Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Smartphone, Tablet und Co sicher nutzen

9 Tipps zum Umgang mit mobilen Geräten

Sicherheit für Smartphone & Co

Wir nutzen unsere mobilen Geräte für eine Vielzahl von Aktivitäten – zum Beispiel für die Teilnahme an sozialen Netzwerken, zum Online-Einkauf, für Bankgeschäfte und zum Surfen im Internet. Doch schlecht gesicherte Geräte bieten Angreifern beispielsweise die Möglichkeit, sensible Informationen auszuspähen.

Folgende Vorsichtsmaßnahmen helfen, Ihre Smartphones, Tablets und andere mobile Geräte sowie die darauf befindlichen Daten vor Angriffen durch Cyberkriminelle zu schützen.

Sicher unterwegs mit Smartphone & Co

Basisschutz leicht gemacht

Hier haben wir die wichtigsten Tipps zum sicheren Umgang mit Smartphones, Tablets und anderen mobilen Geräten für Sie zusammengefasst. Ausführliche Informationen finden Sie auf den nachfolgenden Seiten dieser Broschüre.

1. Halten Sie Apps und Betriebssystem Ihres Geräts mit regelmäßigen Updates auf dem neuesten Stand.
2. Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die erteilten Zugriffsberechtigungen regelmäßig.
3. Nutzen Sie Sperrcodes und Passwörter, um Ihre Geräte und Daten zu schützen. Die Bildschirmsperre Ihres Telefons und die PIN-Abfrage Ihrer SIM-Karte sollten stets aktiviert sein.

4. Deaktivieren Sie Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen.
5. Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht und achten Sie auf verschlüsselte Verbindungen (https).
6. Lassen Sie Ihr Gerät niemals unbeobachtet, um es vor unbefugten Zugriffen und Manipulation zu schützen.
7. Prüfen Sie Nummern, die Sie nicht kennen, vor dem Rückruf. Hilfe gibt es auf www.bundesnetzagentur.de/Rufnummernmissbrauch.
8. Sichern Sie die Daten auf Ihren mobilen Geräten regelmäßig und verschlüsseln Sie sensible Daten.
9. Löschen und formatieren Sie alle Speicher, bevor Sie ein Gerät verkaufen, weitergeben oder entsorgen und vergessen Sie nicht, die SIM-Karte(n) und zusätzliche Speicherkarten zu entfernen.

1

Sorgen Sie für einen Basisschutz

Vergewissern Sie sich in den Einstellungen Ihres Geräts, dass die vorhandenen Sicherheitsfunktionen eingeschaltet sind. Dazu gehören beispielsweise die Bildschirm-Sperre oder die PIN-Abfrage beim Starten des Geräts. Viele Angriffe zielen auf Sicherheitslücken in der Software, die erst durch ein Update der Hersteller geschlossen werden – dazu zählen vor allem Fehler im Betriebssystem und in den Anwendungen. Aktivieren Sie die automatische Update-Funktion oder kontrollieren Sie regelmäßig, ob Aktualisierungen verfügbar sind. So sorgen Sie dafür, dass Ihr Gerät immer auf dem neuesten Stand bleibt.

2

Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die Zugriffsrechte

Installieren Sie Apps nur aus seriösen Quellen und laden Sie nur Anwendungen herunter, die Sie tatsächlich benötigen. Meiden Sie Quellen, bei denen Sie Zweifel an der Seriosität haben. Installieren Sie beispielsweise keine App, die Ihnen unverlangt als E-Mail-Anhang zugesandt oder als Download-Link angeboten wird. Auch Apps, die angeblich mehr können als ‚Originale', sind verdächtig. Wenn Sie Zweifel an der Vertrauenswürdigkeit einer App beziehungsweise eines App-Entwicklers haben, reicht oft eine Suche im Internet aus, um sich über den Anbieter zu informieren. Achten Sie dabei etwa auf Erfahrungsberichte, Bewertungen und Tests von etablierten Online-Portalen. Installieren Sie Updates zeitnah. Deinstallieren Sie Apps, die Sie nicht mehr nutzen.

Viele Apps räumen sich ohne erkennbaren Grund umfassende Zugriffsrechte ein, um beispielsweise Standortdaten, das Adressbuch oder den Telefonstatus auszulesen. Dies ist aber nicht bei jeder App notwendig. Prüfen Sie vorab kritisch, ob die Zugriffsrechte für das Funktionieren der Anwendung wirklich notwendig sind. Im Zweifelsfall ist es besser, die App nicht zu installieren. Sie haben zudem die Möglichkeit, einer bereits installierten App Zugriffsrechte über die Einstellungen des Smartphones wieder zu entziehen.

