Sicherheitseinstellungen für Smartphones

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

Impressum:

ISPA – Internet Service Providers Austria, Währingerstraße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft
3. aktualisierte Auflage.
Inhaltliche Verantwortung: Daniela Drobna
Endgerät: Nokia Lumia 720
BS: Windows Phone 8.0

Gefördert durch die Europäische Union – Safer Internet Projekt

Wien, Februar 2014

ispa Internet Service Providers Austria

95% aller Österreicherinnen und Österreicher nutzen ein Mobiltelefon. Davon besitzt die Hälfte ein Smartphone, die Tendenz ist stetig steigend. Durch die höhere Verbreitung und das ständig wachsende Angebot an Nutzungs-möglichkeiten wird das Smartphone immer mehr zu einem personalisierten Gerät mit hoch sensiblen Informationen. Persönliche Daten wie z.B. das Adressbuch mit allen Kontakten oder private und geschäftliche E-Mail-Accounts sind ein „best of" all jener Daten, die unser Leben bestimmen. Umso mehr gilt es ein paar Verhaltensrichtlinien einzuhalten, die vor allem im Falle eines Verlustes oder Diebstahls hilfreich sind.

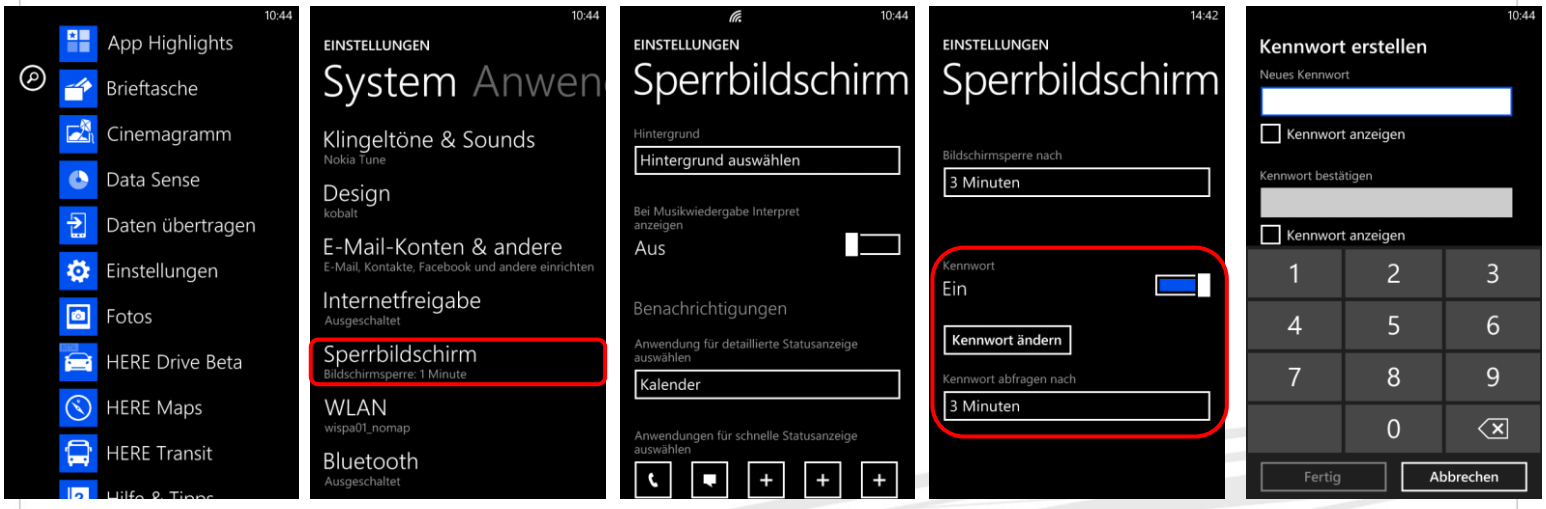
1. Doppelt hält besser: Passwortschutz am Smartphone

Mittlerweile gibt es bei jedem Smartphone die Möglichkeit dieses mittels Passwort zu schützen. Die meisten Smartphones bieten hier zwei Sicherheitsfunktionen: einmal die PIN-Eingabe beim Einschalten des Gerätes (SIM-Kartensperre oder PIN-Eingabe) und als zusätzliche Option die Passwortabfrage bei der Aufhebung des Ruhezustandes (Bildschirmsperre). Ersteres ist eine Standardeinstellung und sollte keinesfalls aus Bequemlichkeit abgeschalten werden. Es ist aber auch ratsam, ebenfalls eine passwortgeschützte Bildschirmsperre zu verwenden – es erscheint zwar zeitaufwendig jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz Ihres Smartphones bzw. Ihrer Daten bei.

Neben der PIN-Abfrage beim Einschalten des Smartphones, gibt es den optionalen Passwortschutz zur Aufhebung des Ruhezustandes „Sperrbildschirm". Hier können Sie einerseits festlegen, wann sich die Bildschirmsperre einschaltet und diese zusätzlich durch eine selbstgewählte Zahlenkombination schützen.

