Sicherheitseinstellungen für Tablets

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 Surface Pro
Betriebssystem: Windows 10 Pro Version 1607

Gefördert durch die Europäische Union – Safer Internet Projekt.

Schutz vor unbefugtem Zugriff auf das Gerät

Wie auch das Smartphone ist das Tablet 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. Diese Informationen sollten durch ein starkes Passwort geschützt werden.

Wie bei vielen Sicherheitsmaßnahmen müssen Nutzerinnen und Nutzer auch bei der Wahl eines Passwortes eine individuelle Abwägung zwischen Komfort im täglichen Umgang mit dem Tablet und höherer Sicherheit treffen. Die höchste Sicherheit bietet ein längeres Passwort, besonders wenn dabei eine Kombination aus Zahlen, Groß- und Kleinbuchstaben und Sonderzeichen verwendet wird. Um „komplizierte" Passwörter nicht zu vergessen, bieten sich die Anfangsbuchstaben eines einprägsamen Merksatzes an. Beispielsweise ergäbe sich aus dem Merksatz „Ich mag Äpfel & bin 1980 geboren" das Passwort „ImÄ&b1980g". Die gewählte Kombination sollte 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.

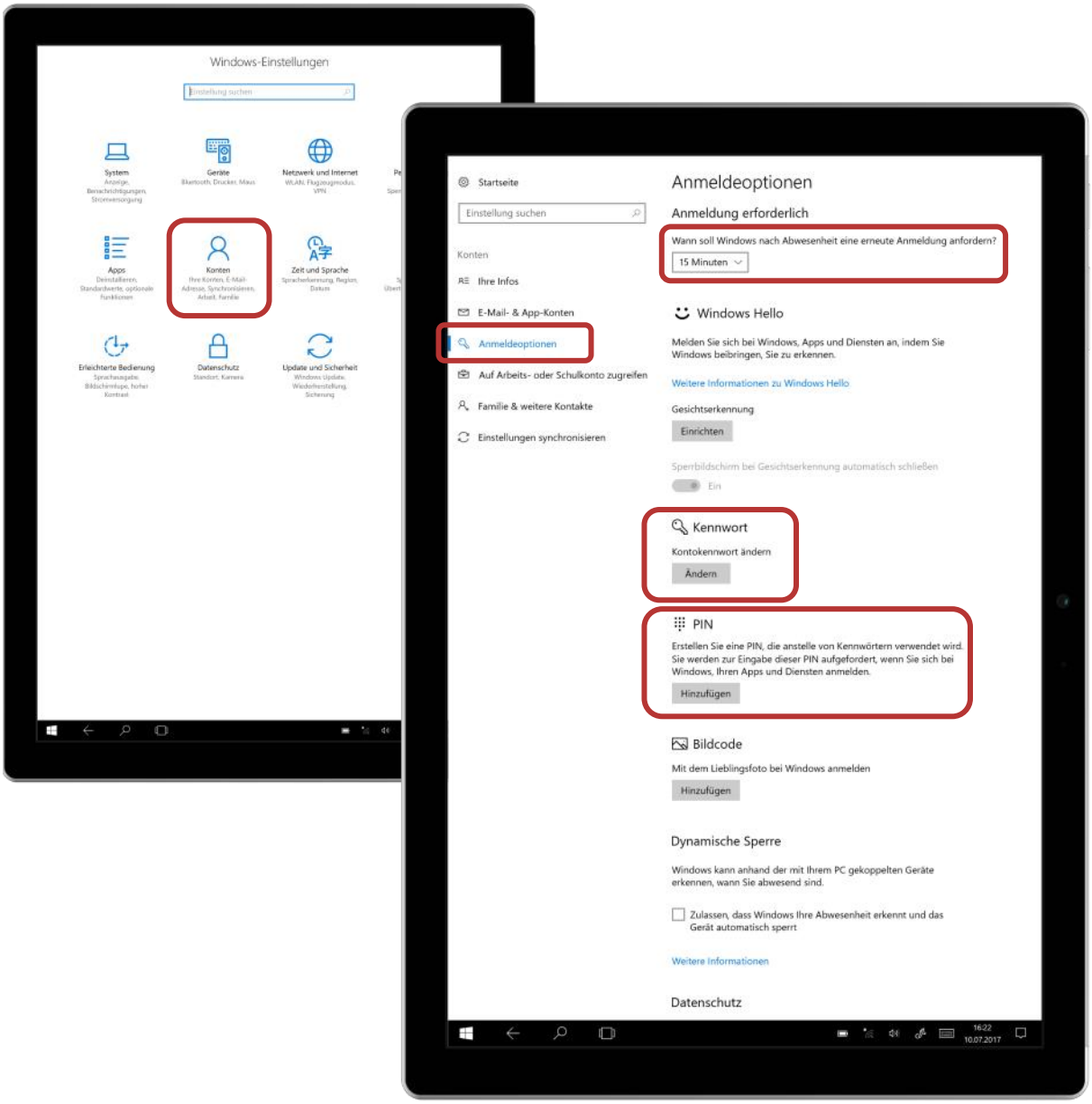
Windows bietet auch alternative Formen der Authentifizierung an: So kann etwa auch ein Ziffern-PIN vergeben werden, und je nach Endgerät ist es auch möglich, sich mittels Fingerabdruck-, Gesichts- oder Iriserkennung anzumelden („Windows Hello"). Bei der Verwendung eines Nummern-PINs sollten leicht zu erratende Kombinationen wie etwa der eigene Geburtstag oder „1234" vermieden werden. Auch hier gilt natürlich: Je länger der Zifferncode, desto sicherer.