Wichtig: Das Update einer App kann dazu führen, dass auch Änderungen oder Erweiterungen der Zugriffsrechte erfolgen und eine App beispielsweise plötzlich doch Zugriff auf das Adressbuch erhält. Prüfen Sie daher regelmäßig die erteilten Zugriffsrechte und wägen Sie ab, ob Sie die App unter den geänderten Bedingungen weiterhin nutzen möchten.

3

Nutzen Sie Sperrcodes und Passwörter

Achten Sie darauf, dass die PIN Ihrer SIM-Karte und die Bildschirmsperre Ihres Telefons stets aktiviert sind. Auch sensible Anwendungen, wie Onlinebanking sowie Online-Käufe per App sollten möglichst mit einer PIN oder einem Passwort geschützt werden. Ersetzen Sie voreingestellte Sperrcodes durch eine eigene Kombination. Achten Sie auf Zahlenkombinationen, die nicht leicht zu erraten sind und vermeiden Sie logische Abfolgen wie 12345 oder Geburtstage. Es besteht zum Teil auch die Möglichkeit, Geräte per Fingerabdruck oder Gesichtserkennung zu entsperren.

Bequemer, aber nicht ganz so sicher: Das Gerät lässt sich über das Betriebssystem mit einer Mustersperre entriegeln. Dabei ziehen Sie mit dem Finger eine bestimmte Spur über den Bildschirm. Achten Sie dabei darauf, dass Wischspuren Ihres Fingers nicht das Muster verraten, indem Sie den Bildschirm Ihres Geräts regelmäßig reinigen.

Ob PIN oder Muster: Sorgen Sie für einen Sichtschutz bei der Eingabe, damit niemand Ihre Kombination ausspähen kann.

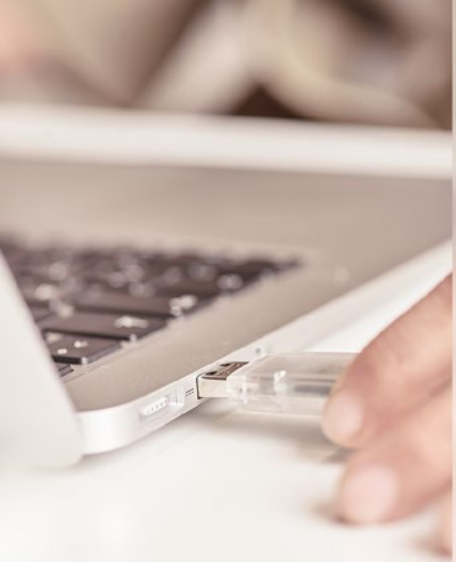
4

Aktivieren Sie Schnittstellen nur bei Bedarf

Kommen mehrere Umstände zusammen, kann ein räumlich naher Angreifer eventuell Datenübertragungen mitlesen. Deshalb kann es ratsam sein, Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, in den Einstellungen Ihres Geräts zu deaktivieren, wenn Sie diese nicht benötigen. Hierdurch schonen Sie zudem den Akku.

Wenn Sie den WLAN-Empfang am Gerät und die GPS-Funktion ausschalten, wird die Positionsbestimmung ungenauer. Der Aufenthaltsort von Mobilfunkgeräten kann jedoch dennoch von den Betreibern der Funknetzwerke und zum Teil auch von App-Anbietern ermittelt werden.

Trotzdem sollten Sie prinzipiell mit der Weitergabe Ihrer Ortsangaben sehr zurückhaltend sein. Cyberkriminelle könnten Ihren Aufenthaltsort ermitteln, weitere persönliche Informationen über Sie herausfinden oder Informationen wie beispielsweise zum Urlaub nutzen, um einen Diebstahl zu planen. Nutzen Sie etwa Navigationsdienste nur dann, wenn es notwendig ist (mehr dazu unter Punkt 6). Löschen Sie mit entsprechenden Apps die Ortsangaben aus den Metadaten der Fotos, die Sie ins Internet laden. Bei Metadaten handelt es sich um alle Informationen (Datum, Ort der Aufnahme etc.), die zusätzlich zum Foto automatisch von Ihrem Gerät bei der Aufnahme gespeichert werden.