Sperrbildschirm bei Windows:

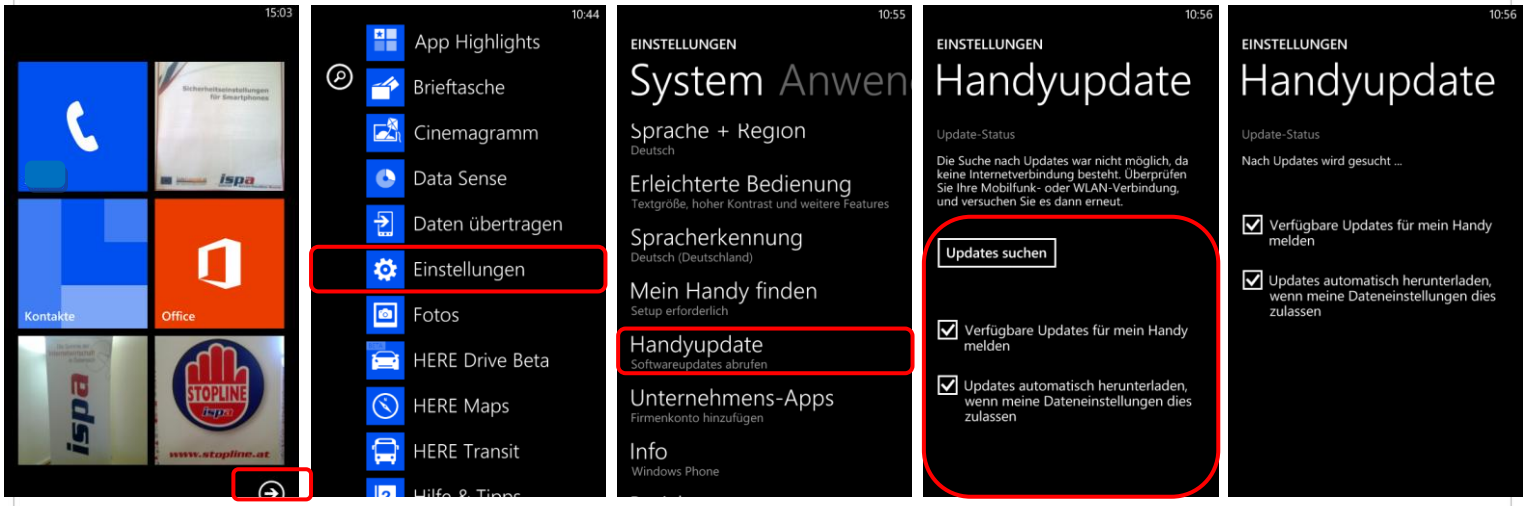
Einstellungen – Sperrbildschirm – Kennwort „Ein"



2. Software-Updates des Geräteherstellers

Führen Sie regelmäßig die vom Hersteller empfohlenen Software-Updates für Ihr Smartphone durch. Software-Updates enthalten kleine Systemverbesserungen, sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Smartphone-Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-)Problem bei einem ihrer Produkte erlangen, großes Interesse umgehend zu reagieren und versuchen schnell eine Lösung des Problems zu erarbeiten.
Sie können auch vorsehen, dass Ihr Smartphone bei bestehender Internetverbindung automatisiert nach Updates sucht und Sie darauf aufmerksam macht.

Suche nach Software-Updates:
Einstellungen – Handyupdate – Updates suchen

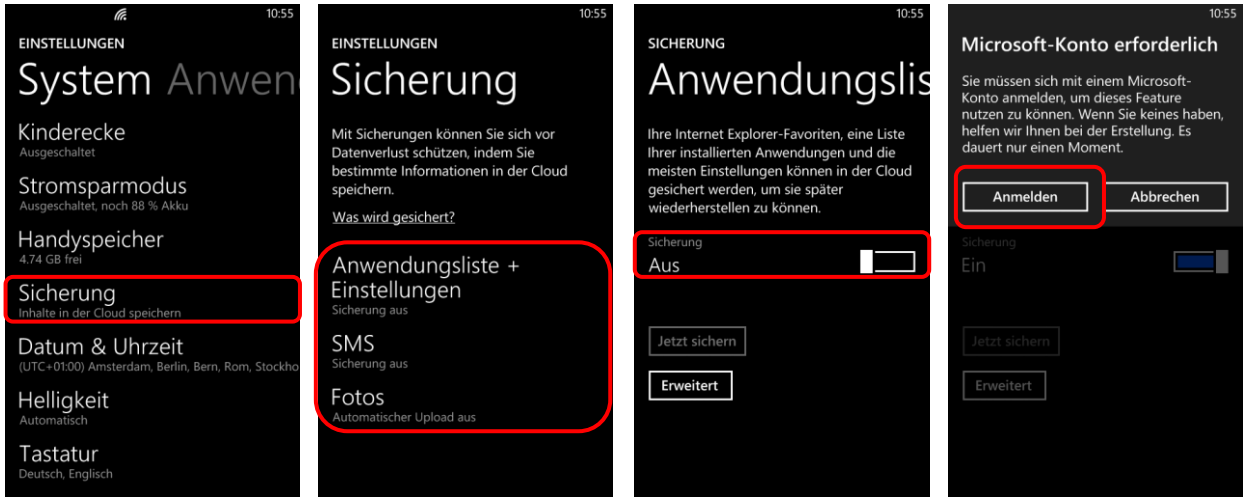


3. Synchronisierung & Backups

Genau wie bei einem PC ist es auch bei einem Smartphone notwendig, regelmäßig Sicherungskopien (Backups) durchzuführen. Im Falle eines Daten- oder Handyverlusts können Sie so auf Ihr Backup zugreifen und haben zumindest den letzten Stand Ihrer gesicherten Daten verfügbar.