Auf jeden Fall sollte darauf Acht gegeben werden, dass die Eingabe des Passworts bzw. PIN-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. Das Entsperren mittels Fingerabdrucksensor bietet diesbezüglich guten Schutz, allerdings sollte man sich bewusst sein, dass auch diese Form der Sicherung keinen absolute Sicherheit bietet und von Angreifern umgangen werden kann.

Die Anmeldeoptionen bearbeiten

In den Windows-Einstellungen auf „Konten" tippen. Unter „Anmeldeoptionen" lässt sich das Kennwort für den eigenen Account ändern. Zudem können alternative Formen der Authentifizierung wie etwa ein PIN-Code oder Gesichtserkennung festgelegt werden.

Der Menüpunkt „Anmeldung erforderlich" legt fest, nach welchem Zeitraum bei Inaktivität die Bildschirmsperre aktiviert wird.

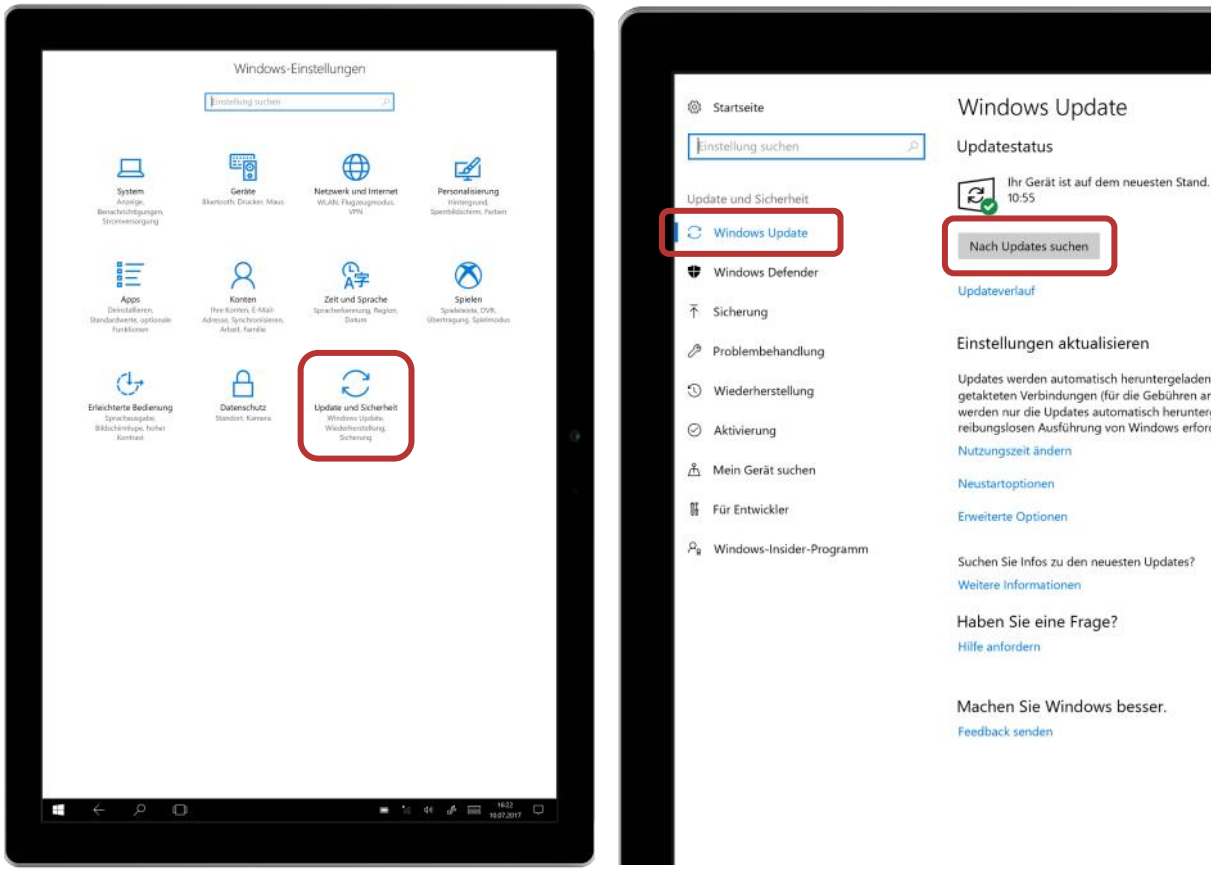


Software-Updates

Die vom Hersteller bereitgestellten Software-Updates („Windows-Update“) sollten regelmäßig durchgeführt werden. Sie enthalten kleine Systemverbesserungen, reparieren Fehler und schließen eventuelle Sicherheitslücken. Üblicherweise sucht das Windows-Tablet 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 „Windows-Update“ werden gegebenenfalls verfügbare Aktualisierungen angezeigt bzw. können mittels „Updates suchen“ angefordert werden.



