast oder es dir geklaut wurde, solltest du sofort die SIM-Karte in deinem Smartphone sperren lassen. Damit wird verhindert, dass der/die Dieb/in (oder Finder/in) auf deine Kosten weiter telefonieren kann. Zur Sperrung deines Smartphones wähle den zentralen Sperr-Notruf 116 116 und halte die Telefonnummer und Kundennummer deines Mobilfunkvertrages bereit.

Klar ist, dass du dein Smartphone immer gut vor Verlust oder Diebstahl schützt. Da man das aber nie ganz ausschließen kann, solltest du darauf achten, keine sensiblen Daten unverschlüsselt auf deinem mobilen Speicher abzulegen. Als sensible Daten gelten Daten mit erhöhtem Schutzbedarf, wie z. B. deine Noten, dein Kontostand, deine Fotos.

Tipp: **Achte immer auf einen aktuellen Anti-Viren-Schutz und speichere möglichst keine sensiblen Daten ungeschützt auf dem Smartphone.**

3. Spionage & Datenklau

Auch ohne dass jemand dein Smartphone in die Hand bekommt, ist es bei Nicht-Beachtung bestimmter Sicherheitsregeln möglich, an die darauf gespeicherten Daten zu gelangen. Über die Bluetooth-Funktion können dir nicht nur unaufgefordert Dateien auf dein Smartphone gesendet werden. Bei Smartphones mit Sicherheitslücken kann es auch für Außenstehende möglich sein, die darauf befindlichen Daten auszulesen und im Extremfall sogar jede denkbare Art von Befehlen auszuführen.

Um dich vor solchen Bluetooth-Attacken zu schützen, solltest du immer die aktuellste Version des Betriebssystems auf deinem Smartphone installiert haben. Weiterhin gilt, was auch schon beim Schutz vor Smartphone-Viren gesagt wurde: Bluetooth-Funktion dauerhaft abschalten und nur bei Bedarf wieder aktivieren.

BLUETOOTH: Bluetooth ist eine Funk-Übertragungstechnik für digitale Daten. In Smartphones dient sie z. B. dazu, Musik auf dein Headset oder Fotos auf ein anderes Smartphone zu senden. Die Reichweite von Bluetooth-Verbindungen liegt zwischen 10 und 100 Metern. Aufgrund der kabellosen Verbindung ist diese Technik besonders anfällig für Angriffe, z. B. von Viren. Aber auch die Werbeindustrie nutzt Bluetooth in verstärktem Maße. So gibt es Bluetooth-fähige Werbetafeln, die dir unaufgefordert im Vorbeigehen Produktinformationen auf dein Smartphone schicken wollen. Um die Bluetooth-Schnittstelle deines Smartphones gegen Angriffe abzusichern, solltest du die Funktion immer auf „unsichtbar“ oder „abgeschaltet“ einstellen.

Eine besonders sichere Variante des Datenaustausches über Bluetooth stellt das sogenannte Pairing-Verfahren dar. Hierbei wird jeweils auf den beiden miteinander kommunizierenden Telefonen die Eingabe desselben Passwortes verlangt. Erst bei Übereinstimmung werden die gewünschten Daten verschlüsselt übertragen.

Und noch etwas: Dein Smartphone hat einen Namen! Diesen findest du in den „Einstellungen“ Deines Smartphones. Andere Bluetooth-fähige Geräte bekommen diesen Namen im Sendebereich deines Smartphones angezeigt. Um potenziellen Angreifern kein allzu offensichtliches Ziel zu bieten, denke dir einen Fantasienamen für dein Smartphone aus, der möglichst nicht darauf schließen lässt, dass das Telefon dir gehört.

Tipp: **Um Datenklau-Attacken zu verhindern, deaktiviere die Bluetooth-Funktion deines Smartphones und halte die Betriebssystemsoftware auf dem aktuellsten Stand.**

4. Datensicherung

Du selbst musst entscheiden, wie wichtig eine regelmäßige Sicherung der Daten in deinem Smartphone ist. Wenn du eigentlich nur die Telefonnummern deiner Freundinnen und Freunde gespeichert hast, dann reicht es sicherlich, gelegentlich das Adressbuch zu Hause zu aktualisieren.

Es gibt aber auch Programme, die die Daten deines Smartphones mit dem Terminkalender und dem Adressbuch auf dem PC abgleichen und automatisch aktualisieren. Schau auf der Webseite des Smartphone-Herstellers nach.

Außerdem gibt es im Internet Backup-Dienste für Smartphones. Beachte dabei aber, dass der Internetdienst alle deine Smartphone-Daten bekommt.