Windows bietet mit der Funktion „Sicherung" die Möglichkeit sich vor Datenverlust zu schützen, indem bestimmte Daten im Cloud-Dienst „SkyDrive" gespeichert werden. Sie können von überall auf Ihre Daten zugreifen und benötigen lediglich ein Microsoft-Konto; Wenn Sie bereits Microsoft-Dienste verwendet haben – beispielsweise Hotmail, Skype, Xbox oder Outlook.com – haben Sie schon ein Konto. Zusätzlich können Sie mit der SkyDrive-App Ihre Daten automatisch auf Ihren Geräten synchronisieren lassen.

Datensicherung mittels SkyDrive:
Einstellungen – Sicherung – Anwendungsliste + Einstellungen – Sicherung „Ein"

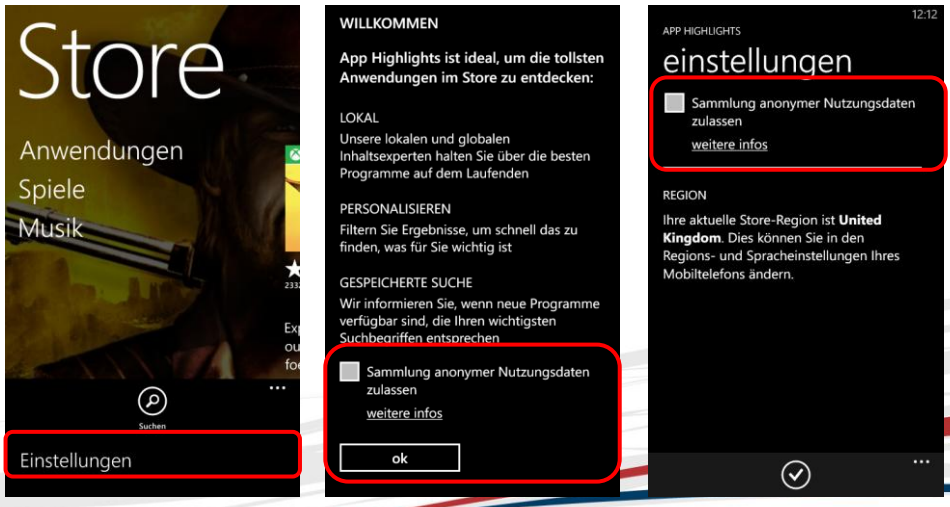


4. Apps! Nur, wie richtig?

Ein Smartphone ohne Apps ist wie Winter ohne Schnee – einfach nicht das Wahre. Jedoch können die kleinen Anwendungen genutzt werden um in Ihr Smartphone und somit an Ihre Daten zu gelangen: diese schädlichen Apps heißen „Malware". Wenn Sie beim Kauf und Download von Apps ein paar wenige Punkte beachten, können Sie ganz leicht dieses Sicherheitsrisiko minimieren.

Beziehen Sie Apps nur aus den offiziellen App-Stores!
Natürlich kann es auch hier keine endgültige Garantie geben, aber die offiziellen Stores von Apple (App Store: http://itunes.apple.com), von Android (Google Playstore: http://play.google.com) und Windows (Windows Phone Store: http://.windowsphone.com/store) sind definitiv vertrauenswürdiger als andere.

