Sicherheitseinstellungen für Smartphones

Windows

Co-financed by the European Union
Connecting Europe Facility

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

Impressum:

ISPA – Internet Service Providers Austria, Währinger Straße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft

5. aktualisierte Auflage
Wien, September 2017
Redaktion: Moritz F. Fürst
Endgerät: Microsoft Lumia 550
Betriebssystem: Windows 10 Mobile 10.0.14393.1066

Gefördert durch die Europäische Union – Safer Internet Projekt.

Schutz vor unbefugtem Zugriff auf das Gerät

Das Smartphone ist für die meisten Menschen zu einem sehr personalisierten Gerät mit hoch sensiblen Informationen geworden. Persönliche Daten wie z. B. das Adressbuch mit allen Kontakten, Fotos, Social Media Apps oder private und geschäftliche E-Mail-Accounts sind ein „best of" all jener Daten, die unser Leben bestimmen. Eine wichtige Sicherheitsvorkehrung zum Schutz dieser Informationen besteht darin, durch Einrichtung einer PIN-Abfrage (Bildschirmsperre) unbefugten Zugriff auf das Telefon und die darauf gespeicherten Informationen zu unterbinden.

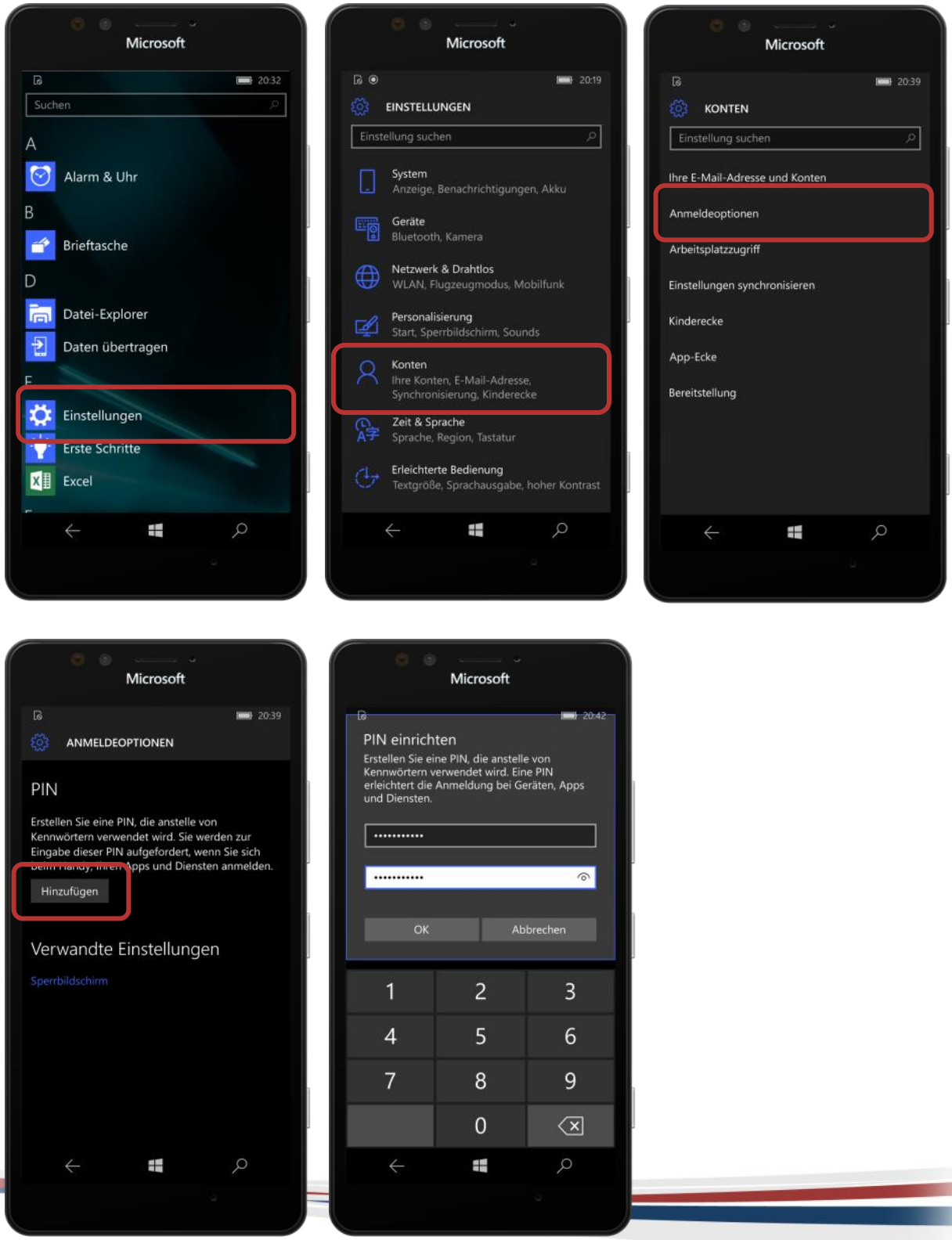
Wie bei vielen Sicherheitsmaßnahmen müssen Nutzerinnen und Nutzer auch bei der Wahl eines Codes eine individuelle Abwägung zwischen Komfort und höherer Sicherheit treffen. Die Länge und Art des PIN-Codes hat nämlich wesentlichen Einfluss auf die Sicherheit: Je länger der Zifferncode, desto sicherer. Leicht zu erratende Kombinationen wie etwa der eigene Geburtstag, „1234" oder gar „0000" sollten tunlichst vermieden werden.

Die gewählte Kombination sollte zudem nicht bei anderen Diensten oder Geräten nochmals verwendet werden, da man es so potentiellen Angreifern einfach macht, mit nur einem Passwort auf mehrere Konten bzw. Endgeräte zuzugreifen.

Auf jeden Fall sollte darauf Acht gegeben werden, dass die Eingabe des Entsperr-Codes stets unauffällig erfolgt. Viele Sicherheitsangriffe sind überraschend trivial, eine weit verbreitete Methode ist etwa das Abschauen oder Abfotografieren von Zugangsdaten und Passwörtern bei deren Eingabe. Besonders auf öffentlichen Plätzen, in dicht gedrängten Verkehrsmitteln oder bei neugierigen Sitznachbarn im Flugzeug sollten Nutzerinnen und Nutzer vorsorglich achtsam sein.

Die PIN-Abfrage einrichten

In den Einstellungen von Windows Mobile auf „Konten“ tippen. Unter „Anmeldeoptionen“ lässt sich ein PIN-Code festlegen.