Für Hardwareschnittstellen wie USB gilt: Schließen Sie Ihr mobiles Gerät zum Aufladen oder Übertragen von Dateien nur an Rechner an, deren Benutzer Sie vertrauen. Denn auch auf diesem Weg können Schadprogramme übertragen werden. In den Einstellungen Ihres mobilen Gerätes können Sie zudem festlegen, ob beim Anschließen per USB überhaupt eine Datenübertragung erfolgen oder Ihr Gerät lediglich aufgeladen werden soll. Nutzen Sie zum Aufladen möglichst nur das mit dem Gerät gelieferte Netzteil.

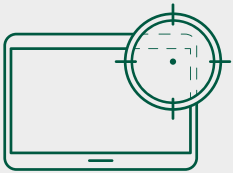
5

Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht

Öffentliche Hotspots, beispielsweise ein WLAN in einem Café oder am Flughafen, verwenden für die Funkstrecke zum Router oft kein Kennwort oder ein für alle Teilnehmer und Teilnehmerinnen gemeinsames Kennwort. Damit besteht das Risiko, dass Dritte Ihre Daten mitlesen können. Umso wichtiger ist es, dass die Kommunikation zwischen Ihrem Endgerät und dem Internetserver verschlüsselt abläuft. Diese sichere Kommunikation wird über das https-Protokoll hergestellt, im Browser erkennbar durch das Schlosssymbol in der Adresszeile. Fehlt dieses oder wird Ihnen eine Warnung über eine unsichere Verbindung angezeigt, besteht keine sichere Verbindung. In diesem Fall sollten Sie in öffentlichen WLAN misstrauisch sein und auf die Übertragung von sensiblen Daten verzichten.

Denken Sie daran, dass neben dem Browser auch Apps Datenverbindungen ins Internet aufbauen. Auch diese könnten unverschlüsselt sein.
Sollten Sie mit Ihrem Mobilfunkgerät einen eigenen Hotspot für andere Nutzer einrichten, ist auch bei dieser Funktion Vorsicht geboten. Beim sogenannten Tethering stellt das Smartphone für andere Geräte einen Hotspot dar, so dass diese über das erzeugte WLAN ins Internet gelangen können. Eine solche Verbindung sollte immer mit einem guten Passwort abgesichert sein, da jeder, der das Passwort kennt oder erraten kann, über die Mobilfunkverbindung des Hotspot-Betreibers ins Internet kommt. Meist ist es möglich, den Zugang einzelner Geräte zu filtern. Dabei muss ein Gerät beim ersten Kontakt zusätzlich bestätigt werden. Schalten Sie den Hotspot wieder ab, wenn er nicht mehr benötigt wird.

6



Lassen Sie Ihr Gerät nicht aus den Augen

Um Ihre Geräte vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Smartphones und Tablets niemals unbeobachtet lassen.

Verlorene oder gestohlene Geräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. Einige Gerätehersteller bieten eigene Apps an, mit denen ein gestohlenes Gerät wiedergefunden werden kann.

Wichtig: Achten Sie auf einen vertrauenswürdigen Anbieter für solche Apps.

Um Ihr Smartphone im Falle eines Verlustes zu sperren, reicht bei vielen solcher Apps der Versand einer vorher definierten Nachricht mit dem richtigen Befehlscode an die eigene Handynummer. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht oder nicht mehr aufzurufen. Daneben besteht auch die Möglichkeit, ein Smartphone oder mobilfunkfähiges Tablet anhand seiner IMEI-Nummer – einer eindeutigen Seriennummer – unter bestimmten Bedingungen über den Netzbetreiber orten zu lassen. Notieren Sie die Nummer im Vorfeld. Die IMEI Ihres Gerätes erhalten Sie über die Einstellungen-App oder mit dem Tastencode *#06#. Sie befindet sich vereinzelt auch auf der Packung oder der Rechnung Ihres Anbieters. Sie gilt als Eigentumsbeweis im Falle eines Diebstahls.

Nach erfolgter Sperrung des Geräts sollten Sie auch die SIM-Karte bei Ihrem Anbieter sperren lassen. Bitte beachten Sie die richtige Reihenfolge. Ist die SIM-Karte deaktiviert, lässt sich auch kein Sperrcode mehr empfangen.