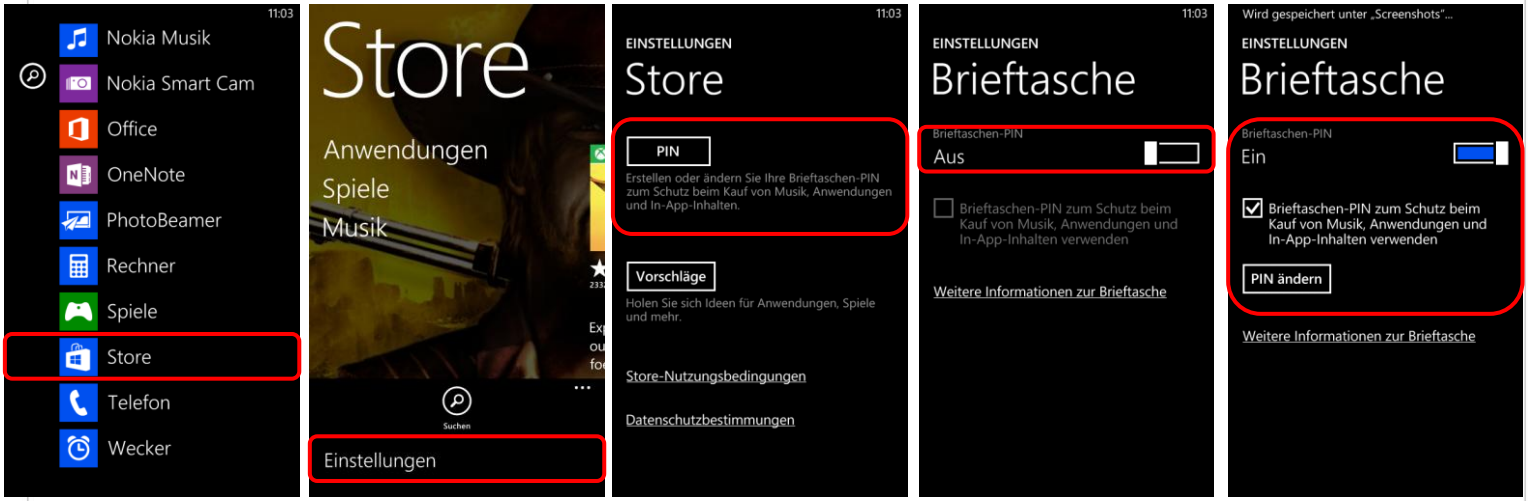
Achtung: Im Windows Store werden anonyme Nutzungsdaten gesammelt. Wenn Sie das nicht möchten, deaktivieren Sie diese Einstellung.



Bei Windows Phones haben Sie mit der Funktion „Brieftasche" die Möglichkeit den App-Kauf und den In-App-Kauf durch ein Passwort zu sperren. Somit muss vor jedem Download oder Kauf der selbstgewählte PIN-Code eingeben werden, unbeabsichtigte Käufe können so leicht verhindert werden.

PIN-Sperre für App-Kauf bei Windows:

Einstellungen – Anwendungen – Unbekannte Quellen



Testen Sie Ihre Apps zuerst!

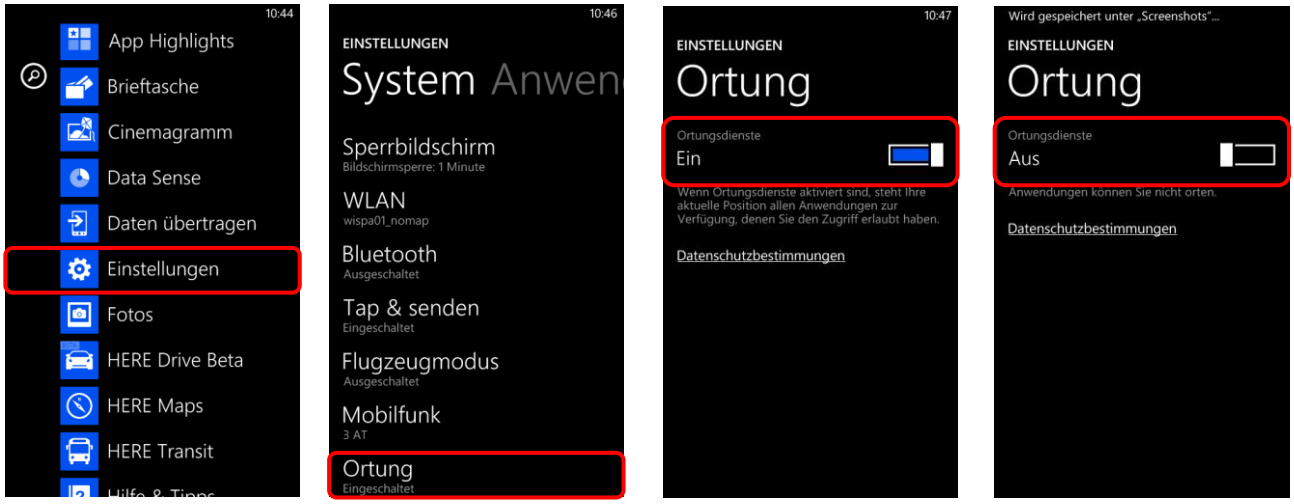
Ein weiterer Vorteil des Kaufes über die offiziellen Stores ist, dass Sie in den meisten Fällen ein Rückgaberecht haben. Beim Windows Phone Store haben Sie leider nicht die Möglichkeit der App-Rückgabe, können aber die meisten Anwendungen für einen begrenzten Zeitraum kostenlos testen. Die Probezeit und die Einschränkungen aller Funktionen können je nach App-Entwickler unterschiedlich ausfallen. Erst nach Ablauf dieser Testphase können Sie sich für den Kauf der Anwendung entscheiden.

Stimmen Sie nicht allen App-Zugriffsberechtigungen zu!