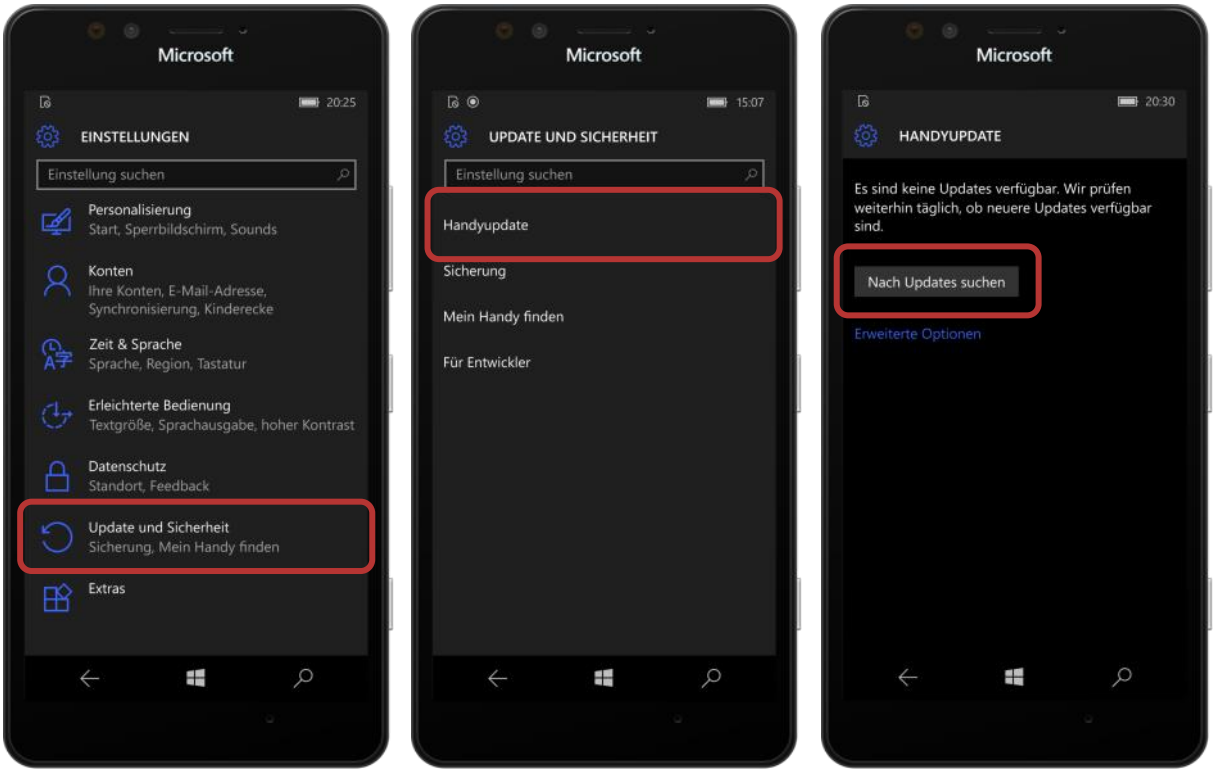


Software-Updates

Die vom Hersteller bereitgestellten Software-Updates („Handyupdates“) sollten regelmäßig durchgeführt werden. Sie enthalten kleine Systemverbesserungen, reparieren Fehler und schließen eventuelle Sicherheitslücken. Üblicherweise sucht das Windows-Smartphone bei bestehender Internetverbindung automatisiert nach Updates und macht gegebenenfalls darauf aufmerksam. Es ist empfehlenswert, Software-Updates möglichst zeitnah nach deren Veröffentlichung durchzuführen.

Manuelle Suche nach Software-Updates

In den Einstellungen auf „Update und Sicherheit“ tippen. Unter dem Menüpunkt „Handyupdate“ werden gegebenenfalls verfügbare Aktualisierungen angezeigt bzw. können mittels „Updates suchen“ angefordert werden.



Datenschutzeinstellungen

Moderne Smartphones verfügen über zahlreiche Sensoren (z. B. Mikrofon, Kamera, GPS-Empfänger), sind ständig mit dem Internet verbunden und speichern jede Menge persönliche Daten – diese Informationen können nicht nur mittels gezielter Angriffe bzw. durch physischen Zugriff auf das Telefon, sondern auch durch auf dem Gerät installierte Software in unbefugte Hände gelangen.

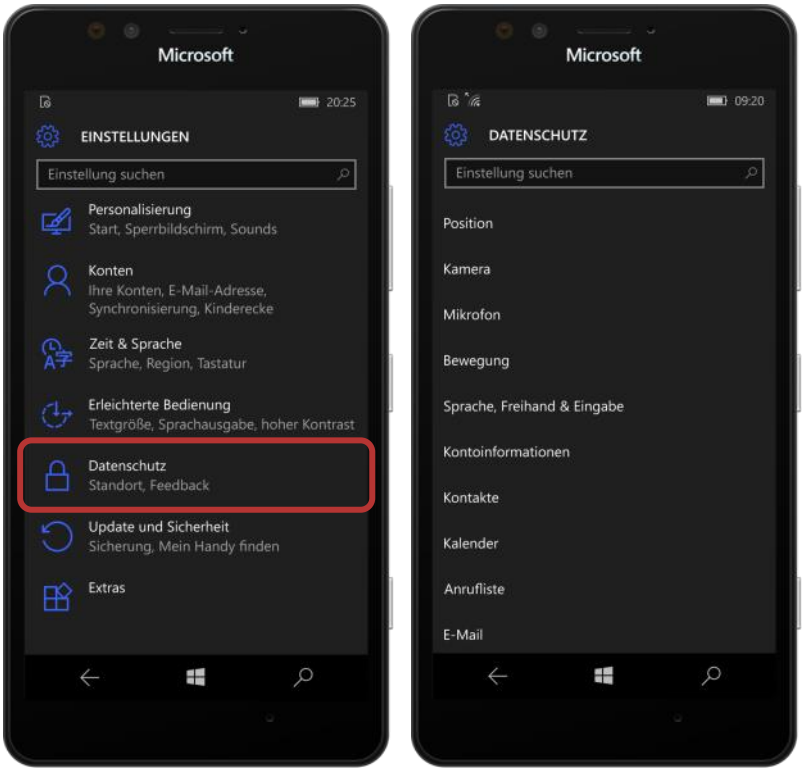
Um sich vor Schadsoftware zu schützen, sollten Apps von Drittanbietern nur aus dem Windows Store geladen werden. Diese müssen nämlich ein Testverfahren durchlaufen, bevor sie zum Download verfügbar sind und auf dem Gerät installiert werden können. Auch dieses Verfahren kann naturgemäß keinen absoluten Schutz garantieren, solange aber nur Apps aus dem offiziellen Store geladen werden und Nutzerinnen und Nutzer grundlegende Sicherheitsregeln beachten (Vorsicht bei E-Mail-Anhängen etc.), ist das Smartphone so vor der unbeabsichtigten Installation von Schadsoftware relativ sicher.