Tipp: **Nutze Online-Backup-Dienste nur, wenn diese vertrauenswürdig sind.**

5. Datenlöschung bei Weitergabe & Entsorgung

Möchtest du dein altes Smartphone verkaufen, verschenken oder einfach nur entsorgen? Dann solltest du selbstverständlich darauf achten, dass deine gespeicherten persönlichen Daten niemand anderem dabei in die Hände fallen.

Um dein Smartphone von allen personenbezogenen Daten zu säubern, müssen die SIM-Karte und eventuell vorhandene Speicherkarten entfernt werden. Außerdem solltest du über das Menü (sofern vorhanden) folgende private Daten löschen:

- Telefonbuch, Adressbuch bzw. Kontakte
- Kalenderdaten, Notizen, Aufgabenlisten
- Video- und Tondateien
- Verbindungsdaten wie gewählte oder angenommene Anrufe
- Mitteilungen (SMS, MMS, E-Mails)
- Internetdaten (Cache-Speicher, Cookies, Lesezeichen)
- Kommunikationsdaten (wie E-Mail-Provider, Bluetooth-Verbindungseinstellungen)
- Apps und deren Daten

Nutze hierfür die Option „Auf Werkseinstellungen zurücksetzen“. Die Funktion führt einen „harten Reset“ durch, bei dem der gesamte Speicher in den Auslieferungszustand zurückversetzt wird. Befinden sich besonders sensible Daten auf deinem Smartphone, solltest du eine spezielle Lösch-Software einsetzen.

ACHTUNG UMWELTSCHUTZ: Alte Smartphones dürfen nicht einfach in die Mülltonne geworfen werden, sondern müssen fachgerecht entsorgt werden. Bringe dein Smartphone zu diesem Zweck zu einer der dafür vorgesehenen öffentlichen Sammelstellen bzw. frage in deinem Mobil-

telefonshop oder einem Elektromarkt, ob dieser die Entsorgung für dich übernimmt.

Tipp: **Achte darauf, dass sich bei Weitergabe oder Entsorgung deines alten Smartphones keine persönlichen Daten mehr darauf befinden.**

6. Lockanrufe

Immer wieder kommt es vor, dass Betrüger/innen mit sogenannten „Lockanrufen" Handybesitzerinnen und Handybesitzern das Geld aus der Tasche ziehen wollen. Dabei wird eine SMS an dein Smartphone geschickt (meist mit einer darin enthaltenen Frage) oder kurz auf deinem Smartphone angeklingelt, sodass du es nicht schaffst, den Anruf rechtzeitig anzunehmen. Der/die Betrüger/in hofft nun, dass du eine SMS zurückschickst oder den/die unbekannte/n Anrufer/in zurückrufst. Handelt es sich dann bei der zurückgerufenen Nummer um einen sogenannten „Mehrwertdienst", bist du um einiges ärmer und der/die Betrüger/in verdient sich durch die Vielzahl der Rückrufer/innen eine goldene Nase.

Beginnt die Absendernummer mit den Ziffern „0137" oder „0900", bzw. „+49137" oder „+49900" oder hat die Nummer nur 5-6 Stellen, steckt ganz sicher ein Mehrwertdienst dahinter, der dich teuer zu stehen kommen kann. Also nicht zurückrufen! Vorsicht auch bei ausländischen Telefonnummern. Die beginnen auch mit einem „+" oder „00", es folgt aber eine andere Zahl als die 49 (die 49 ist die internationale Telefonvorwahl für Deutschland).

Tipp: **Antworte am besten nie auf SMS oder Anrufe von dir unbekannten Rufnummern, um so ungewollte Kosten von vornherein zu vermeiden.**

7. Lokalisierung (Bewegungsprofile)

Damit du überhaupt unterwegs telefonieren kannst, muss sich dein Smartphone immer bei der nächstgelegenen Mobilfunk-Sendeantenne anmelden. Somit weiß dein Netzanbieter prinzipiell immer, wo du dich ungefähr befindest. Fasst man diese Informationen über einen gewissen Zeitverlauf zusammen, ist es auch möglich, sogenannte „Bewegungsprofile" von dir zu erstellen, also z. B. zu erfahren, wo du dich den lieben langen Tag herumgetrieben hast.

