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

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

Sicherheit für Smartphone & Co

Wir nutzen unsere mobilen Geräte für eine Vielzahl von Aktivitäten – für die Teilnahme an sozialen Netzwerken, zum Online-Einkauf, für Bankgeschäfte und zum Surfen im Internet.

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

Sorgen Sie für einen Basisschutz

Vergewissern Sie sich, dass die vorhandenen Sicherheitseinstellungen Ihres Geräts eingeschaltet sind. Aktualisieren Sie Apps und Betriebssystem umgehend, sobald Aktualisierungen erhältlich 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 aber auch hier, welche Erweiterungen der Berechtigungen mit dem Update verbunden sind (Tipp 8).

Prüfen Sie unbekannte Nummern vor dem Rückruf

Rufen Sie unbekannte Rufnummern nicht zurück. Aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf unerwünschte Rufnummern zu Mehrwertdiensten von Ihrem Netzbetreiber sperren.

www.bundesnetzagentur.de/Rufnummernmissbrauch

3 Verschlüsseln Sie vertrauliche Gespräche

Mobiles Telefonieren ist nicht abhörsicher. Wenn Sie schützenswerte oder gar geheime Informationen austauschen wollen, weichen Sie besser auf verschlüsselte Kommunikation aus. Beachten Sie auch Vorgaben Ihres Arbeitgebers bei der privaten Nutzung eines dienstlichen Gerätes oder der dienstlichen Nutzung eines privaten Gerätes.

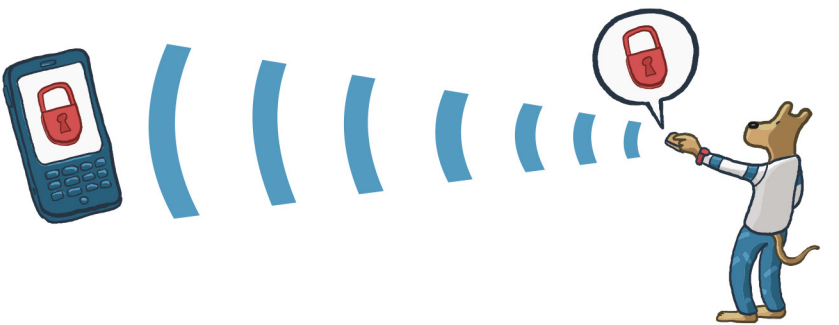
4 Lassen Sie Ihr Gerät nicht aus den Augen

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

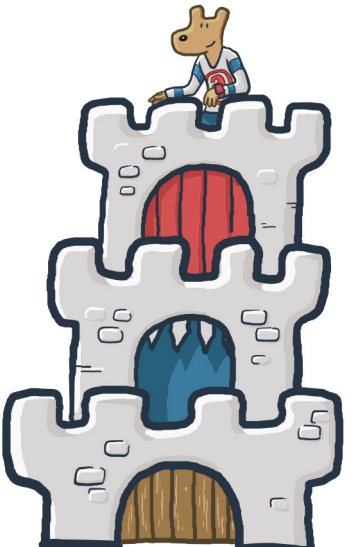


5 Nutzen Sie Sperrcodes und Passwörter

Achten Sie darauf, dass die SIM/USIM-PIN und die Bildschirmsperre Ihres Telefons stets aktiviert sind. Auch sensible Anwendungen, wie Online-Banking und App-Käufe, können 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.

Ob PIN oder Muster: Sorgen Sie für einen Sichtschutz bei der Eingabe, damit niemand Ihre Kombination ausspähen kann. Bitte reinigen Sie auch regelmäßig Ihr Display um Wischspuren zu beseitigen.



6 Aktivieren Sie Schnittstellen nur bei Bedarf und sichern Sie diese

Deaktivieren Sie Drahtlosschnittstellen, wie Bluetooth, WLAN oder NFC, wenn Sie diese nicht benötigen. So ist ihr Gerät weniger anfällig für Cyber-Angriffe.

