ispa
Internet Service Providers Austria

Sicherheitseinstellungen für Tablets

Windows

AK NIEDER ÖSTERREICH

Saferinternet.at
Das Internet sicher nutzen!

Co-financed by the European Union
Connecting Europe Facility

Inhaltsverzeichnis

Hinweis: Je nach Hersteller Ihres Geräts können die genauen Bezeichnungen für einzelne Einstellungen bzw. deren Positionen im Menü unter Umständen von den Darstellungen in diesem Leitfaden abweichen. Die Funktionen sind allerdings bei den meisten Geräten vorhanden. Konsultieren Sie im Zweifelsfall die Dokumentation des Herstellers.

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

6. aktualisierte Auflage
Wien, 2020
Redaktion: Birgit Mühl & Jonas Müller
Endgerät: Microsoft Surface Pro 7
Betriebssystem: Windows 10 Pro Version 1909

Gefördert durch die Europäische Union – Safer Internet Projekt. Alle Angaben erfolgen ohne Gewähr. Eine Haftung der Autorinnen und Autoren, durch die ISPA, das Projekt Saferinternet.at oder die Europäische Union ist ausgeschlossen.

Diese Broschüre wurde in Kooperation mit der Arbeiterkammer Niederösterreich im Rahmen ihrer Digitalisierungsoffensive umgesetzt. Die Arbeiterkammer macht Arbeitnehmerinnen und Arbeitnehmer fit für die digitale Zukunft. Infos unter noe.arbeiterkammer.at/zukunftsprogramm. Eine Haftung durch die Arbeiterkammer Niederösterreich ist ausgeschlossen.

Vorwort

Ein Tablet ist ein praktischer Begleiter und aus dem Alltag nicht mehr wegzudenken. Bereits fast 40 Prozent der Bevölkerung in Österreich verwenden ein Tablet und konsumieren darüber Medien und Informationen, nutzen soziale Netzwerke, recherchieren zu Produkten und Dienstleistungen, machen Preisvergleiche oder erledigen ihre Einkäufe. Doch nicht alle Nutzerinnen und Nutzer sind Profis, weshalb sie Unterstützung benötigen. Damit Sie Ihr Tablet sicher einsetzen können, sollten Sie einige Dinge beachten. Dieser Ratgeber hilft Ihnen mit Tipps und Schritt-für-Schritt-Anleitungen grundlegende Sicherheitseinstellungen an Ihrem Smartphone vorzunehmen.

Schutz vor unbefugtem Zugriff auf das Gerät

Es gibt verschiedene Möglichkeiten sein Tablet vor unbefugtem Zugriff z. B. bei Verlust oder Diebstahl zu schützen. Die meisten Tablets bieten zwei Sicherheitsfunktionen an: einmal die PIN-Abfrage beim Einschalten des Gerätes (SIM-Kartensperre oder PIN-Eingabe) und als zusätzliche Option die Passwortabfrage bei der Aufhebung des Ruhezustandes (Bildschirmsperre).

SIM-Karte schützen

Mittlerweile werden auch viele Tablets mit SIM-Karten ausgestattet. Die SIM-PIN-Abfrage schützt aktiv vor missbräuchlicher Verwendung und sollte auch am Tablet keinesfalls aus Bequemlichkeit ausgeschaltet werden. Im Falle von Verlust oder Diebstahl kann diese Bequemlichkeit unangenehme und teure Konsequenzen haben. Denn die SIM-Karten verbleiben im Normalfall im Eigentum der Netzbetreiber und werden den Kundinnen und Kunden nur zur Verfügung gestellt. Diese verpflichten sich, die SIM-Karte vor schädlichen Einflüssen und Missbrauch durch Dritte zu schützen. Die Endnutzerinnen und -nutzer haften deshalb auch bis zur Sperrmeldung an den Netzbetreiber für fast alle Entgeltforderungen, die sich auf Missbrauch der SIM-Karte und das Verschulden der Teilnehmerin oder des Teilnehmers zurückführen lassen, z. B. eben auch durch das Deaktivieren des SIM-PINs. Nähere Informationen dazu finden Sie beispielsweise in den allgemeinen Geschäftsbedingungen ihres Netzbetreibers.