Nicht bedenkenlos allen App-Zugriffsberechtigungen zustimmen

Oftmals ist es aber gar nicht unbedingt eine Sicherheitslücke im engeren Sinne, die von "bösartigen" Apps ausgenutzt wird, um an Daten zu kommen. Vielmehr macht man sich die Unachtsamkeit der Userinnen und User zu Nutze und fordert Berechtigungen, etwa für den Zugriff auf das Adressbuch, obwohl diese für die Funktionalität der App gar nicht nötig sind. Hier sollte man vorsichtig sein und nur dann zustimmen, wenn diese Zugriffsrechte plausibel und notwendig erscheinen. Handelt es sich zum Beispiel um eine Spiele-App, braucht diese eher keinen Zugriff auf das Adressbuch; dass hingegen eine Navigations-App Zugriff auf die Standort-Daten benötigt, macht wiederum Sinn. Es empfiehlt sich, bewusst auszuwählen, welche Daten welcher App zur Verfügung gestellt werden. Die Zugriffsrechte einer App können zudem auch jederzeit wieder deaktiviert werden.

Einzelne Zugriffsberechtigungen anzeigen und deaktivieren

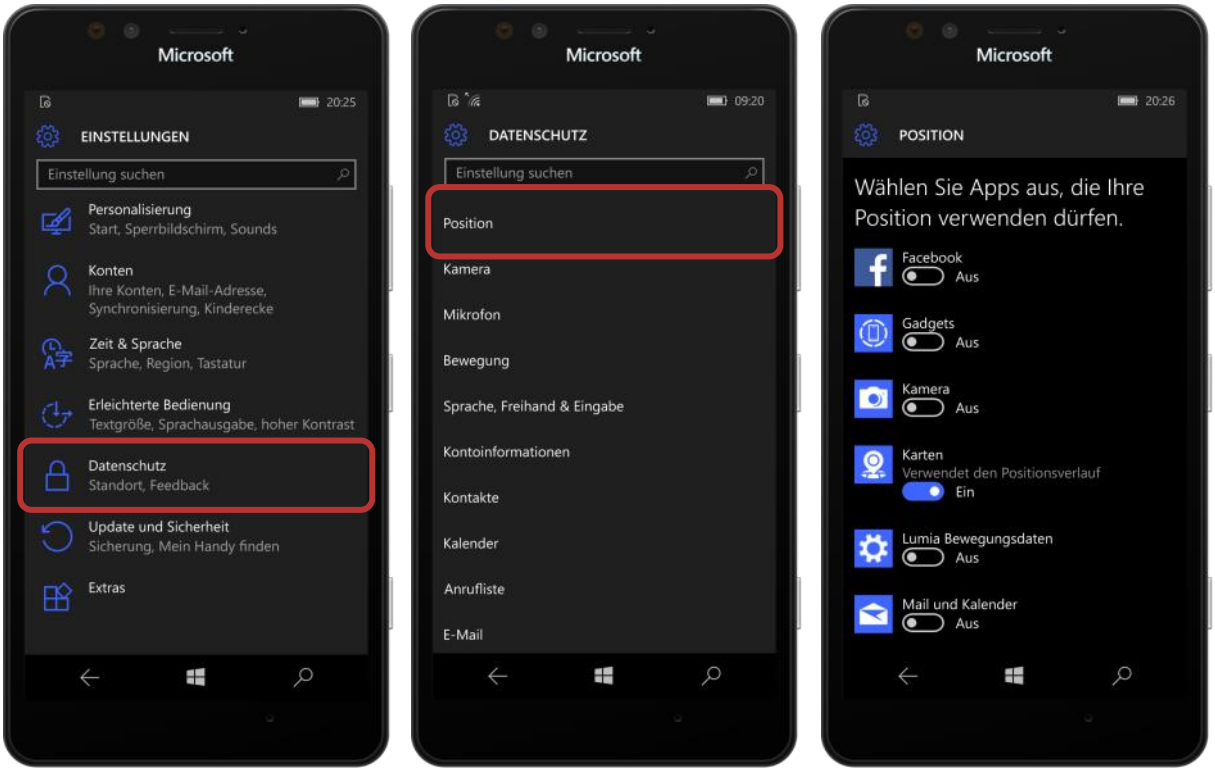
Der Menüpunkt „Datenschutz" in den Einstellungen ermöglicht es, genau festzulegen, welche Apps auf den eigenen Standort („Position"), die Kontakte, Kalender, aber auch Sensoren wie Kamera oder Mikrofon zugreifen können.

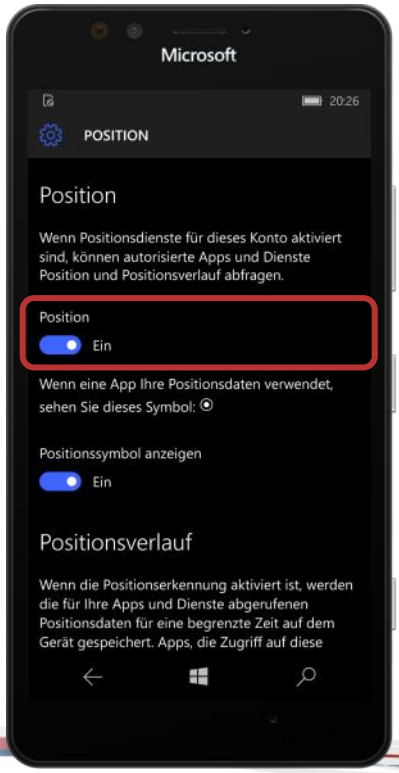


Zugriff auf den eigenen Standort einschränken

Die sogenannten "Positionsdienste" ermöglichen dem Windows Phone, den eigenen Standort aus GPS-Daten, Bluetooth- und WLAN-Informationen und der Position von Mobilfunkmasten zu errechnen. Der Standort kann sowohl vom System selbst, als auch von installierten Apps verwendet werden. Der Zugriff auf die Positionsdienste sollte nur jenen Apps gewährt werden, die diese auch wirklich benötigen. Sollte nicht schlüssig ersichtlich sein, warum eine App den Standort benötigt, ist es sicherer, diesen zu deaktivieren. Ein positiver Nebeneffekt besteht in einer verlängerten Akkulaufzeit, da insbesondere eine häufige Aktivierung des GPS-Sensors den Stromverbrauch deutlich erhöht.