Datenschutzeinstellungen

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

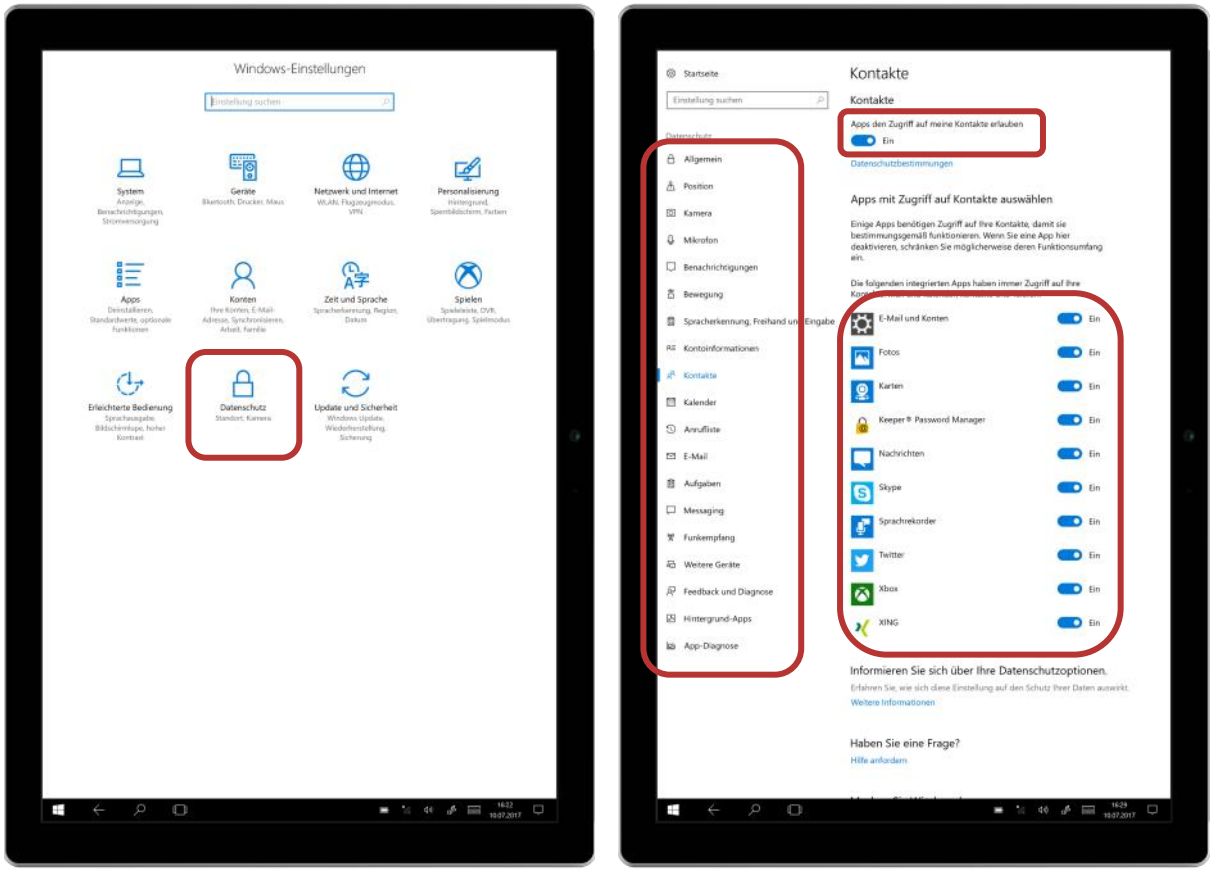
Um sich vor Schadsoftware zu schützen, sollten Apps von Drittanbietern nur aus dem Windows Store geladen werden. Diese müssen nämlich ein Testverfahren durchlaufen, bevor sie zum Download verfügbar sind und auf dem Gerät installiert werden können. Auch dieses Verfahren kann naturgemäß keinen absoluten 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 Tablet so vor der unachtsamen 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 vom Betriebssystem Berechtigungen an, etwa für den Zugriff auf das Adressbuch, obwohl diese für die Funktionalität der App gar nicht nötig sind. Hier sollte man regelmäßige Überprüfungen vornehmen und Berechtigungen nur dann aktivieren, wenn diese 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