Installieren Sie nur solche Sicherheitslösungen für mobile Geräte (beispielsweise Ortung, Remote-Sperrung, Verschlüsselung, Antiviren-App), die Ihrem konkreten Bedarf entsprechen und wägen Sie ab, ob Sie im Gegenzug hierfür bereit sind, beispielsweise Standortangaben dauerhaft zu aktivieren.

7

Prüfen Sie Nummern, die Sie nicht kennen, vor dem Rückruf

Seien Sie bei Anrufen mit unbekannter oder unterdrückter Nummer misstrauisch. Einige Betrüger versuchen, telefonisch Passwörter oder PINs abzufragen. Rufen Sie niemals ungeprüft Nummern zurück, die Ihnen unbekannt sind. Aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf Rufnummern zu Mehrwertdiensten, die im Falle eines Rückrufs hohe Kosten auf Ihrer Telefonrechnung verursachen können, durch Ihren Netzbetreiber für ausgehende Anrufe sperren.
www.bundesnetzagentur.de/Rufnummernmissbrauch

8

Schützen Sie Ihre Daten

Bei modernen Smartphones ist die Verschlüsselung des internen Speichers voreingestellt. Die Daten auf einer zusätzlich eingesetzten SD-Karte sind meist nicht von der Speicherverschlüsselung des Geräts geschützt. Fotos und andere Daten können so durch Herausnehmen der Karte extern gelesen werden.

Um eine SD-Karte zu verschlüsseln, muss diese „als intern formatiert“ werden. Wird die SD-Karte als portabler Speicher formatiert, werden die Daten auf der Karte unverschlüsselt gespeichert.

Sichern Sie die Daten Ihrer mobilen Geräte regelmäßig auf einem geeigneten Backup-Medium – das können beispielsweise USB- (siehe dazu Punkt 4) oder auch Online-Speicher sein.

Wichtig: Eine als intern formatierte SD-Karte können Sie außerhalb Ihres Smartphones nicht lesen.

9

Bereinigen Sie alle Speicher, bevor Sie das Gerät verkaufen oder entsorgen

Wenn Sie Ihr Handy weiterverkaufen, verschenken oder entsorgen, achten Sie darauf, den Speicher Ihres Gerätes zu löschen. Andernfalls können Datenspuren verbleiben, die den neuen Besitzern oder Kriminellen möglicherweise private Informationen über Sie geben. Durch das Rücksetzen des Gerätes in den Werkszustand werden alle Daten der internen Speicher unbrauchbar gemacht. Den Menüpunkt dazu finden Sie in den Einstellungen.

Denken Sie daran, zusätzliche Speichermedien wie eine externe SD-Karte zu entfernen. Eine solche SD-Karte kann mit Hilfe eines Lesegerätes am PC sicher gelöscht werden. Auch die SIM-Karte sollten Sie grundsätzlich entfernen und vernichten – falls Sie diese nicht weiterverwenden wollen. Vergessen Sie nicht, gegebenenfalls den zugehörigen Vertrag zu kündigen.

Weiterführende Informationen

- Sie nutzen mit Ihrem Smartphone oder Tablet Cloud-Dienste? Auch hier haben wir Empfehlungen zum Thema Sicherheit. bsi.bund.de/cloud-sicherheit
- Wenn Sie die Möglichkeit haben, sich über ein Virtuelles Privates Netzwerk (VPN) mit Ihrem Heimnetz bzw. dessen Router zu verbinden, können Sie auch in öffentlichen WLAN-Hotspots genauso sicher unterwegs sein, wie Sie es von zu Hause gewohnt sind. Ein VPN ist eine besonders gesicherte Verbindung zwischen zwei Punkten. Dabei wird ein Tunnel aufgebaut, z. B. von einem Smartphone durch das öffentliche Internet zu Ihrem Heimnetz, von wo aus Sie dann Ihren eigenen Internetzugang nutzen können. Moderne Router bieten oft die Möglichkeit, ein VPN einzurichten. bsi.bund.de/vpn

Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Als unabhängige und neutrale Anlaufstelle bietet es Ihnen für einen sicheren digitalen Alltag umfangreiche Informationen.

IMPRESSUM

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsquelle:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi_bund
Service-Center: +49 (0) 800 274 1000

Stand: März 2021
Bilder: © GettyImages
Layout und Gestaltung: Faktor 3 AG

Artikelnummer: BSI-IFB 21/251