Vor der endgültigen Installation einer App müssen Sie deren Zugriffsberechtigungen zustimmen. Seien Sie hier vorsichtig und stimmen Sie Berechtigungen nur dann zu, wenn diese notwendig erscheinen. Bösartige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen, die einerseits nicht notwendig sind und andererseits Ihr Smartphone und Ihre Daten angreifbar machen. Handelt es sich zum Beispiel um eine Game-App, braucht diese auch keinen Zugriff auf Ihr Telefonbuch.

Wählen Sie ganz bewusst aus, welche Daten Sie welcher App zur Verfügung stellen wollen. Beispielsweise können Sie vorsehen, dass GPS-Daten Programmen wie einem Navigationssystem oder Routenplaner vorbehalten bleiben. Warum sollten Sie einer App Zugriff zu Daten gestatten, wofür staatliche Einrichtungen in der Regel eine richterliche Anordnung brauchen?

Deaktivierung der GPS-Ortung:
Einstellungen – Ortung – Ortungsdienste „Aus"



5. Virenscanner

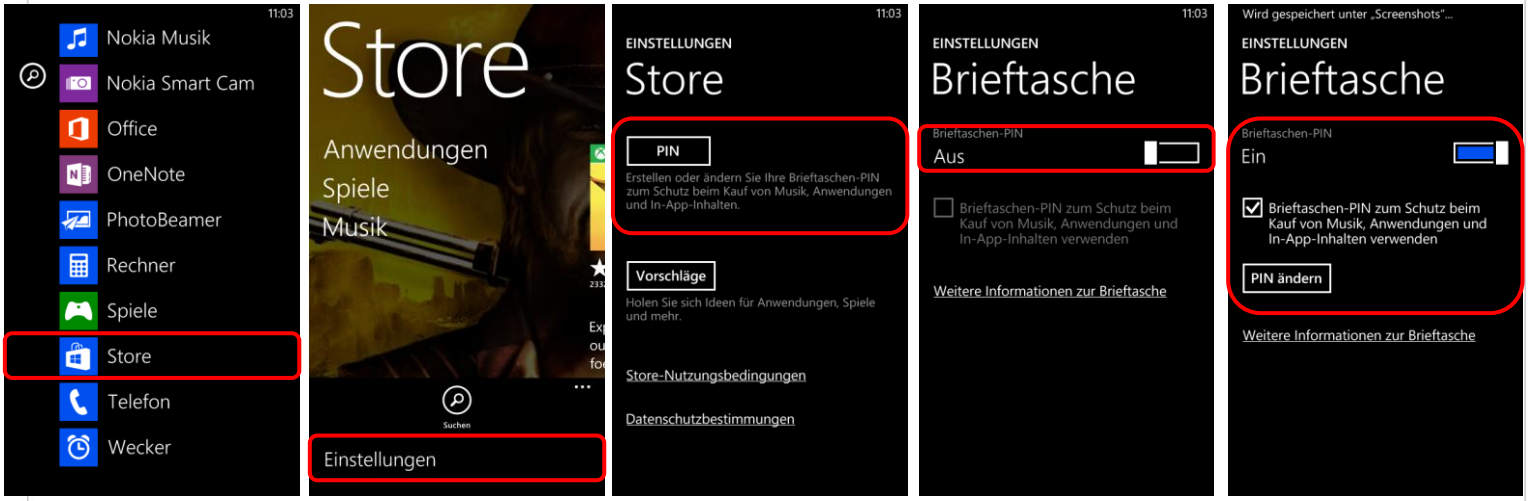
Wenn Sie Ihr Smartphone intensiv nutzen, viele Apps runterladen oder auch Handy-Banking bzw. Handy-Bezahlung verwenden, sollten Sie eventuell die Anschaffung einer Sicherheits-App andenken. Virenschutzprogramme durchsuchen das Smartphone nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren bzw. beseitigen diese wenn möglich. Wenn Sie die Sicherheit Ihrer Daten erhöhen möchten, sollten Sie sich auf jeden Fall eine Virenscanner-App zulegen. Speziell beim Kauf eines Virenscanners empfiehlt es sich natürlich, besonders aufmerksam und auf Ihre persönlichen Bedürfnisse abgestimmt auszuwählen!

6. Kostenfalle In-App-Käufe

Bei manchen Apps (z.B. Spielen) besteht die Möglichkeit unbeabsichtigt in den Anwendungen Guthaben oder Punkte zu kaufen, ohne den klassischen Bestellvorgang zu durchlaufen (so genannte „In-App-Käufe"). Damit steigt die Gefahr unbeabsichtigt Geld auszugeben. In-App-Käufe können so zur unvorhergesehenen Kostenfalle werden: Besonders Kindern und Jugendlichen ist es oft nicht bewusst, dass sie auf ein kostenpflichtiges Angebot klicken, wenn sie zum Beispiel zusätzliches Spielguthaben erwerben um in einem Spiel schneller voranzukommen.
Bei Windows-Phones haben Sie mit der Funktion „Brieftasche" die Möglichkeit den App-Kauf und den In-App-Kauf durch ein Passwort zu sperren. Somit muss vor jedem Download oder Kauf der selbstgewählte PIN-Code eingeben werden, unbeabsichtigte Käufe können so leicht verhindert werden.