In den Einstellungen für Ortungsdienste lässt sich für jede App einzeln einstellen, ob diese auf den eigenen Standort zugreifen kann. Zudem lässt sich die Positionsbestimmung auch vollständig deaktivieren.





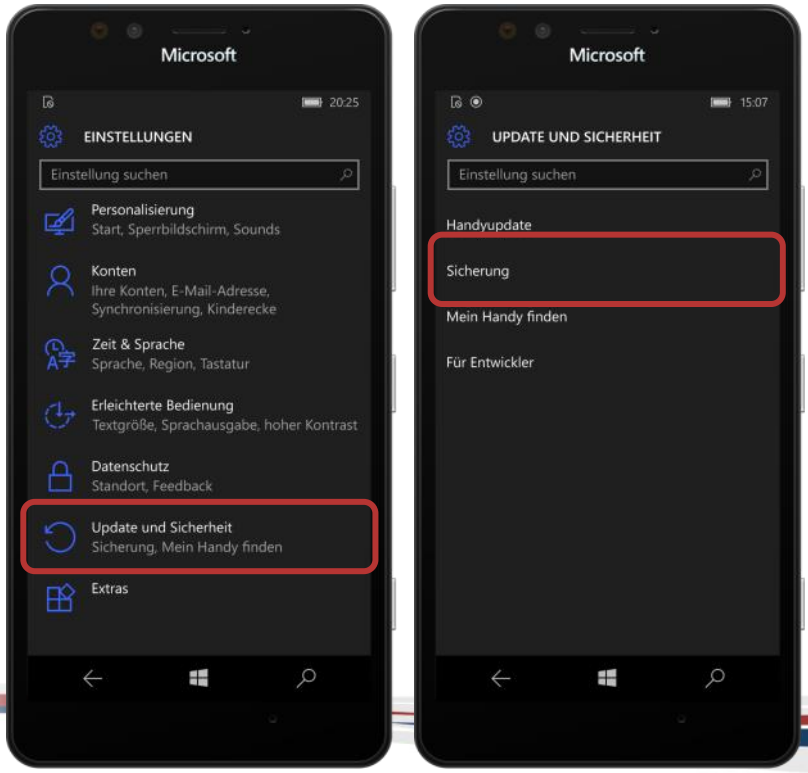
Synchronisierung & Backups

Genau wie bei einem PC ist es auch bei einem Smartphone notwendig, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Daten- oder Handyverlusts kann so auf das Backup zugegriffen werden und zumindest der letzte Stand der gesicherten Daten ist verfügbar.

Windows bietet mit der Funktion „Sicherung" die Möglichkeit, sich vor Datenverlust zu schützen. Bestimmte Daten können dabei im Cloud-Dienst „OneDrive" gespeichert werden; hierfür wird ein Microsoft-Konto benötigt (ein Microsoft-Konto wird beispielsweise auch für die Dienste Skype, Xbox Live oder Outlook.com verwendet; weitere Informationen dazu finden sich auf account.microsoft.com). Zusätzlich können die Daten mittels der OneDrive-App automatisch auf mehreren Geräten synchronisiert werden. Bei der Speicherung in einem Cloud-Service gilt es jedoch zu bedenken, dass dies gewisse Sicherheitsrisiken mit sich bringt – Datenschutz und -sicherheit sollten dabei bedacht werden.

Datensicherung mit OneDrive

In den Einstellungen auf „Update und Sicherheit" tippen. Unter dem Menüpunkt „Sicherung" ist es nach Anmeldung mit dem Microsoft-Konto möglich, das Backup auf OneDrive zu konfigurieren.



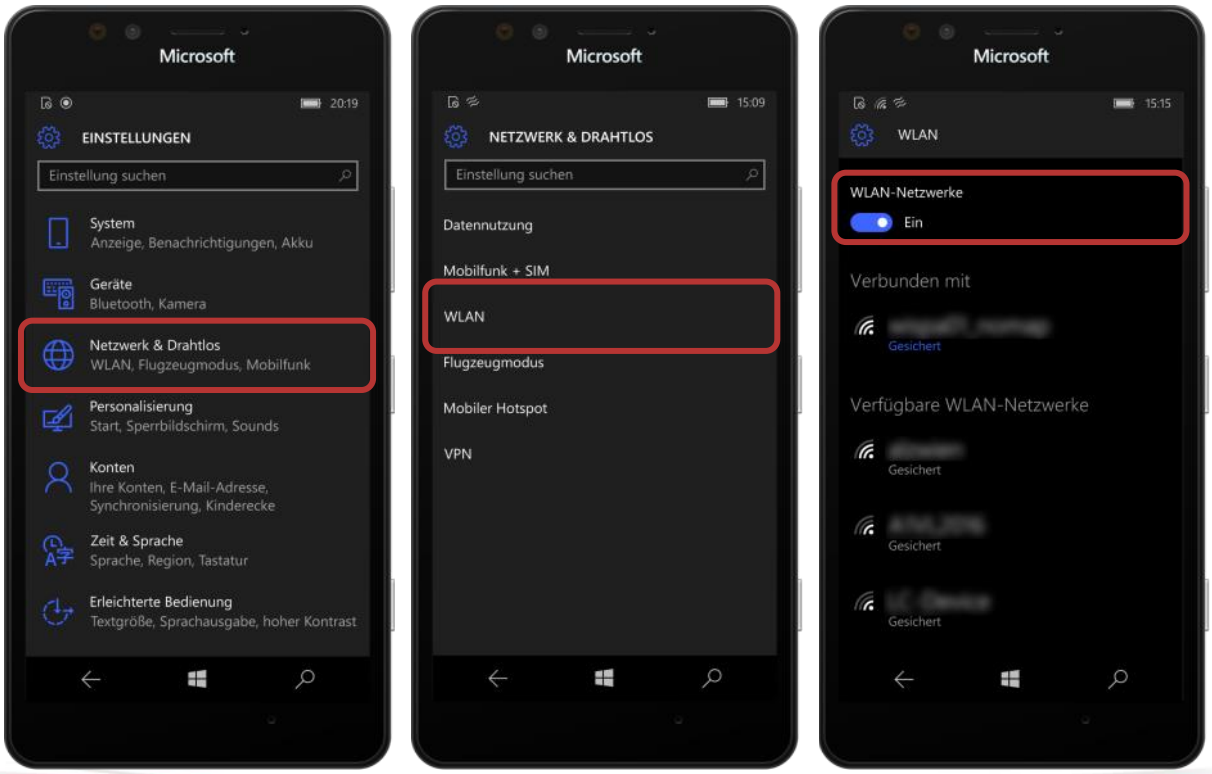
WLAN, Bluetooth und mobile Hotspots

„Home is where your wifi connects automatically" : Wenn sich das Smartphone selbstständig mit verfügbaren WLANs verbindet, ist das zwar praktisch und bequem, kann aber unter Umständen ein Sicherheitsrisiko darstellen. Drahtlose Schnittstellen sollten nur für die unmittelbare Verwendung aktiviert werden.