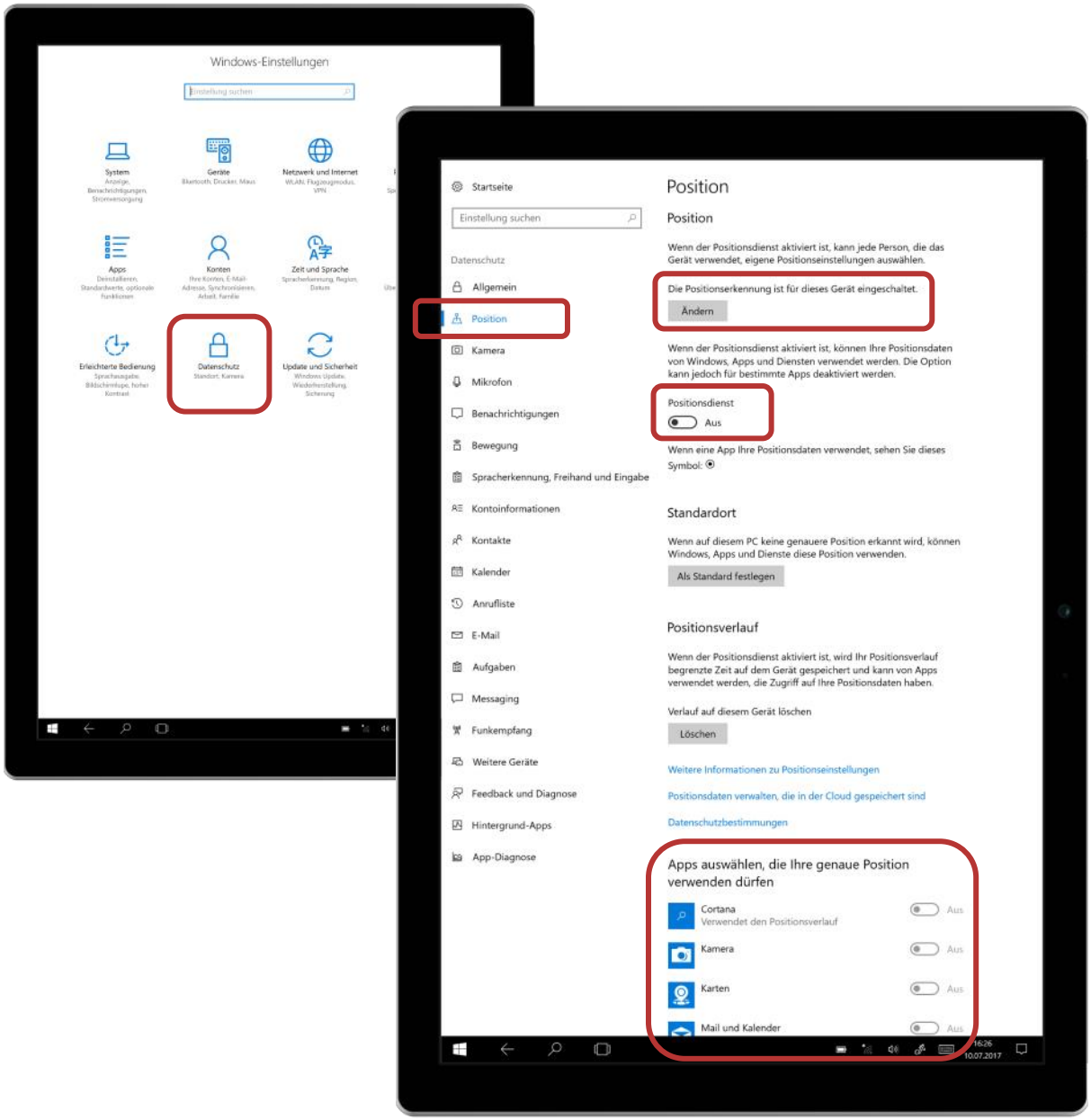
Der Menüpunkt „Datenschutz" in den Windows-Einstellungen ermöglicht es genau festzulegen, welche Apps auf den eigenen Standort („Position"), die Kontakte, Kalender, aber auch Sensoren wie Kamera oder Mikrofon zugreifen können. Es empfiehlt sich, diese Berechtigungen möglichst restriktiv zu setzen.



Beispiel: Zugriff auf den eigenen Standort einschränken

Die sogenannten „Positionsdienste" ermöglichen dem Windows Tablet 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 diesen 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 nicht unwesentlich viel Strom benötigt. In den Einstellungen für Positionsdienste lässt sich für jede App einzeln einstellen, ob diese auf den eigenen Standort zugreifen kann. Zudem lässt sich die Positionsbestimmung auch vollständig deaktivieren.