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‹.

WICHTIG

Das gleiche Passwort sollte bei anderen Diensten nicht nochmals verwendet werden, da man es so potenziellen Angreifern einfach macht, mit nur einem Passwort auf mehrere Konten 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.

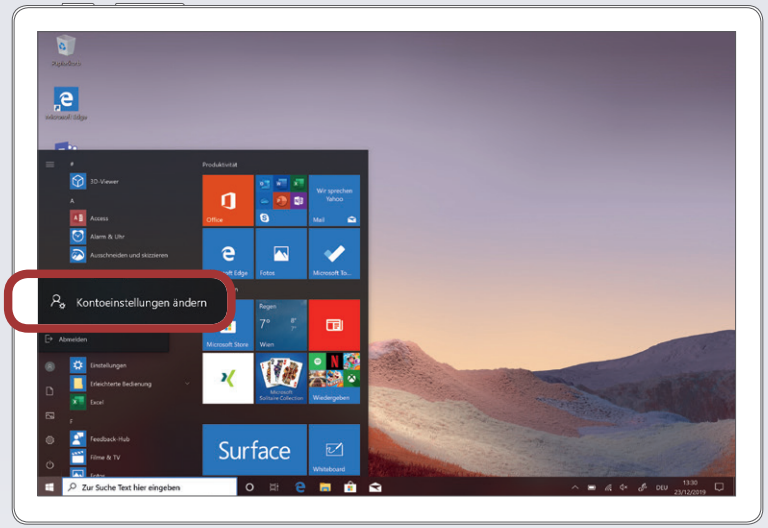
Auf jeden Fall sollte darauf Acht gegeben werden, dass die Eingabe des Passworts bzw. PIN-Codes stets unauffällig erfolgt. Viele Sicherheitsangriffe sind überraschend trivial, eine weit verbreitete Methode ist etwa das Abschauen oder Abfotografieren von Zugangsdaten und Passwörtern bei deren Eingabe. Besonders auf öffentlichen Plätzen, in dicht gedrängten Verkehrsmitteln oder bei neugierigen Sitznachbarinnen und 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 keine absolute Sicherheit bietet und von Angreifern umgangen werden kann.

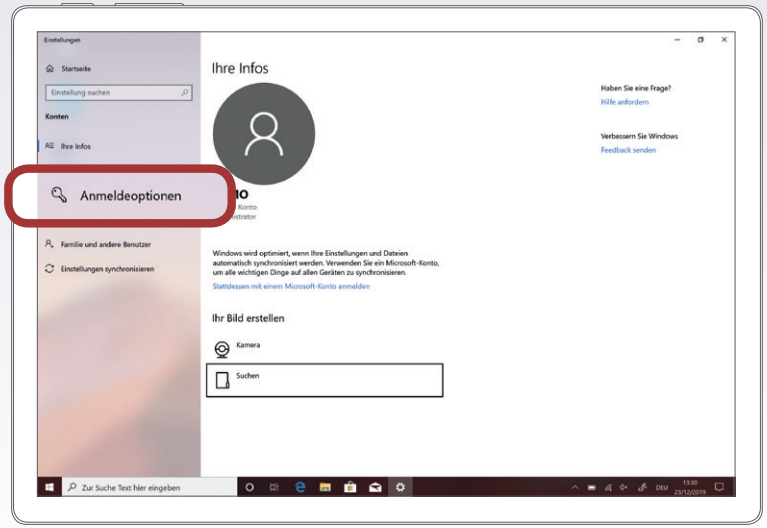
Schutz vor unbefugtem Zugriff auf das Gerät