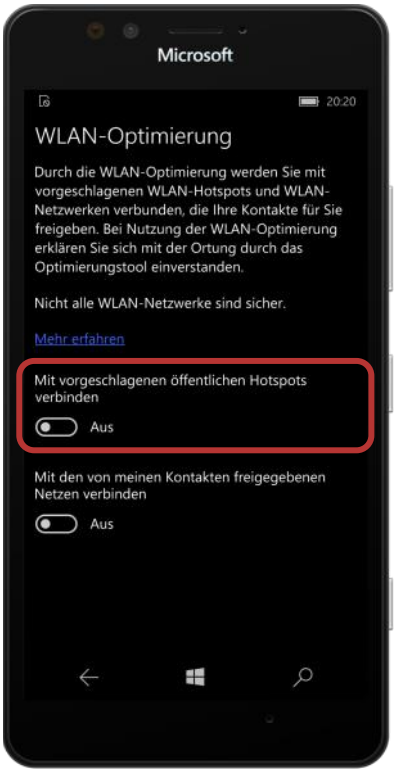
WLAN, Bluetooth und sonstige drahtlose Schnittstellen stellen potentielle Angriffspunkte dar. Die WLAN- und Bluetooth-Funktion sollte deshalb nur dann eingeschalten werden, wenn auch wirklich auf ein WLAN-Netzwerk zugegriffen werden soll oder die Bluetooth-Funktion unmittelbar benötigt wird. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist ein stark reduzierter Stromverbrauch.

WLAN deaktivieren

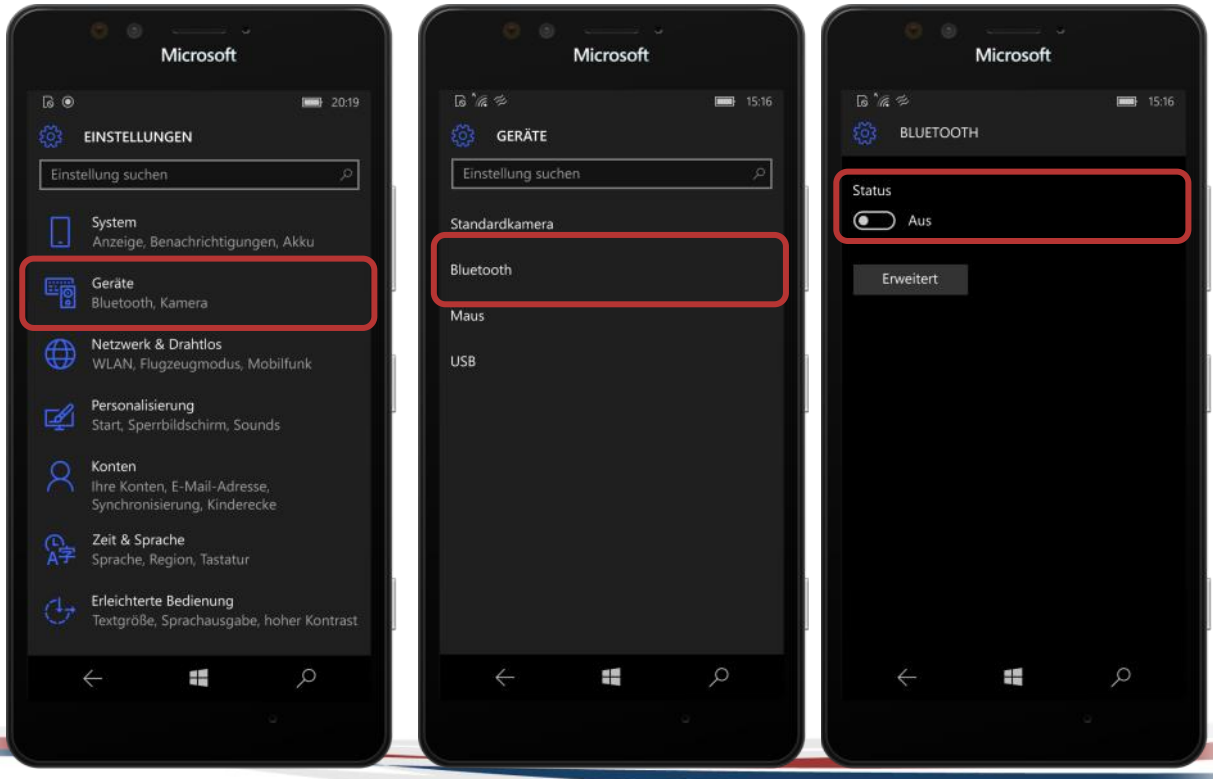
In den Einstellungen auf „Netzwerk & Drahtlos" tippen. Unter „WLAN" werden die verfügbaren Netzwerke angezeigt und die WLAN-Funktion kann abgeschalten werden.



Über die Schaltfläche „WLAN-Optimierung“ in diesem Menü sollte konfiguriert werden, dass sich das Telefon nicht automatisch mit offenen WLAN-Netzen verbindet. Diese sind oft nur mangelhaft gesichert und können es Angreifern ermöglichen, den gesamten Netzwerkverkehr mitzulesen.

