Bundesamt
für Sicherheit in der
Informationstechnik

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

Sicher unterwegs mit Smartphone, Tablet & Co

Basisschutz leicht gemacht

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, Smartphones, Tablets & Co und die darauf befindlichen Daten vor Angriffen durch Cyberkriminelle zu schützen.

1 Sorgen Sie für einen Basisschutz

Vergewissern Sie sich in den Sicherheitseinstellungen Ihres Geräts, dass die vorhandenen Sicherheitsfunktionen eingeschaltet sind. Aktualisieren Sie Apps und Betriebssystem umgehend, sobald Updates erhältlich sind. Prüfen Sie regelmäßig, ob weitere Aktualisierungen verfügbar sind. Viele Angriffe zielen auf bekannte Schwachstellen, die erst durch Updates der Hersteller geschlossen werden. Aktivieren Sie daher die automatische Update-Funktion, damit Sicherheitsupdates direkt nach dem Erscheinen eingespielt werden. Kontrollieren Sie, ob mit dem Update erweiterte Berechtigungen verbunden sind (Tipp 2).

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

Installieren Sie nur Apps, die Sie tatsächlich benötigen. Haben Sie Zweifel an der Vertrauenswürdigkeit einer Anwendung, reicht eine kurze Suche im Internet meistens aus, um sich über den Anbieter zu informieren. Entfernen Sie Anwendungen, die Sie nicht mehr nutzen. Denn jede zusätzliche App ist eine mögliche Sicherheitslücke. Veraltete Apps sollten durch solche ersetzt werden, für die weiterhin Updates bereitgestellt werden.

Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind, und nutzen Sie die Möglichkeit, Zugriffsrechte zu entziehen. Im Zweifelsfall ist es besser, die App nicht zu installieren.

Wichtig: Durch Updates können auch Änderungen oder Erweiterungen der Zugriffsberechtigungen erfolgen. Prüfen Sie daher regelmäßig die erteilten Zugriffsberechtigungen und wägen Sie ab, ob Sie die App unter den geänderten Bedingungen weiterhin nutzen möchten.

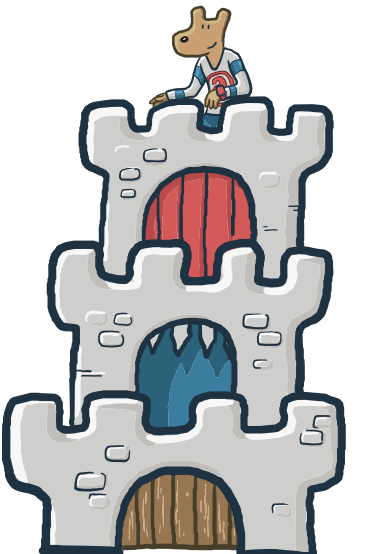
Vermeiden Sie „Sideloading“ – also das Installieren von Apps aus einer anderen Quelle als den offiziellen App-Stores – so weit wie möglich und überprüfen Sie andernfalls die Quellen.

Nutzen Sie Sperrcodes und Passwörter

Achten Sie darauf, dass die SIM/USIM-PIN und die Bildschirmsperre Ihres Telefons stets aktiviert sind. Auch sensible Anwendungen, wie Onlinebanking und App-Käufe, sollten möglichst mit einer PIN oder einem Passwort geschützt werden. Ersetzen Sie voreingestellte Codes durch eine eigene Kombination.

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. Das bietet zwar weniger Sicherheit, ist aber schneller ausführbar als das Eintippen einer Zahlenkombination. Achten Sie dabei darauf, dass Wischspuren nicht das Muster verraten.

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



Aktivieren Sie Schnittstellen nur bei Bedarf

Deaktivieren Sie Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen. So ist Ihr Gerät weniger anfällig für Cyber-Angriffe – und Sie gewinnen Akku-Laufzeit.

Wenn Sie Ihr WLAN und die GPS-Funktion ausschalten, wird auch die mögliche Positionsbestimmung ungenauer. Der Aufenthaltsort von Mobilfunkgeräten kann von den Betreibern der Funknetzwerke und zum Teil auch von App-Anbietern jederzeit ermittelt werden. Trotzdem sollten Sie prinzipiell mit der Weitergabe Ihrer Ortsangaben sehr zurückhaltend sein – also etwa Lokalisierungsdienste meiden und Ortsangaben aus den Metadaten der Fotos löschen, die Sie ins Internet laden.

Auch für USB gilt: Schließen Sie Ihr mobiles Gerät nur an vertrauenswürdige Rechner an, denn auch auf diesem Weg kann Malware übertragen werden. Gleiches gilt für die Stromzufuhr. Auch hier ist auf eine vertrauenswürdige USB-Verbindung zu achten.

Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht

In öffentlichen WLAN-Netzen, etwa im Café oder am Flughafen, ist der Zugang zum Internet meist unverschlüsselt. Hier ist erhöhte Vorsicht geboten. Nutzen Sie, sofern möglich, eine gesicherte Verbindung, die Sie am Kürzel https in der Adresszeile erkennen. Anwendungen wie Onlinebanking sollten Sie in offenen Netzwerken nur über eine sichere Verbindung nutzen. Verwenden Sie dafür eine App, die ein Virtuelles Privates Netzwerk (VPN) aufbauen kann. Moderne Router bieten oft die Möglichkeit, ein VPN einzurichten. Sie können dann Ihr Smartphone an Ihrem Router registrieren und so über Ihr Heimnetz gesichert im Internet surfen. Ist Ihnen das zu riskant, verzichten Sie auf sensible Anwendungen in offenen Netzwerken.