PIN-Sperre für App-Kauf:

Einstellungen – Anwendungen – Unbekannte Quellen

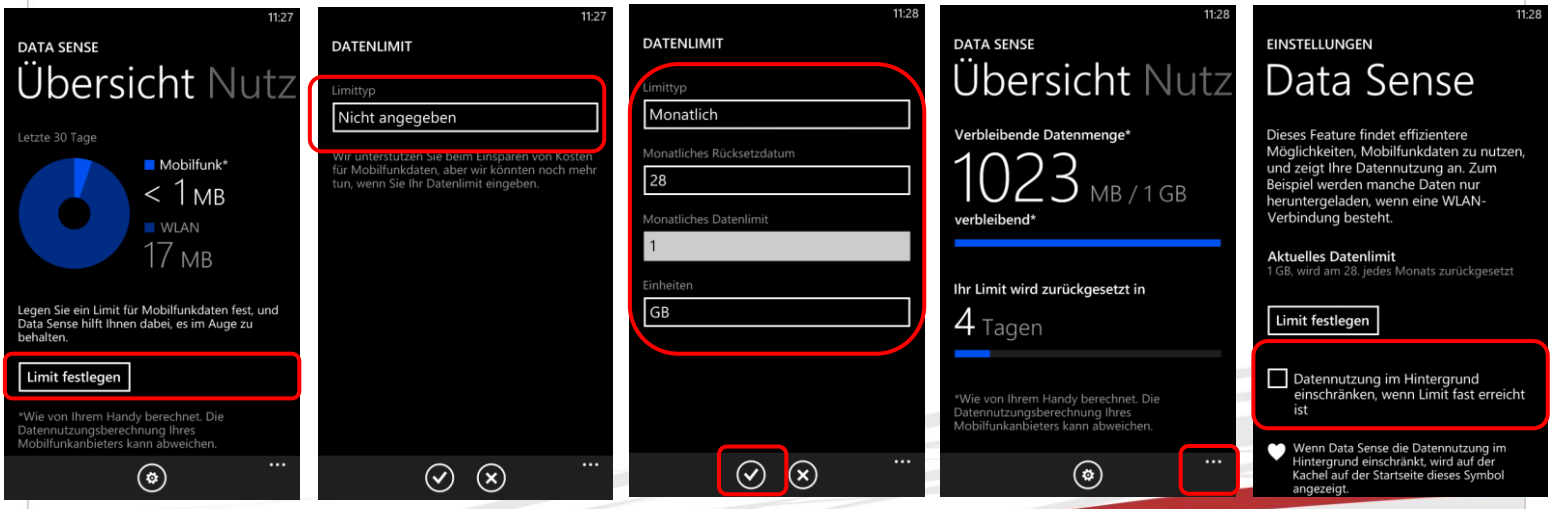


7. Kostenfalle Datentarife

Viele Smartphone-Nutzerinnen und -Nutzer haben Handyverträge mit einem limitierten Internet-Paket, pro Monat können sie somit ein bestimmtes Datenvolumen verbrauchen. Wird dieses überschritten, wird es meistens teuer. Wenn Sie einen Datentarif mit begrenztem Internetvolumen haben, empfiehlt es sich den eigenen Verbrauch im Auge zu behalten.
Windows Phones bieten zur Volumenkontrolle den Menüpunkt „Mobile Datennutzung", bei dem der eigene Verbrauch ermittelt und maximale Obergrenzen festgelegt werden können. Auch können Sie die „unsichtbare" Datennutzung die im Hintergrund abläuft einschränken.

Datenlimit ermitteln & festlegen:

Einstellungen – Data Sense – Limit festlegen

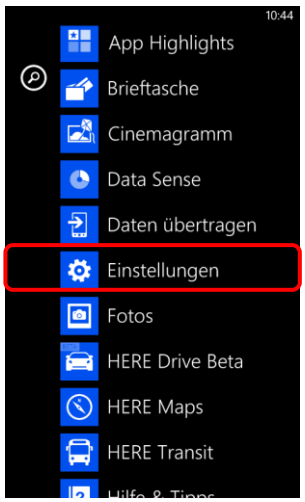


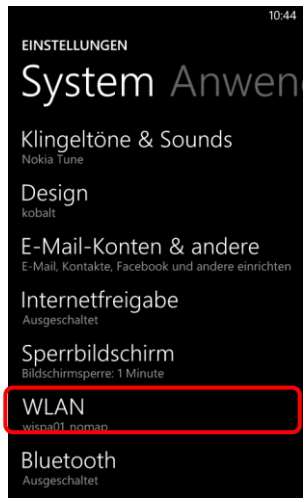
8. WLAN, Bluetooth und mobile Hotspots

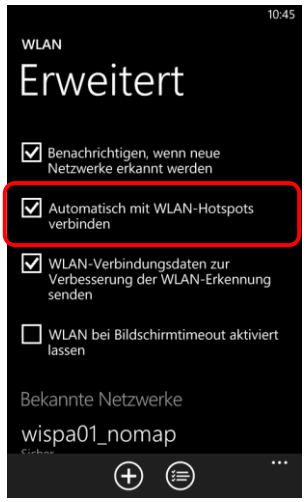
„Home is where your wifi connects automatically."
Wenn sich das Smartphone selbstständig im Büro oder daheim mit dem WLAN verbindet, ist das zwar praktisch und bequem, aber auf Dauer ein Sicherheitsrisiko. Der Datenaustausch über WLAN oder Bluetooth ist oft nur mangelhaft gesichert und kann relativ leicht ausspioniert werden. Sie sollten die WLAN- und Bluetooth-Funktion nur dann einschalten, wenn Sie auf ein lokales WLAN-Netzwerk zugreifen wollen, oder Sie die Bluetooth-Funktion unmittelbar benötigen. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist ein stark reduzierter Akku-Verbrauch.

WLAN bei Windows deaktivieren:

Einstellungen – WLAN – Wlan Netzwerke „Aus"

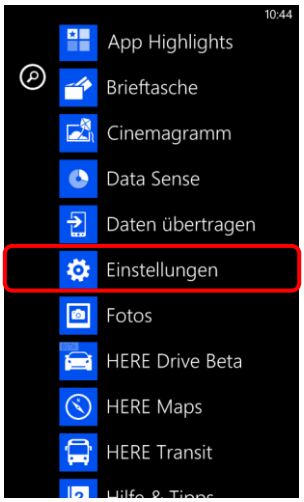


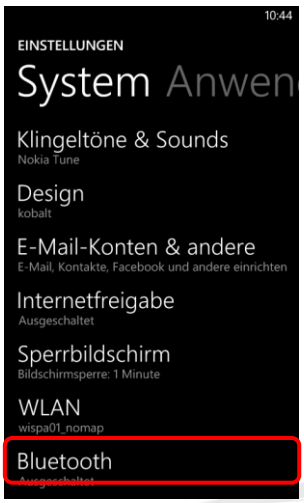


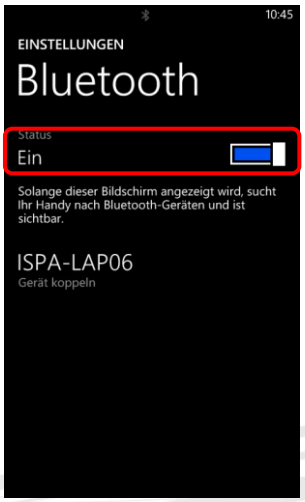


Bluetooth bei Windows deaktivieren:

Einstellungen – Bluetooth – Bluetooth Status „Aus"

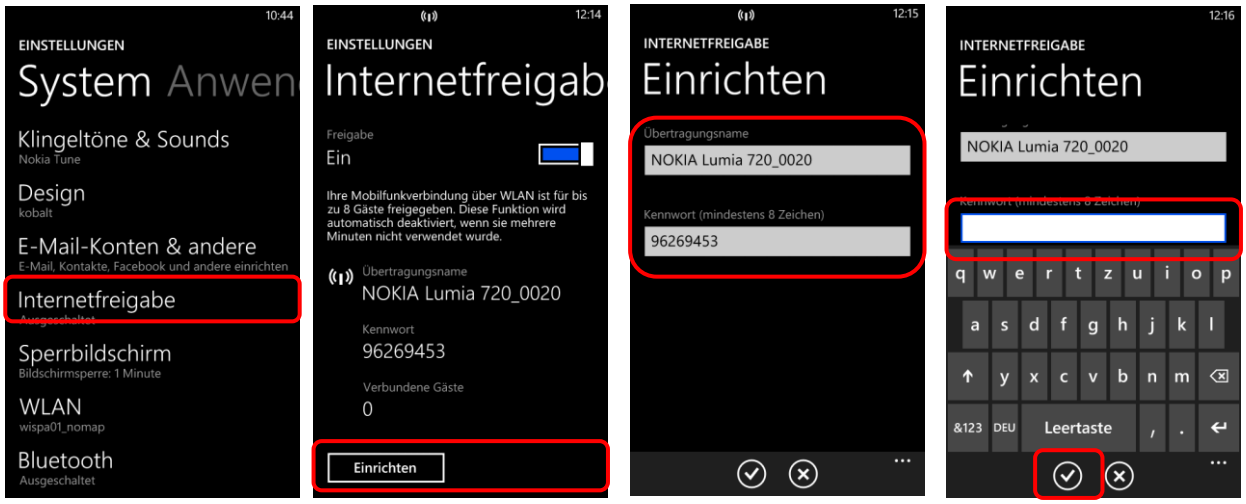






Viele Smartphones mit Datenverbindung bieten die Möglichkeit das Handy als WLAN-Router zu verwenden und so beispielsweise als mobiler Hotspot für den eigenen Laptop zu fungieren. Die Hotspot-Funktion sollten Sie jedenfalls mit einem Passwort sichern und ebenfalls nur bei Bedarf aktivieren.