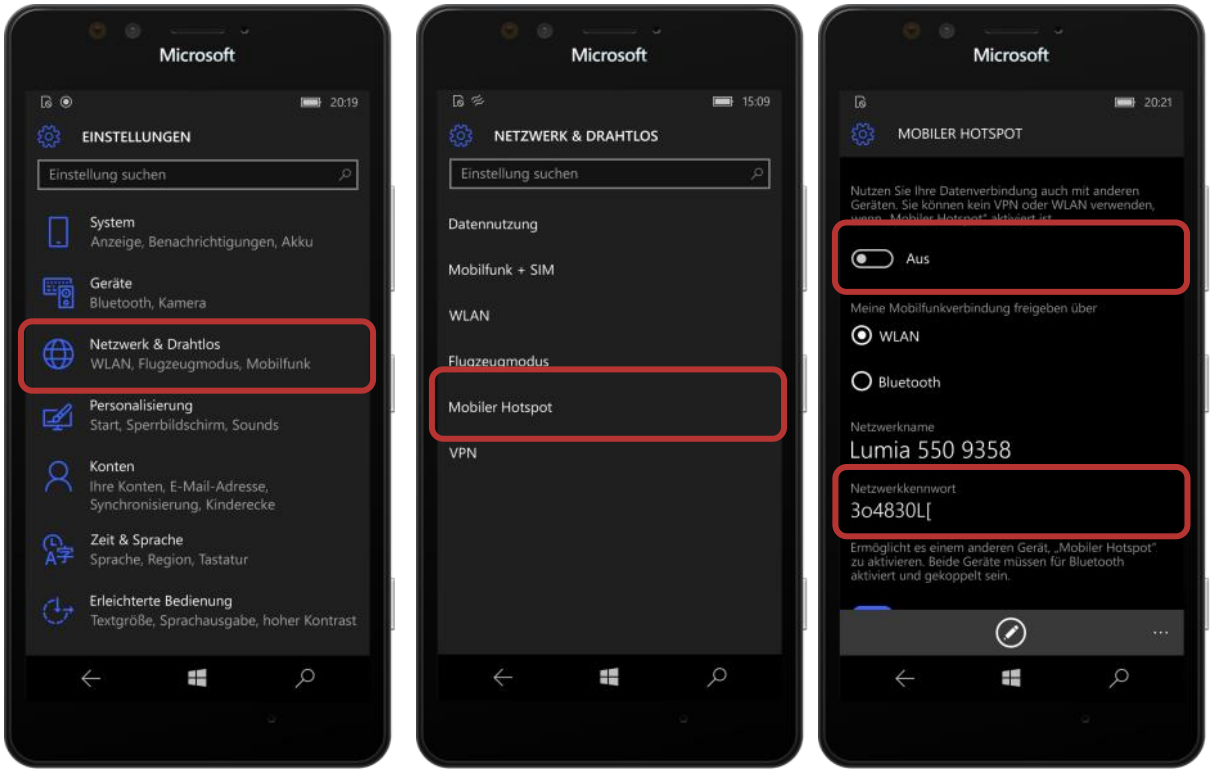


Bluetooth deaktivieren



Den mobilen Hotspot sicher konfigurieren

Windows bietet die Möglichkeit, das eigene Smartphone als WLAN-Router zu konfigurieren und so beispielsweise als mobiler Hotspot für den eigenen Laptop zu dienen. Die Hotspot-Funktion sollte jedenfalls mit einem starken Passwort, das aus Zahlen und Buchstaben besteht, gesichert und ebenfalls nur bei Bedarf aktiviert werden.



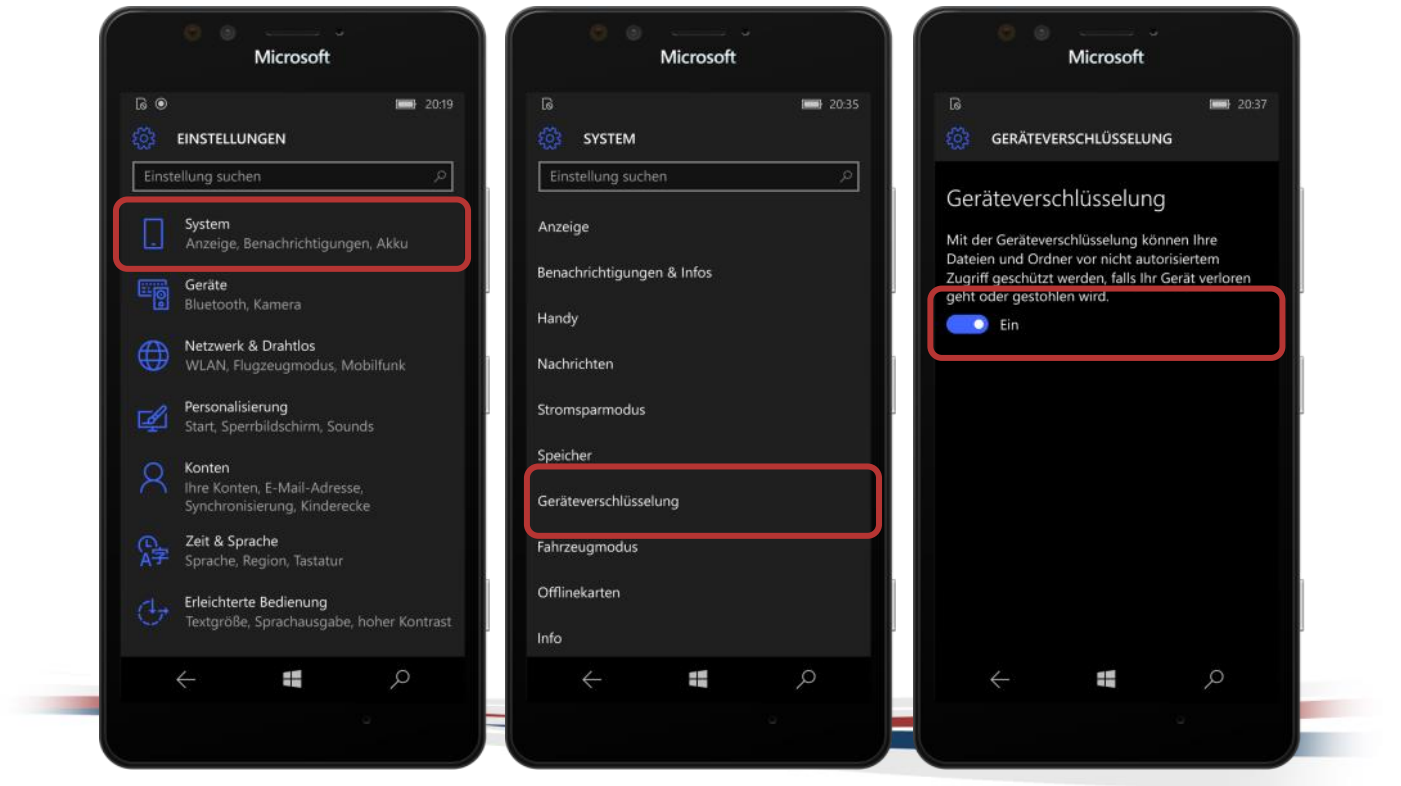
Geräteverschlüsselung

Die auf Windows-Smartphones gespeicherten Daten können mit der Funktion „Geräteverschlüsselung" zusätzlich geschützt werden.