Der Aufenthaltsort von Mobilfunkgeräten kann von den Betreibern der Funknetzwerke und zum Teil auch von den App-Anbietern jederzeit ermittelt werden. Prinzipiell sollten Sie mit der Weitergabe Ihrer Ortsangaben sehr zurückhaltend sein – also etwa Lokalisierungsdienste meiden und keine Ortsangaben in Fotos speichern, die Sie ins Internet laden. Schalten Sie die GPS-Funktion aus. Dadurch wird die Positionsbestimmung zumindest ungenauer.

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.

7 Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht

In öffentlichen WLAN-Netzen im Café oder am Flughafen ist der Zugang 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 Online-Banking sollten Sie in offenen Netzwerken nicht ausführen. Falls es doch notwendig ist, empfiehlt sich der Aufbau einer sicheren Verbindung. Nutzen Sie dafür eine App, die ein Virtuelles Privates Netzwerk (VPN) aufbauen kann.

Mit der Tethering-Funktion können andere Anwender Ihre Internetverbindung nutzen. Ihr Gerät wird so zu einem Hotspot. Nutzen Sie das WLAN-Sicherheitsprotokoll 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.

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

Informieren Sie sich vor Installation einer App, wenn Ihnen der Anbieter nicht bekannt ist. Eine kurze Suche im Internet reicht meistens aus, um sich zu informieren. Entfernen Sie veraltete Anwendungen oder solche, die Sie nicht mehr nutzen. Denn jede zusätzliche App ist eine mögliche Sicherheitslücke.

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. Wichtig: Durch Updates können auch Änderung oder Erweiterung der Zugriffsberechtigungen erfolgen. Die daraus resultierenden Konsequenzen sind gegen den Mehrwert des Updates abzuwägen.

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

Schützen Sie Ihre Daten

Nutzen Sie die Funktionen zur Datenverschlüsselung, wenn vorhanden oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware.

Sichern Sie Ihre Daten auf den mobilen Geräten regelmäßig.

10 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.

Die SIM-Karte sollten Sie grundsätzlich entfernen und – falls Sie diese nicht weiter verwenden wollen – vernichten.

Sicher unterwegs mit Smartphone & Co

Basisschutz leicht gemacht – 10 Tipps

- ✔ Sorgen Sie für einen Basisschutz. Vergewissern Sie sich, dass die vorhandenen Sicherheitseinstellungen Ihres Geräts eingeschaltet sind und aktualisieren Sie Apps und Betriebssystem umgehend.
- ✔ Prüfen Sie unbekannte Nummern vor dem Rückruf. Hilfe gibts auf www.bundesnetzagentur.de/Rufnummernmissbrauch.
- ✔ Verschlüsseln Sie vertrauliche Gespräche.
- ✔ Lassen Sie Ihr Gerät niemals unbeobachtet und verleihen Sie es nicht, um es vor unbefugten Zugriffen und Manipulation zu schützen.

- 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, NFC oder Infrarot, wenn Sie diese nicht benötigen. Sie erschweren die Erstellung von Bewegungsprofilen, wenn Sie die GPS- und die WLAN-Funktion ausschalten.
- Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die geforderten Zugriffsberechtigungen.
- Sichern Sie ihre 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.

Weitere Hinweise ...

... finden Sie auf den BSI-Seiten, beispielsweise unter:

www.bsi-fuer-buerger.de/MobileSicherheit
www.bsi.bund.de/Publikationen

» Wie bewege ich mich sicher im mobilen Netz?

» Mobile Geräte und Apps:
Sicherheitsgefährdungen und Schutzmaßnahmen

» Sicherheitstipps für fremde WLANs

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

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
Telefon +49 (0) 22899 9582-0
Service-Center +49 (0) 800 274 1000

Stand
August 2016

Illustrationen
Leo Leowald

Artikelnummer
BSI-IFB 16/251