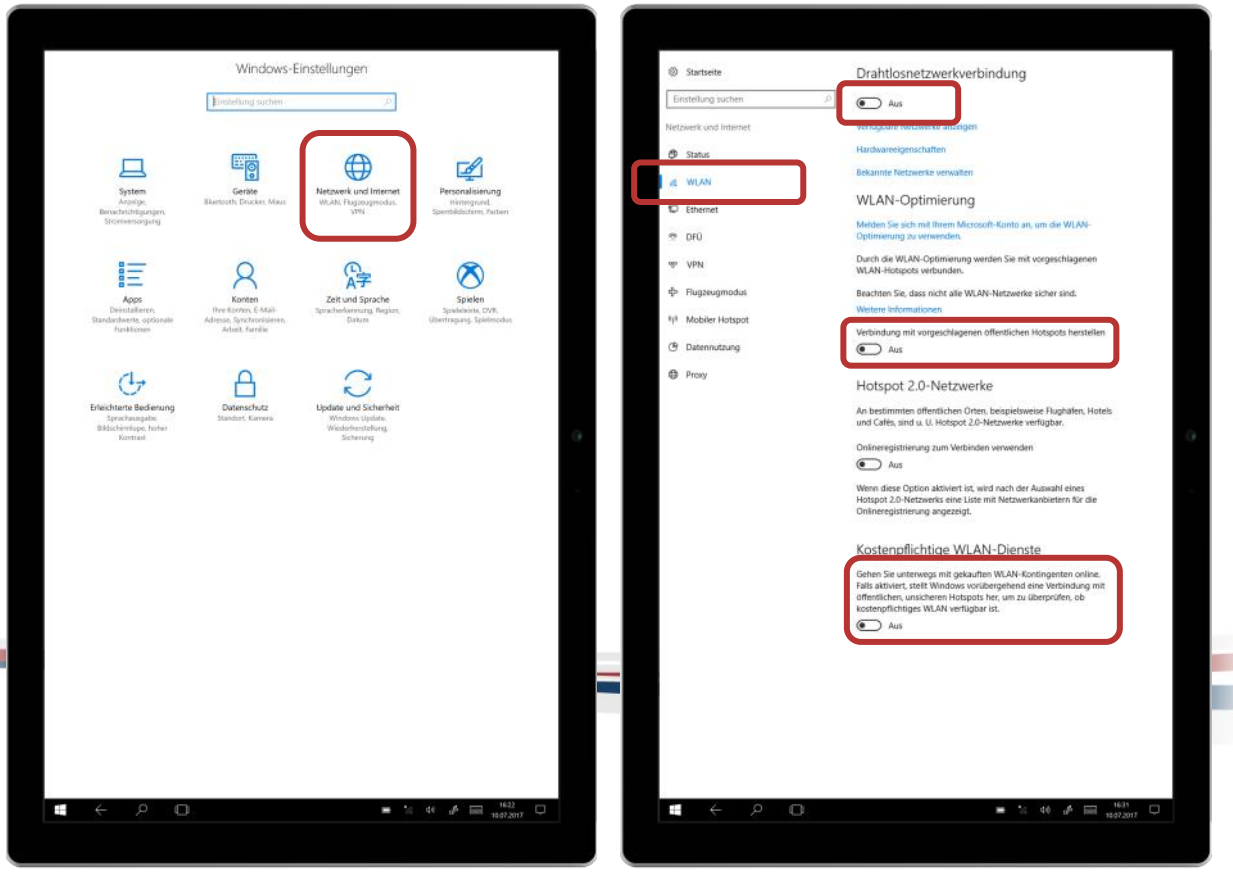
WLAN, Bluetooth und mobile Hotspots

„Home is where your wifi connects automatically“: Wenn sich das Tablet 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.