Mit der Tethering-Funktion können andere Anwenderinnen oder Anwender Ihre Internetverbindung nutzen. Ihr Gerät wird so zu einem Hotspot. Nutzen Sie möglichst das WLAN-Sicherheitsprotokoll WPA3 oder, wenn dieses noch nicht unterstützt wird, bis auf Weiteres WPA2 und richten Sie für den Hotspot ein sicheres Passwort ein. Teilen Sie dieses Passwort nur vertrauenswürdigen Personen mit und beenden Sie die Hotspot-Funktion, wenn Sie sie nicht mehr benötigen.

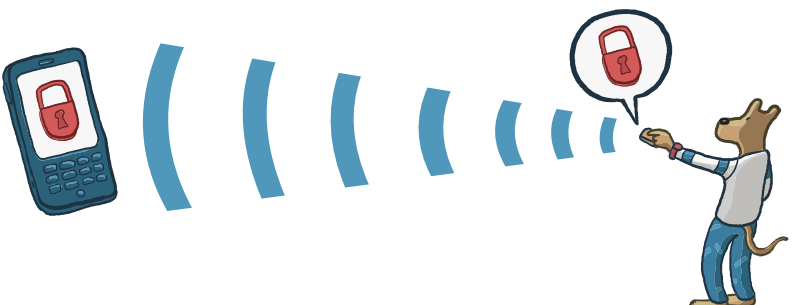
Lassen Sie Ihr Gerät nicht aus den Augen

Um das Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Ihr Smartphone niemals unbeobachtet lassen oder verleihen.

Verlorene oder gestohlene Geräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. Hier reicht meist der Versand einer vorher definierten Nachricht mit dem richtigen Befehlscode an die eigene Nummer. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht oder nicht mehr aufzurufen. Doch Vorsicht: Derartige Befehle können ebenso von böswilligen Dritten genutzt werden. Achten Sie auch hier auf einen vertrauenswürdigen Anbieter.

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 Mobilgeräte (beispielsweise Ortung, Remote-Sperrung, Verschlüsselung, AV-App), die Ihrem konkreten Bedarf entsprechen.



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

Rufen Sie Nummern, die Ihnen unbekannt sind, nicht ungeprüft zurück. Aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf Rufnummern zu Mehrwertdiensten durch Ihren Netzbetreiber für ausgehende Anrufe sperren.

www.bundesnetzagentur.de/Rufnummernmissbrauch

Schützen Sie Ihre Daten

Nutzen Sie die Funktionen zur Datenverschlüsselung – wenn vorhanden – oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware. Dies gilt auch für die Daten, die auf einer zusätzlichen SD-Karte gespeichert sind.

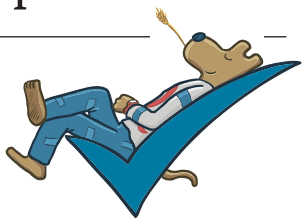
Sichern Sie die Daten auf Ihren mobilen Geräten regelmäßig auf einem geeigneten Backup-Medium.

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

Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, dann sollten Sie bedenken, dass Datenspuren verbleiben können, wenn nicht vorher alle Datenspeicher überschrieben wurden.

Denken Sie daran, zusätzliche Speichermedien wie eine externe SD-Karte zu entfernen. Auch die SIM-Karte sollten Sie grundsätzlich entfernen und – falls Sie diese nicht weiter verwenden wollen – vernichten. Vergessen Sie nicht, gegebenenfalls den zugehörigen Vertrag zu kündigen.

Sicher unterwegs mit Smartphone & Co



Basisschutz leicht gemacht

- Sorgen Sie für einen Basisschutz. Vergewissern Sie sich, dass die vorhandenen Sicherheitseinstellungen Ihres Geräts eingeschaltet sind und aktualisieren Sie Apps und Betriebssystem umgehend.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die geforderten Zugriffsberechtigungen.
- Nutzen Sie Sperrcodes und Passwörter. SIM/USIM-PIN und die Bildschirmsperre Ihres Telefons sollten stets aktiviert sein. Schützen Sie auch sensible Anwendungen mit einer PIN oder einem Passwort.

Deaktivieren Sie Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen. Die Erstellung von Bewegungsprofilen wird erschwert, wenn Sie die GPS- und die WLAN-Funktion ausschalten.

Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.

Lassen Sie Ihr Gerät niemals unbeobachtet und verleihen Sie es nicht, um es vor unbefugten Zugriffen und Manipulation zu schützen.

Prüfen Sie Nummern, die Sie nicht kennen, vor dem Rückruf. Hilfe gibt es auf www.bundesnetzagentur.de/Rufnummernmissbrauch.

Sichern Sie die Daten auf Ihren mobilen Geräten regelmäßig und verschlüsseln Sie sensible Daten.

Löschen Sie alle Speicher, bevor Sie das Gerät verkaufen oder entsorgen und vergessen Sie nicht, die SIM-Karte zu entfernen.

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. Mit dem Informationsangebot „BSI für Bürger“ bietet es eine unabhängige und neutrale Anlaufstelle zu Fragen der Informations- und Cyber-Sicherheit.

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: mail@bsi-fuer-buerger.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger
Service-Center: +49 (0) 800 274 1000

Stand
Juli 2019

Illustrationen
Leo Leowald · www.leowald.de

Artikelnummer
BSI-IFB 19/251