Dabei werden mittels des PIN-Codes das Betriebssystem sowie alle Dateien und Ordner auf dem Gerät verschlüsselt. Wird diese Funktion aktiviert, können alle auf dem Hauptspeicher abgelegten Daten nur noch mit dem richtigen Schlüssel (dem PIN-Code) lesbar gemacht werden. Es empfiehlt sich, diese Funktion zu aktivieren, um das Risiko von Datenmissbrauch bzw. -verlust bei Diebstahl oder Verlust des Geräts zu minimieren. Voraussetzung ist, dass ein PIN-Code auf dem Gerät eingerichtet wurde (Kapitel „Schutz vor unbefugtem Zugriff auf das Gerät"), denn dieser bildet die Basis für die Verschlüsselung. Ist noch kein Code gesetzt, leitet Windows automatisch zur PIN-Vergabe weiter und die Aktivierung der Verschlüsselung muss anschließend nochmals gestartet werden.

Achtung: Derzeit ermöglicht diese Funktion lediglich die Verschlüsselung des Hauptspeichers, die Micro-SD-Karte lässt sich so nicht schützen (dies wird lediglich von firmenverwalteten Geräten ab Version Windows 10 Build 15007 unterstützt).

Geräteverschlüsselung aktivieren



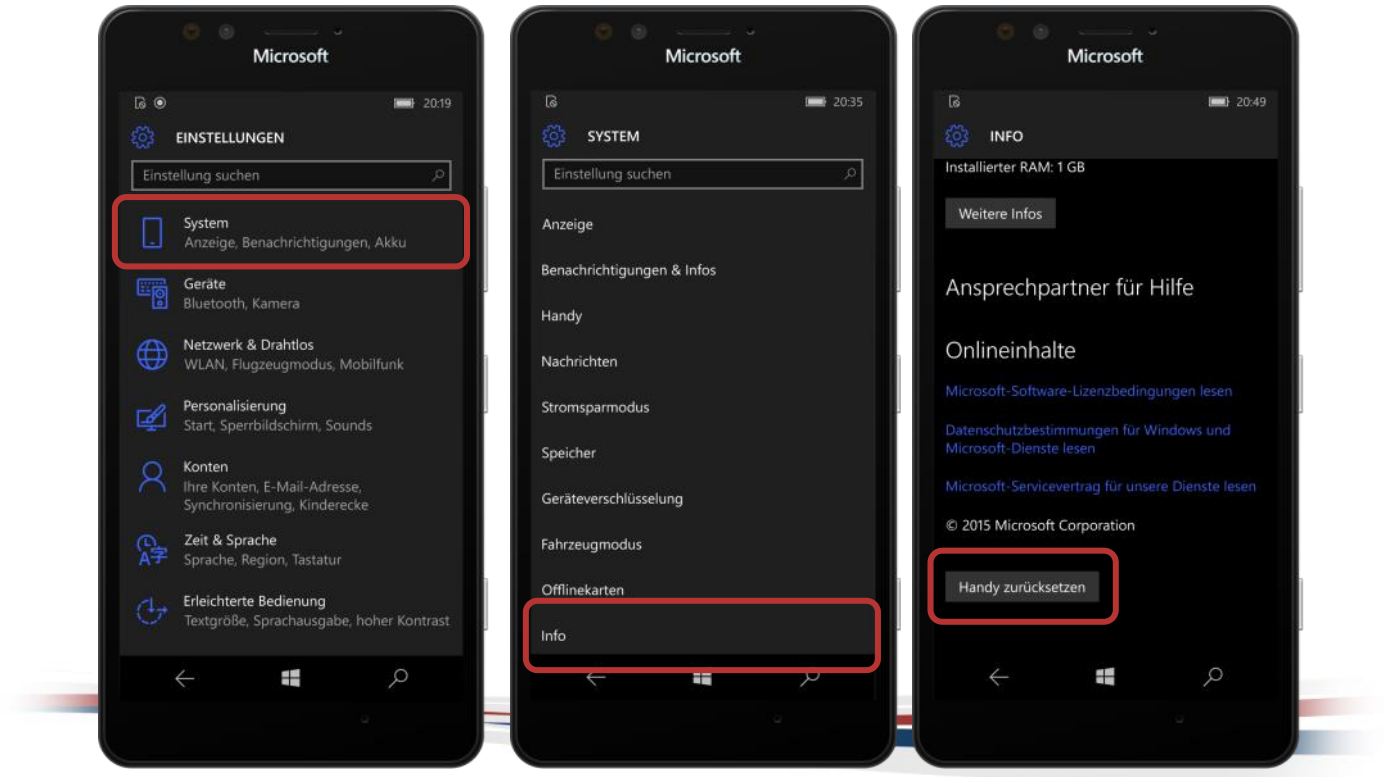
Verkaufen, Verschenken & Verborgen

E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem Smartphone sind sehr viele persönliche Daten gesammelt. Soll das Gerät weitergegeben oder verkauft werden, sollte das Gerät unbedingt auf den Werkzustand zurückgesetzt werden.

Um die Weitergabe der persönlichen Daten zu verhindern, sollten alle vorhandenen Speicher gelöscht werden, also nicht nur der interne Speicher, sondern gegebenenfalls auch der externe (die Micro-SD-Karte). Hierfür reicht es nicht, diesen einfach nur zu löschen, da gelöschte Daten unter Umständen wiederhergestellt werden können. Neben dem Einsatz einer speziellen Löschsoftware (diese überschreibt den Speicher mehrmals mit „Unsinn") ist die sicherste Variante natürlich, die Micro-SD-Karte vor einem Verkauf oder Verschenken des Telefons aus dem Gerät zu nehmen.

Auf Werkzustand zurücksetzen

In den Einstellungen auf „System" tippen. Unter „Info" findet sich am Ende die Schaltfläche „Handy zurücksetzen". Dadurch werden alle persönlichen Inhalte (Apps, Bilder, Musik, Videos, Konten, etc.) vom Gerät entfernt und das Smartphone wird auf Werkseinstellungen zurückgesetzt.