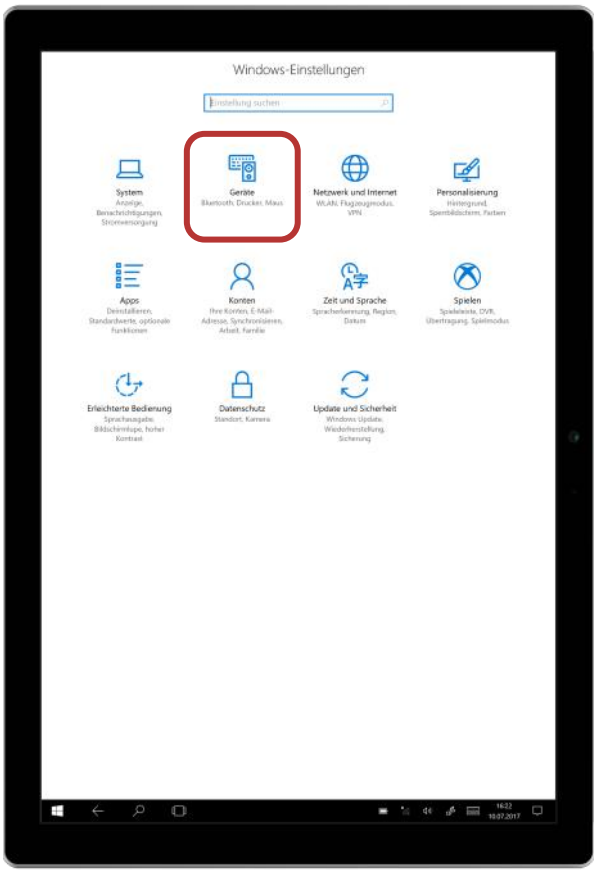
WLAN deaktivieren

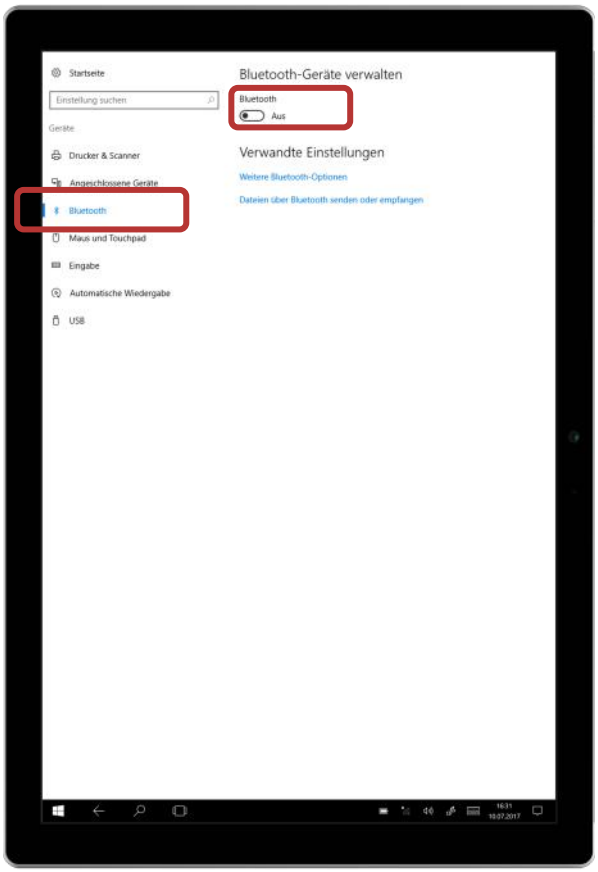
In den Einstellungen auf „Netzwerk & Drahtlos“ tippen. Unter „WLAN“ werden die verfügbaren Netzwerke angezeigt und die WLAN-Funktion kann abgeschalten werden. Zudem sollte konfiguriert werden, dass sich das Tablet nicht automatisch mit offenen WLAN-Netzen verbindet. Diese sind oft nur mangelhaft gesichert und können es Angreifern ermöglichen, den gesamten Netzwerkverkehr mitzulesen.

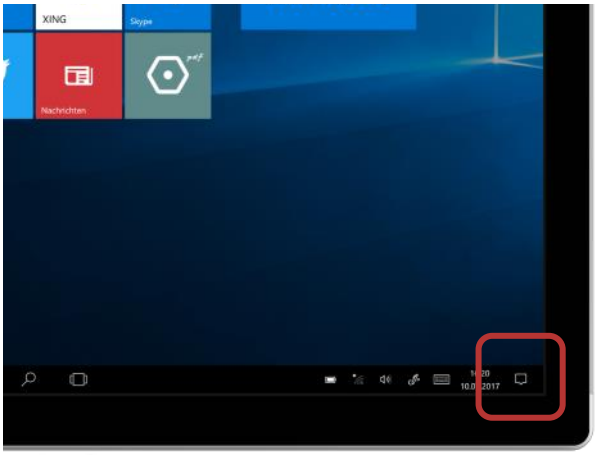


Bluetooth deaktivieren

In den Einstellungen auf „Geräte“ tippen. Unter „Bluetooth“ kann die Funktion abgeschalten werden.







Tipp: Alternativ lassen sich WLAN und Bluetooth auch mittels der Funktion „Schnelle Aktionen“ einfach und schnell an– bzw. abschalten. Diese ist Teil des Info-Centers von Windows und findet sich ganz rechts in der Taskleiste.