Solche Profile von fremden Personen zu erstellen, ist zwar gesetzlich verboten. Es gibt aber Anbieter, die es Eltern erlauben, den Standort ihres Kindes (bzw. des Telefons ihres Kindes) zu orten. Eltern, die zu solchen Maßnahmen greifen, tun dies in aller Regel nur aus Besorgnis um ihre Kinder. Dennoch gehören in einer freiheitlichen Gesellschaft auch die Vorbereitung auf ein selbstbestimmtes Leben und das Vertrauen auf Mündigkeit und Verantwortung zur Erziehung der Heranwachsenden dazu. Außerdem ist ein Missbrauch solcher Ortungsanwendungen außerhalb von Eltern-Kind-Kontrollen nicht auszuschließen.

Sollten deine Eltern diese Art der Überwachung in Erwägung ziehen oder tatsächlich schon vornehmen, dann sprich mit ihnen über ihre Gründe und deine Einstellung zu dieser Maßnahme. Der Standort eines eingeschalteten Smartphones kann durch den Mobilfunknetzbetreiber bis auf unter 100 Meter genau bestimmt werden. Die Erlaubnis zu einer solchen Ortung ist allerdings gesetzlich stark eingeschränkt.

Bei Smartphones besteht dagegen viel eher die Gefahr, dass im Gerät verfügbare, sehr genaue Ortungstechniken wie GPS von einigen Apps missbraucht werden. Du solltest dir bei jeder App überlegen, ob diese die Ortungsfunktion wirklich benötigt. Bei jedem Smartphone kannst du einzelnen Apps verbieten, die Ortungsfunktionen zu nutzen. Bedenke bei Apps für soziale Netzwerke vorher, ob du solche Ortungsfunktionen wirklich nutzen möchtest und wem du mitteilen willst, wo du gerade bist. Denn auch durch solche Programme (z. B. Facebook Places, Foursquare oder durch den Live-

Standort bei WhatsApp) entsteht ein Bewegungsprofil, das ggf. vom Anbieter des Netzwerkes oder auch von manchen „Freundinnen“ und „Freunden“ missbraucht werden kann.

Tipp: Schalte dein Smartphone ab, wenn du es nicht bei dir führst, oder verwende zumindest eine PIN-geschützte Sperrfunktion. Sei vorsichtig bei eigenartigen SMS-Nachrichten mit Inhalten, die dir merkwürdig vorkommen, wie Meldungen über durchgeführte Ortungen, Anmeldebestätigungen oder Freischaltcodes. Erlaube nur Apps den Zugriff auf die Ortungsfunktion, denen du vertraust und die dies aus nachvollziehbaren Gründen benötigen.

8. Lauschangriff

Das Abhören von Handy-Gesprächen ist genauso wie das Abhören von Festnetztelefonaten prinzipiell möglich. Eine solche Maßnahme verstößt aber gegen deine Grundrechte. Zu Telefonabhörmaßnahmen durch den Mobilfunkanbieter kommt es in aller Regel nur im Rahmen von Ermittlungen der Polizei oder anderer staatlicher Sicherheitsbehörden bei Verdacht auf eine besonders schwere Straftat.

Smartphones lassen sich zudem so manipulieren, dass mit ihnen Räume abgehört werden können, in denen sie sich befinden. So etwas erfordert allerdings aufwendige Veränderungen am Telefon oder das Installieren einer „Schnüffelsoftware“. Mit einer solchen Software könnten auch deine Smartphone-Gespräche abgehört und deine Nachrichten mitgelesen werden. Achte daher auch hier auf die Hinweise zum Schutz vor Viren und anderer Schadsoftware.

Du darfst auch selbst keine heimlichen Ton- oder Bildaufnahmen machen, z. B. von Mitschülerinnen/Mitschülern und Lehrerinnen/Lehrern im Unterricht oder in der Pause. Sie sind nicht erlaubt, weil sie die Grundrechte der Betroffenen beeinträchtigen.

PRIVATSPHÄRE: Natürlich musst du aufpassen, dass deine Daten möglichst auch bei dir bleiben – achte z. B. darauf, wer zuhört, wenn du telefonierst. Umgekehrt folgt daraus aber auch, dass du selbst deine Mitmenschen nicht unerlaubt ausspionieren darfst. Auch heimliche Tonaufnahmen, z. B. im Klassenraum, sind verboten.

9. Unverschlüsselte WLAN-Hotspots

Jede/r kann deinen Datenverkehr mitschneiden und auslesen, sofern er nicht gesondert verschlüsselt ist. Eine gesonderte Verschlüsselung ist z. B. durch „https://" erkennbar. Allerdings können neugierige Dritte selbst dann zumindest noch mitlesen, zu welchen Servern (wikipedia.org., facebook.com usw.) du dich verbindest (Metadaten).