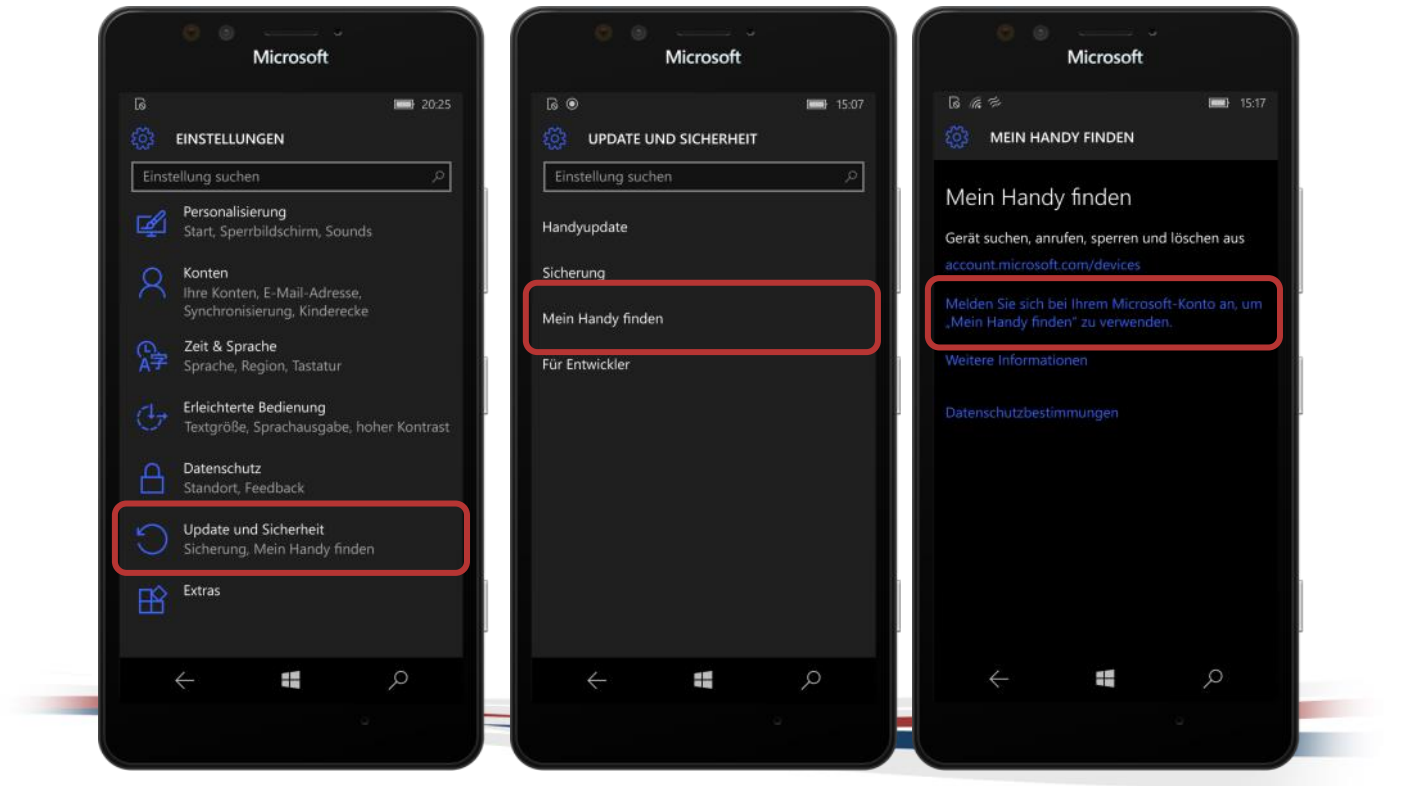
„Mein Handy finden“: das Smartphone finden, sperren und löschen

Die meisten Smartphones bieten die Möglichkeit, es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen. Windows unterstützt dies im Rahmen der Funktion „Mein Handy finden“.

Ist diese Funktion aktiviert, kann das Smartphone über das Microsoft-Konto geortet und gesperrt werden. Zudem können die Daten aus der Ferne gelöscht werden. Eine durchaus praktische Funktion ist „klingeln lassen“, welche einen Klingelton auf dem Handy startet, der auch im Lautlos-Modus in voller Lautstärke ertönt. Damit dieser Fernzugriff-Service funktioniert, muss der Standortzugriff in den Einstellungen erlaubt werden. Ebenso muss der Standortzugriff beim Microsoft-Konto aktiviert werden. Um das Smartphone im Fall des Falles zu orten, müssen sich Nutzerinnen und Nutzer in der Web-App einloggen (account.microsoft.com/devices).

Aktivierung von „Mein Handy finden“

In den Einstellungen auf „Update und Sicherheit“ tippen. Unter „Mein Handy suchen“ steht nach Anmeldung mit einem Microsoft-Konto die Funktion bereit.



„Kinderecke" – das kindersichere Smartphone

Um das Smartphone bei Bedarf kindersicher zu machen, lässt sich über die Funktion „Kinderecke" ein eigenes Profil für die jüngeren Userinnen und User einrichten, indem genau festgelegt wird, welche Programme, Videos und Fotos für diese verfügbar sein sollen und welche nicht.

Hierfür muss aber zuerst die passwortgeschützte Bildschirmsperre aktiviert werden (Kapitel „Schutz vor unbefugtem Zugriff auf das Gerät"). Ist die Kinderecke einmal eingerichtet, erscheint auf dem Startbildschirm ein Thumbnail („Kachel") mit welchem diese gestartet werden kann. Alternativ lässt sich die Kinderecke durch eine Wischgeste nach links am Sperrbildschirm schnell und unkompliziert aktivieren. Ohne den Code für die Bildschirmsperre kann die Kinderecke nicht deaktiviert werden.

Erziehungsberechtigte sollten allerdings bedenken, dass Medienerziehung nicht an Software delegiert werden kann. Eine allzu penible Überwachung sämtlicher Aktivitäten ist zudem pädagogisch wenig sinnvoll: Sie verleitet zum Einschreiten, wo Kinder eigentlich gut alleine zurechtkommen und steht einer vertrauensvollen, guten Kommunikationsbasis eher im Wege. Viel wichtiger ist es, mit Kindern offen über ungeeignete Inhalte und Online-Gefahren zu sprechen und ganz generell die Medienkompetenz der jüngsten Userinnen und User zu fördern. Ebenso sollten Eltern – und ältere Geschwister – bedenken, dass sie eine Vorbildfunktion haben, denn Kinder ahmen gerne das Verhalten von Älteren nach. Diesbezügliche Tipps, Hilfestellungen und Info-Materialien für Eltern und Bezugspersonen von Kindern gibt es unter www.saferinternet.at/fuer-eltern. Pädagoginnen und Pädagogen finden unter www.saferinternet.at/fuer-lehrende auch Materialien und Übungen für den Einsatz im Unterricht.

Saferinternet.at
Das Internet sicher nutzen!

Die „Kinderecke“ aktivieren