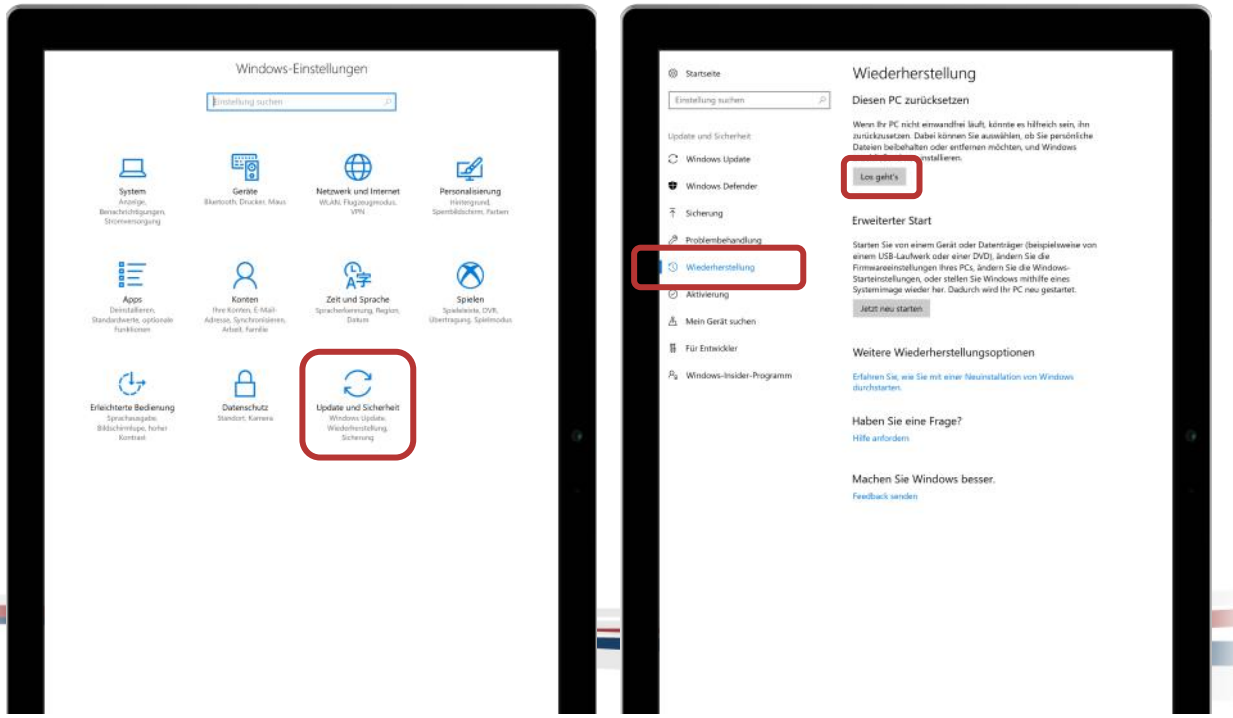
Verkaufen, Verschenken & Verborgen

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

Um die Weitergabe persönlicher Daten zu verhindern, sollte der Speicher des Tablets nach Möglichkeit vollständig zurückgesetzt werden. Hierfür reicht es nicht, diesen einfach nur zu löschen, da gelöschte Daten unter Umständen wiederhergestellt werden können. Um Daten vollständig und sicher vom Gerät zu entfernen, gibt es speziellen Löschsoftware, die den Speicher mehrmals mit „Unsinn" überschreibt. Microsoft bietet für Surface-Tablets ein eigenes Programm dafür an, den Surface Data Eraser (docs.microsoft.com/de-de/surface/microsoft-surface-data-eraser). Auf jeden Fall sollte das Gerät aber auf den Werkzustand zurückgesetzt werden.

Auf Werkzustand zurücksetzen

In den Einstellungen auf „Update und Sicherheit" tippen. Unter „Wiederherstellung" findet sich die Option „Diesen PC zurücksetzen". Mit dieser Funktion können alle persönlichen Inhalte (Apps, Bilder, Musik, Videos, Konten, etc.) vom Gerät entfernt werden und das Tablet wird auf Werkseinstellungen zurückgesetzt.



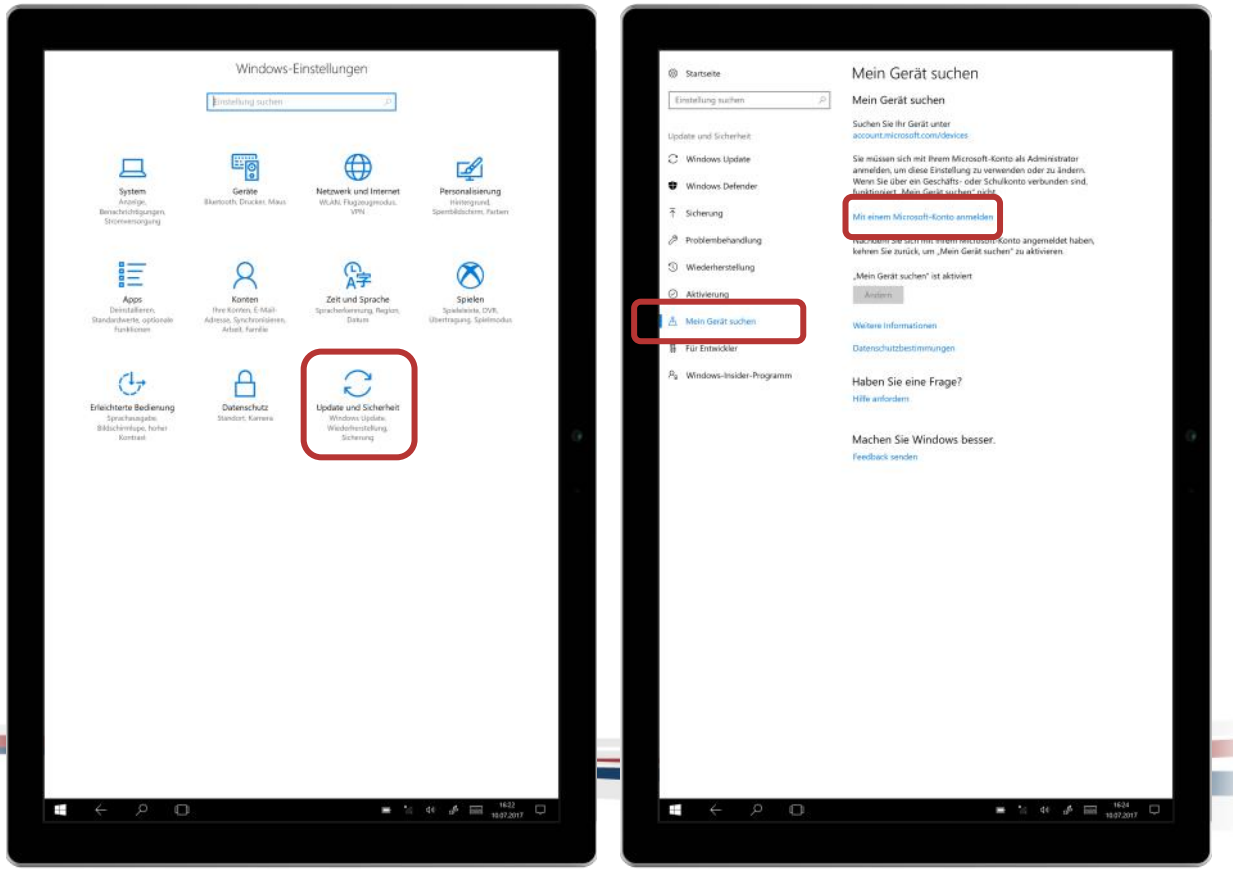
„Mein Gerät suchen“: Das Tablet finden, sperren und löschen

