https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/BasisschutzHandy/basisschutzHandy_node.html

Basisschutz für Handy, Smartphone und Co.

Mittlerweile entsprechen die mobilen, internetfähigen Geräte kleinen Computern, auf denen gearbeitet, kommuniziert und vertrauliche Daten gespeichert werden. Dadurch gelten für sie mindestens die gleichen Sicherheitsanforderungen wie für stationäre PCs. Die Sicherheit spielt im Grunde sogar eine noch größere Rolle, denn die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden, birgt zusätzliches Gefahrenpotenzial.

Alle Benutzer von Handy, Smartphone, Tablet-PC und Co. sollten daher folgende, kurze Sicherheitshinweise beachten.

Die wichtigsten Sicherheitshinweise für mobiles Telefonieren und mobiles Internet:

1. **Prüfen Sie unbekannte Rufnummern vor Rückruf.** Rufen Sie unbekannte Dienste-Rufnummern nicht zurück. Weitere und 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.

2. **Führen Sie Gespräche mit vertraulichem Inhalt nicht über das Handy:** Das Telefonieren über GSM (Standard zur mobilen Sprach- und Datenübertragung) ist nicht abhörsicher. Wenn Sie vermehrt besonders schützenswerte, geheime Informationen austauschen wollen, weichen Sie auf andere Kommunikationsmittel aus.

3. **Sorgfältiger Umgang mit Zugangsdaten:** Nutzen Sie die Tastatursperre sowie den Gerätesperrcode und aktivieren Sie stets die SIM/USIM-PIN. Zusätzlich können Sie mittlerweile bei vielen Smartphones eine Display-Sperre aktivieren. Diese kann über die Eingabe eines Pincodes oder eines Musters aufgehoben werden. Halten Sie Ihre Zugangsdaten unter Verschluss. Dies gilt insbesondere auch für Zugangscodes für Dienste wie Online-Banking. Geben Sie PIN und Codes nur unter Sichtschutz gegenüber Dritten ein und wechseln Sie die Passwörter.

4. **Deaktivieren Sie drahtlose Schnittstellen** (z.B. WLAN und Bluetooth), wenn Sie diese nicht nutzen. Koppeln Sie externe Geräte mit Ihrem Mobilfunkgerät (etwa über Bluetooth) nur in gesicherter Umgebung.

5. **Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht** und – soweit möglich – über eine gesicherte Verbindung (https). Vermeiden Sie es, kritische Anwendungen wie Online-Banking in offenen Netzwerken durchzuführen. Einige Geräte bieten auch die Möglichkeit, sie als mobilen, eigenen Hotspot einzurichten, sodass andere Anwender die Internetverbindung des eigenen Gerätes mitbenutzen können. Wenn Sie diese Funktion nutzen wollen, sollten Sie sehr vorsichtig sein. Machen Sie Ihren Hotspot niemals ohne Passwort frei zugänglich. Nutzen Sie mindestens das WLAN-Sicherheitsprotokoll WPA, besser 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.

6. **Halten Sie mobile Geräte stets unter Aufsicht.**

7. **Installieren Sie Apps nur aus vertrauenswürdigen Quellen.** Falls Ihnen der Anbieter der App nicht bekannt ist, informieren Sie sich vor der Installation. Dazu reicht meist eine kurze Suche im Internet. Falls der Anbieter nicht vertrauenswürdig ist und die Applikation Schadsoftware beinhaltet, wird im Internet meist sehr schnell gewarnt. Einige Hersteller bieten Nutzern die Möglichkeit, sich anzeigen zu lassen, auf welche Daten und Funktionen die zu installierende App Zugriffsrechte hat. Prüfen Sie in diesem Fall kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind.

8. **Führen Sie regelmäßig Sicherheitsupdates durch.** Achten Sie darauf, ob es Sicherheitsupdates für die Firmware Ihres Gerätes oder das auf dem Gerät ausgeführte Betriebssystem und sonstige von Ihnen installierte Software und Apps gibt und führen Sie diese durch. Vermeiden Sie die Installation von Software aus nicht vertrauenswürdiger Quelle. Über erhältliche Updates können Sie sich auch auf den Internetpräsenzen der Gerätehersteller infomieren. Dort gibt es häufig detaillierte Anleitungen zur Umsetzung.

9. **Lassen Sie bei Verlust Ihres mobilen Gerätes die SIM-Karte unverzüglich sperren.** Zusätzlich bieten einige Hersteller die sogenannte Remote-Wipe-Funktion an, bei der das Gerät aus der Ferne zurückgesetzt und gesperrt werden kann. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht oder nicht aufzurufen (siehe Backups/Fernzugriff).

10. **Verkauf und Entsorgung:** 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 sicher gelöscht wurden. Wie das bei Smartphones funktioniert, ist für viele Modelle und Betriebssysteme auf dem IT-Nachrichten- und Service-Portal Chip Online, für iPhone, iPad oder iPod touch auf der Internetseite von Apple beschrieben. Die SIM-Karte sollten Sie entfernen und – falls Sie diese nicht weiter verwenden wollen – vernichten.

11. **Bewegungsprofile:** Der Aufenthaltsort von Mobilfunkgeräten – und damit auch ihrer Besitzer – kann von den Betreibern der Funknetzwerke und zum Teil auch von den App-Anbietern jederzeit ermittelt werden. Durch die Zusammenstellung solcher Daten könnte ein detailliertes Bewegungsprofil erstellt werden. Prinzipiell sollten Sie mit der Weitergabe Ihrer Positionierungsdaten sehr zurückhaltend sein – also etwa Lokalisierungsdienste meiden und keine Ortsdaten in Fotos speichern, die Sie ins Internet laden. Schalten Sie die GPS- und die WLAN-Funktion aus – dadurch wird die Positionsbestimmung zumindest ungenauer.