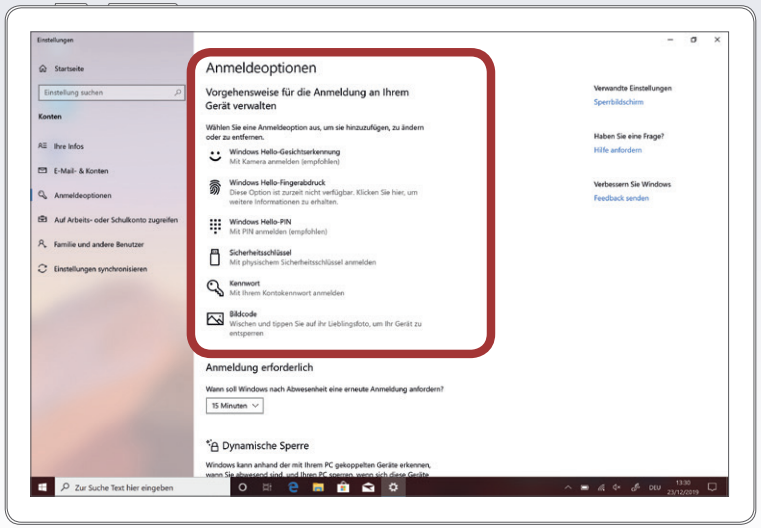
Die Anmeldeoptionen bearbeiten

Start ▸ Konto ▸ Kontoeinstellungen ändern ▸ Anmeldeoptionen ▸ gewünschte Option auswählen

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, ein physischer Sicherheitsschlüssel, Bildcode oder Gesichtserkennung festgelegt werden.
Der Menüpunkt ›Anmeldung erforderlich‹ legt fest, nach welchem Zeitraum bei Inaktivität die Bildschirmsperre aktiviert wird.



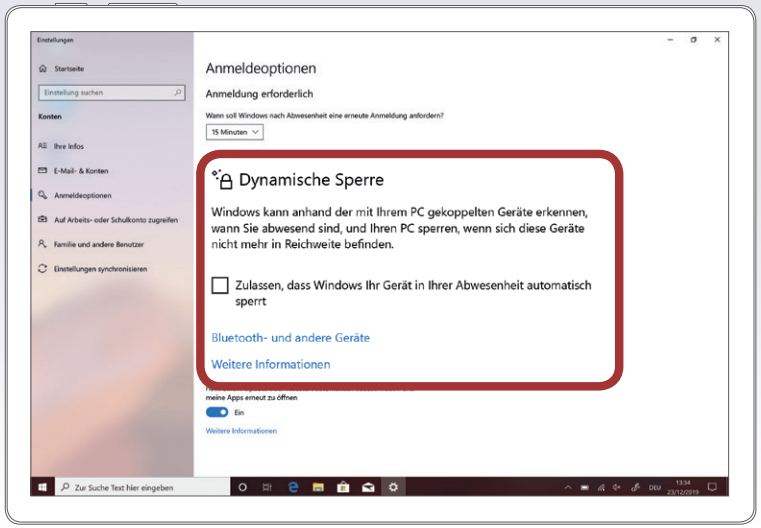




Dynamische Sperre

Start ▸ Konto ▸ Kontoeinstellungen ändern ▸ Anmeldeoptionen ▸ Dynamische Sperre

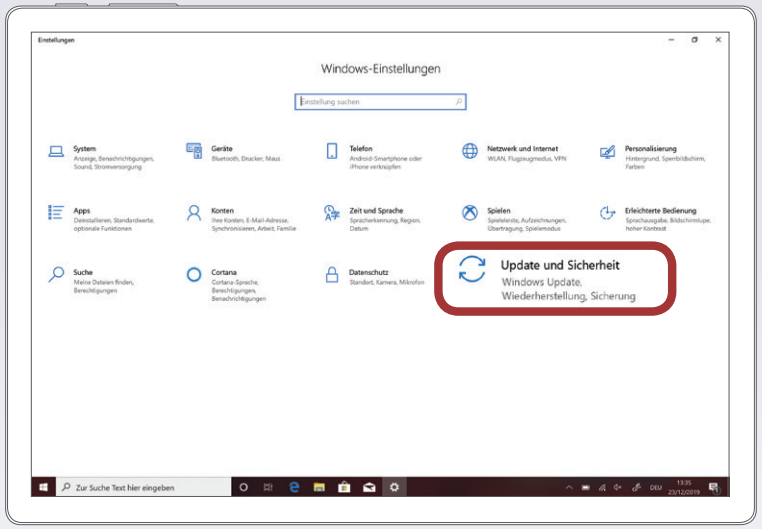
Um diese Funktion zu nutzen, muss ein vertrauenswürdiges Gerät, z. B. das eigene Smartphone mit dem Tablet gekoppelt werden. Entfernt man sich dann mit dem gekoppelten Gerät vom Tablet, wird das Tablet automatisch gesperrt kurz, nachdem das gekoppelte Gerät außerhalb der Bluetooth-Reichweite ist. Dies verhindert, dass Personen das Tablet verwenden können, wenn Sie sich davon entfernen und vergessen, es zu sperren – vorausgesetzt man hat das gekoppelte Gerät mitgenommen.