Hotspot bei Windows einrichten:
Einstellungen – Internetfreigabe – Freigabe „Ein" – Einrichten



9. Jailbreak, Root und gesperrte Smartphones

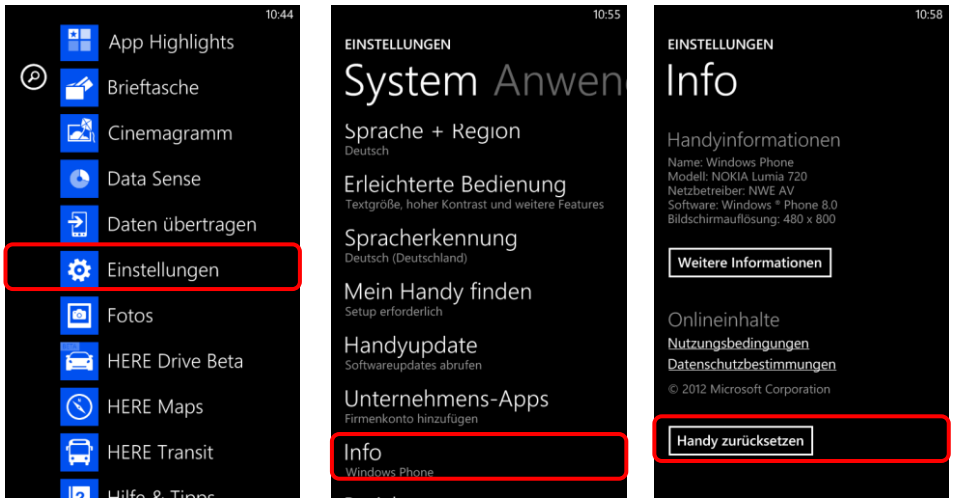
„Jailbreaking" ist das inoffizielle Entsperren von Software und Hardware, meint in den meisten Fällen aber das Entsperren von Smartphones.

Achtung: Durch den Jailbreak kann das Betriebssystem des Smartphones beeinträchtigt oder sogar beschädigt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Jailbreak-Programmen oder von Schadsoftware werden. Zudem fällt das Jailbreaking in eine rechtliche Grauzone und kann unter Umständen die Garantie beeinträchtigen!

10. Verkaufen, Verschenken & Verborgen

E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: auf Ihrem Smartphone sind sehr viele persönliche Daten gesammelt. Sollten Sie sich dazu entschließen, Ihr Smartphone weiterzugeben oder es sogar zu verkaufen, sollten Sie Ihr Gerät unbedingt in den Werkzustand zurücksetzen.

Auf Werkzustand zurücksetzen:
Einstellungen – Info – Handy zurücksetzen



Achtung: Um die Weitergabe Ihrer persönlichen Daten zu verhindern sollten Sie alle vorhandenen Speicher löschen, also nicht nur den internen Handyspeicher, sondern auch den externen (die Micro-SD-Karte). Hierfür reicht es nicht diese einfach nur zu löschen oder das Smartphone auf die Werkseinstellungen zurückzusetzen, da mittels einiger Programme gelöschte Daten wiederhergestellt werden können. Erst spezielle Löschprogramme machen durch mehrfaches Überschreiben des Speichers eine Wiederherstellung der Daten unmöglich.

11. Smartphone-Finder: finden oder sperren

Die meisten Smartphones bieten mittlerweile die Möglichkeit es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen.
Bei Windows heißt diese Funktion „Mein Handy finden". Sie können Ihr Smartphone über Windowsphone.com anrufen, sperren, löschen oder auf einer Karte anzeigen lassen, sowie Anwendungen an das Gerät schicken. Hierzu muss die Funktion aktiviert sein und Sie benötigen Ihre Windows Live ID.
Es gilt aber bei dieser Funktion zwischen Privatsphäre und Sicherheit abzuwägen: möchten Sie solche Funktionen nutzen, müssen Sie das GPS-Tracking aktivieren.

Aktivierung des Telefonfinders bei Windows:

Einstellungen – Mein Handy finden – Meine Position speichern „Ein"

12. Das kindersichere Smartphone

Um Ihr Smartphone bei Bedarf kindersicher zu machen, sollten Sie das Roaming sowie In-App-Käufe deaktivieren und ebenso Mehrwertdienste sperren. In letzter Konsequenz können Sie das Internet deaktivieren und in den Flugmodus wechseln.
Mittlerweile gibt es auch zahlreiche Apps, die sich dem Thema Kindersicherheit widmen. Diese sind dann aber Endgerät-basiert und funktionieren primär über Sperren und Filter.
Bei Windows Phones gibt es hierzu die Funktion „Kinderecke". Hier können Sie ein eigenes Profil für kleine Userinnen und User einrichten, indem Sie genau festlegen, welche Programme, Videos und Fotos verfügbar sein sollen und welche nicht. Ist die Kinderecke einmal eingerichtet, können Sie diese noch individuell anpassen und nach Bedarf ein- und ausschalten. Die Kinderecke kann nur durch die Eingabe eines vorher festgelegten Passwortes wieder deaktiviert werden.

Aktivierung der Kinderecke bei Windows:

Einstellungen – Kinderecke