Hier noch einige Hinweise, die dir den Umgang mit WLAN-Hotspots erleichtern:

- Das Betriebssystem macht meist kenntlich, welche WLANs verschlüsselt und welche unverschlüsselt sind.
- Viele Chat-Apps, wie z. B. Threema und Signal, verschlüsseln von sich aus alle Nachrichten.
- Wenn du dich mit dem WLAN verbinden kannst und dann auf eine Webseite weitergeleitet wirst, wo du Nutzungsbedingungen akzeptieren und evtl. Nutzernamen und/oder Passwort eingeben musst, ist das WLAN meist **nicht** verschlüsselt.

Tipp: **Stelle die E-Mail-App so ein, dass E-Mails nur über verschlüsselte Verbindungen abgerufen und verschickt werden.**

10. Fotos auf sozialen Netzwerken

Überlege dir genau, ob deine privaten Fotos wirklich für die Öffentlichkeit bestimmt sein sollen. Vor allem solltest du niemals Fotos von Freundinnen und Freunden veröffentlichen oder sie auf Fotos markieren, ohne vorher gefragt zu haben.

Erst recht nicht, wenn die Fotos öffentlich sichtbar und nicht nur einem bestimmten Personenkreis zugänglich sind. Denn es ist nicht erlaubt, mit einem Smartphone einzelne Menschen ohne deren Einwilligung zu fotografieren, zu filmen oder diese Fotos ohne die Zustimmung der fotografierten Personen zu veröffentlichen.

Bevor du Fotos von Freundinnen und Freunden auf sozialen Netzwerken hochlädst, solltest du mit deinen Eltern sprechen, ob das erlaubt ist. Deine Freundinnen und Freunde sollten gegebenenfalls auch erst mit ihren Eltern reden, bevor sie dir die Zustimmung geben.

Tipp: **Wenn du nicht auf Fotos markiert werden willst, solltest du in den Einstellungen des sozialen Netzwerks nachschauen, ob man festlegen kann, dass man nicht markiert wird. Gegebenenfalls kann man auch einschränken, durch wen man markiert werden kann.**

11. Mobile Apps und Fake-Apps

Mobile Apps (meist kurz Apps genannt) gibt es für verschiedene Bereiche. Der Großteil davon ist kostenlos, ein kleinerer Teil muss, für meist geringe Beträge, im jeweiligen App Store oder Play Store gekauft werden.

Achte darauf, dass du die richtige App installierst. Manchmal gibt es nachgemachte Apps, die unerwünschte Funktionen beinhalten. Das sind Apps, die keine Funktionen haben, aber Geld kosten oder heimlich die Nutzer ausspionieren (Fake-Apps).

In den letzten Jahren sind Gefahren durch selbst installierte Smartphone-Apps relevanter geworden. Bitte bedenke vor der Installation einer neuen App, dass diese meist nicht vom Hersteller des Smartphones, sondern aus mitunter zweifelhaften Quellen stammt. Es gibt mittlerweile unzählige Beispiele für Apps, die persönliche Daten an den Hersteller der App weitergeben. Beispielsweise wird sehr oft der Aufenthaltsort ermittelt oder es werden die Telefonbucheinträge weitergegeben (z. B. bei der Smartphone-App von Facebook).

Vor der Installation einer App solltest du dich daher erkundigen, wer der Hersteller ist, ob die App vom Shop-Betreiber bzw. Smartphone-Hersteller geprüft wurde oder ob sich bei den Bewertungen durch andere Nutzer/innen Hinweise auf einen unseriösen Anbieter finden lassen. Bei der Installation sollte man genau überlegen, ob eine App auch wirklich alle Daten benötigt, die abgefragt werden oder auf die die App Zugriff einfordert.

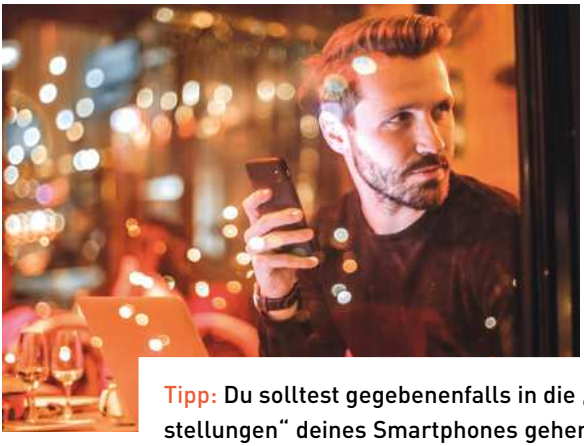
Tipp: **Stimme nicht der Installation von Apps zu, deren Herkunft und Zweck du nicht sicher kennst – selbst wenn sie von einem Bekannten geschickt oder empfohlen wurden. Schau vorher nach, wie viele Downloads die App schon hat und wie sie bewertet wird.**