Die meisten Tablets 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 Gerät suchen“. Ist diese Funktion aktiviert, kann das Tablet über das Microsoft-Konto geortet, gesperrt oder die Daten können aus der Ferne gelöscht werden.

Damit dieser Fernzugriff-Service funktioniert, muss der Standortzugriff in den Einstellungen erlaubt werden. Ebenso muss der Standortzugriff beim Microsoft-Konto aktiviert werden. Um das Tablet im Fall des Falles zu orten, müssen sich Nutzerinnen und Nutzer in der Web-App einloggen (account.microsoft.com/devices).

Aktivierung von „Mein Gerät suchen“

In den Windows-Einstellungen auf „Update und Sicherheit“ tippen. Unter „Mein Gerät finden“ steht nach Anmeldung mit einem Microsoft-Konto die Funktion zur Aktivierung bereit.



Einrichten von „Family Features" - das kindersichere Tablet

Um das Tablet bei Bedarf kindersicher zu machen, bietet Windows eine Reihe an „Family Features" an: So lässt sich etwa ein eigenes Profil für die jüngeren Userinnen und User einrichten, es ist möglich, sich Berichte zur Online-Aktivität der Kinder anzeigen zu lassen und Zeitlimits für die Benutzung des Tablets können festgelegt 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 Erziehungsberechtigte 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.

Ein Kinderkonto anlegen

Um die Familien-Funktionen zu nutzen, benötigt das Kind ein eigenes Microsoft-Konto. Der Vorteil: Dadurch gelten die Einschränkungen, die für ein Kind eingestellt werden, für jedes Tablet, jeden PC und jedes Windows-Smartphone, auf dem es sich anmeldet. Dazu in den Windows-Einstellungen auf „Konten" tippen. Unter „Familie und weitere Benutzer" findet sich die Schaltfläche „Familienmitglied hinzufügen". Mit der Option „Kind hinzufügen" und Eingabe der E-Mail-Adresse des Kindes lässt sich das Kinderkonto anlegen. Ist der E-Mail-Adresse noch kein Microsoft-Konto zugeordnet, kann dies im nächsten Schritt erledigt werden. Wenn das Kind noch nicht über eine eigene E-Mail-Adresse verfügt, kann diese kostenlos angelegt werden. Danach wird eine Bestätigungsnachricht an die E-Mail-Adresse des Kindes gesendet. Nach einem Klick auf den darin enthaltenen Link ist das Konto freigeschalten und kann zur Anmeldung auf dem Tablet benutzt werden.

Familieneinstellungen/Einschränkungen online verwalten

Um die Beschränkungen und Zeitlimits zu bearbeiten oder sich Berichte über die Aktivitäten des Kindes anzeigen zu lassen, steht die Online-Verwaltung der Familieneinstellungen unter account.microsoft.com/family bereit. Nach Anmeldung mit dem eigenen Benutzerkonto können unter dem Menüpunkt „Familie" die Einstellungen angezeigt und bearbeitet werden.

Unter „Letzte Aktivitäten" können Berichte zu den Aktivitäten des Kindes am Tablet angezeigt werden, etwa welche Websites besucht wurden, welche Apps und Spiele heruntergeladen und gespielt wurden und wie viel Zeit das Kind insgesamt mit dem Gerät verbracht hat.

In der Rubrik „Webbrowsen" können nur bestimmte Websites zugelassen oder blockiert werden, alternativ lässt sich der Zugriff auf Websites mit entsprechender Altersfreigabe einschränken. Was für Jugendliche „ungeeignet" ist, legt allerdings Microsoft nach eigenen Kriterien fest, die nicht im Detail eingesehen oder bearbeitet werden können.

Unter „Apps, Spiele und Medien" kann der Zugriff auf Anwendungen, Spiele und Inhalte beschränkt werden.

Mittels „Computerzeit" lässt sich festlegen, wie lange das Kind das Tablet verwenden darf. Neben einer maximalen täglichen Nutzungsdauer kann z.B. auch eingestellt werden, dass eine Verwendung nur bis spätestens 21 Uhr möglich ist.

Tipp: Weitere Informationen zur Medienkompetenz von Kindern und Jugendlichen für Eltern, Lehrende und sonstige erwachsene Bezugspersonen:

Saferinternet.at
Das Internet sicher nutzen!