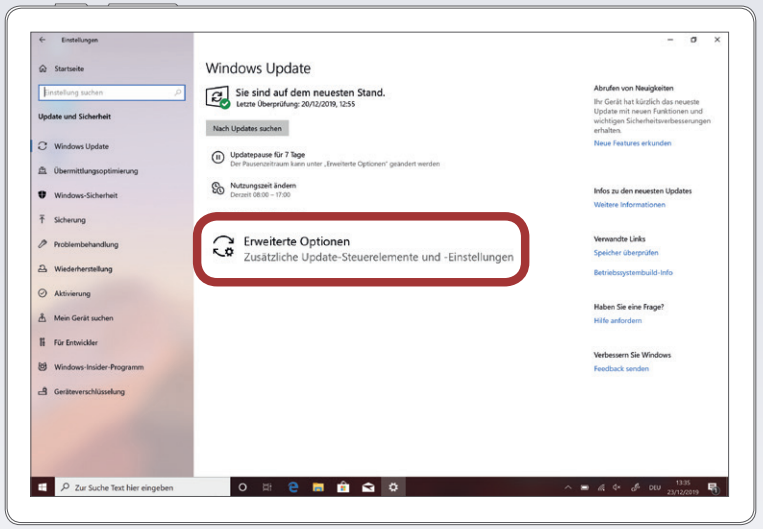


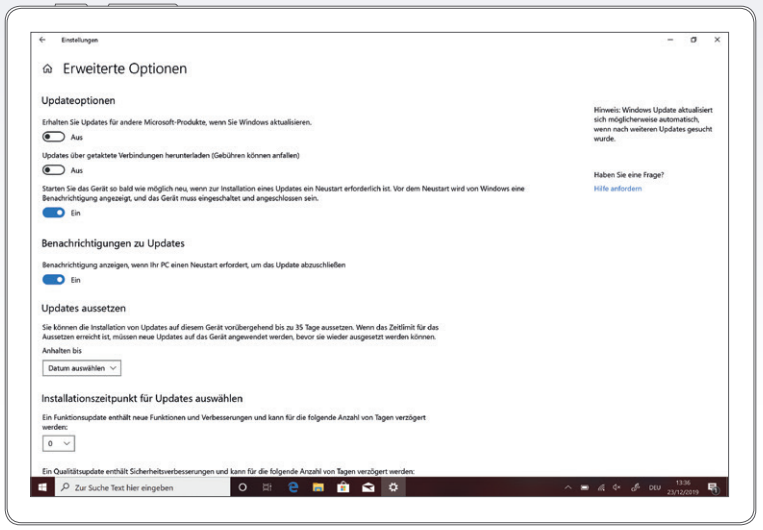
Software-Updates

Die vom Hersteller empfohlenen System-Updates sollten unbedingt durchgeführt werden, denn Updates enthalten kleine Systemverbesserungen: Sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-) Problem bei einem ihrer Produkte erlangen, großes Interesse, umgehend zu reagieren und schnell eine Lösung des Problems zu erarbeiten. Sicherheitslücken sind sehr gut dokumentiert und können von unbefugten Personen für eigene Angriffe schnell ausgenützt werden. Die meisten Tablets haben eine Funktion, die automatisch auf System-Aktualisierungen überprüft. Sollte keine automatische Aktualisierung gewünscht sein, kann die Aktualisierung für bis zu 35 Tage pausiert werden.