12. App-Zugriffsrechte

Die Berechtigungen, die eine App beansprucht, werden häufig ignoriert. Dabei greifen viele Anwendungen Daten vom Mobilgerät ab, die ihnen nicht zustehen – auch besonders schützenswerte sensitive Daten. Vor dem Installieren von Apps solltest du die App-Zugriffsrechte im App Store/Play Store kontrollieren.

Benötigt das neue Spiel tatsächlich Zugriff auf das Adressbuch? Braucht eine Fitness-App wirklich Zugriff auf die Kamera? Erklärt der Hersteller irgendwo (z. B. auf seiner Webseite), wofür die App welche Zugriffsrechte benötigt?

Wie übergriffig eine App sein darf, solltest du als Smartphone-Nutzer/in vor der Installation gut überlegen. Du kannst gegebenenfalls auch einen Blick in die Datenschutzerklärung werfen. Dort sollte erklärt werden, welche Daten der Anbieter der App verarbeitet und was er damit macht. Meistens kann man einzelne Zugriffsrechte auch nach der Installation wieder entziehen.



Tipp: **Du solltest gegebenenfalls in die „Einstellungen“ deines Smartphones gehen und unerwünschte Funktionen deaktivieren.**

13. AppStore des Plattformanbieters

Üblicherweise werden die Apps über einen zentralen, vom Plattformbetreiber kontrollierten Dienst, den sogenannten AppStore, installiert. Der AppStore ermöglicht dem Plattformbetreiber die Kontrolle über die auf der Plattform eingesetzten Anwendungen. Dies kann vorteilhaft sein, da die Apps vor Veröffentlichung geprüft und so zumindest prinzipiell gefährliche und besonders datenhungrige Anwendungen von der Plattform ferngehalten werden.

Allerdings erfährt der Plattformbetreiber so auch besonders viel über die Nutzenden.

Eine Möglichkeit, das Wissen des Plattformanbieters zu beschränken, wäre die Anmeldung unter einem ausgedachten Namen. Mittlerweile ist allerdings i. d. R. die Angabe der Mobiltelefonnummer erforderlich, um eine höhere Sicherheit gegen Kontodiebstahl zu erreichen.

Tipp: **Für den Kauf von Apps oder Musik solltest du keine Kreditkarte benutzen, sondern auf die Guthabenkarten der Anbieter zurückgreifen, die man überall anonym kaufen kann.**

14. Entsperrcode/PIN

Jedes Smartphone hat eine Sperrfunktion, die es vor unbefugtem Zugriff schützt. Du solltest einen Entsperrcode für dein Smartphone festlegen. So kommen fremde Menschen nicht gleich an deine Daten, wenn du das Smartphone verlierst oder es gestohlen wird.

Es empfiehlt sich, dafür eine PIN oder ein Passwort festzulegen. Allerdings helfen einfache PINs wie „1111“ nicht viel. Eine kompliziertere Zahlenkombination sollte es schon sein. Wenn es möglich ist, kannst du auch eine „Reserve-PIN“ einstellen, die benötigt wird, wenn du die PIN zehnmal falsch eingegeben hast. Die „Reserve-PIN“ sollte nach Möglichkeit länger sein. Gegebenenfalls kannst du sie aufschreiben und gut zu Hause verwahren (aber nicht in deinem Portemonnaie).

Tipp: **„Wisch-Codes“ sind nicht sicher. Man kann sie oft auf dem Bildschirm erkennen, wenn man das Smartphone gegen das Licht hält.**

15. Updates

Täglich werden neue Sicherheitslücken aufgedeckt. Die Hersteller von Smartphones veröffentlichen Updates, die die Sicherheitslücken schließen sollen. Damit dein Smartphone geschützt ist, solltest du Updates von Apps und vom Betriebssystem immer so schnell wie möglich installieren.

Tipp: **Wenn möglich, solltest du die Updates herunterladen, solange du mit einem WLAN verbunden bist. So spart man mobiles Datenvolumen.**

Mehr Informationen im Internet

www.datenschutz-berlin.de
www.data-kids.de
www.datenschutz.de
www.handy-sektor.de
www.stiftung-warentest.de

www.datenschutz-berlin.de