Start ▸ Einstellungen ▸ Windows Update ▸ Erweiterte Optionen







TIPP

Tipp: Achten Sie schon beim Kauf auf etwaige Update-Garantien des Anbieters

Synchronisierung & regelmäßige Sicherungskopien (Backups)

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

Hierfür können beispielsweise die Daten per USB-Kabel auf den PC übertragen werden. Ebenso gibt es die Möglichkeit Daten, die mit einem oder mehreren Microsoft-Konten verknüpft sind, über einen Cloud-Dienst, wie z. B. OneDrive von Microsoft zu sichern. Das birgt gewisse Sicherheitsrisiken – beispielsweise sollten hierbei Datenschutz und -sicherheit bedacht werden.

2 Faktor Authentifizierung

Um die Daten möglichst sicher abzuspeichern, ist es sinnvoll für Konten wie das Microsoft-Konto eine 2 Faktor Authentifizierung zu verwenden, auch Bestätigung in zwei Schritten genannt. Sie ist eine weitere Sicherheitsmaßnahme, die missbräuchlichen Zugriff auf das Konto verhindert. Nach erfolgter Einrichtung sind zwei Schritte nötig, um sich beim Konto anzumelden.

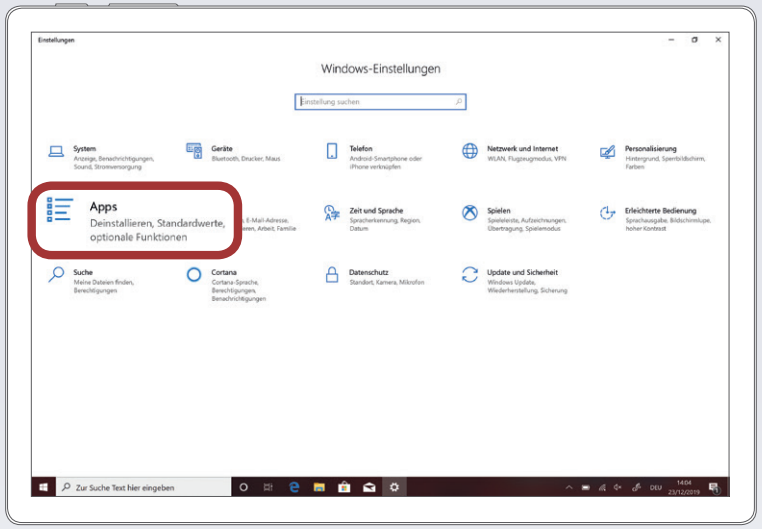
Für ein erfolgreiches Login braucht man ...
1. ... etwas, das man weiß ▸ Passwort
2. ... etwas, das man hat ▸ Smartphone bzw. PIN, Token, Fingerprint etc.

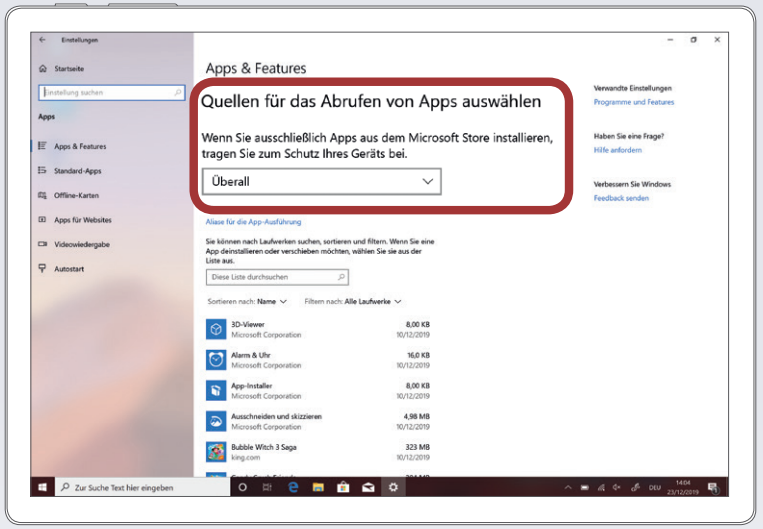
Durch die zusätzliche Sicherheitsebene wird das jeweilige Konto, auf welchem einerseits Kontaktdaten, Emails, Fotos und viele weitere persönliche Daten gespeichert sind, besser abgesichert.

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.

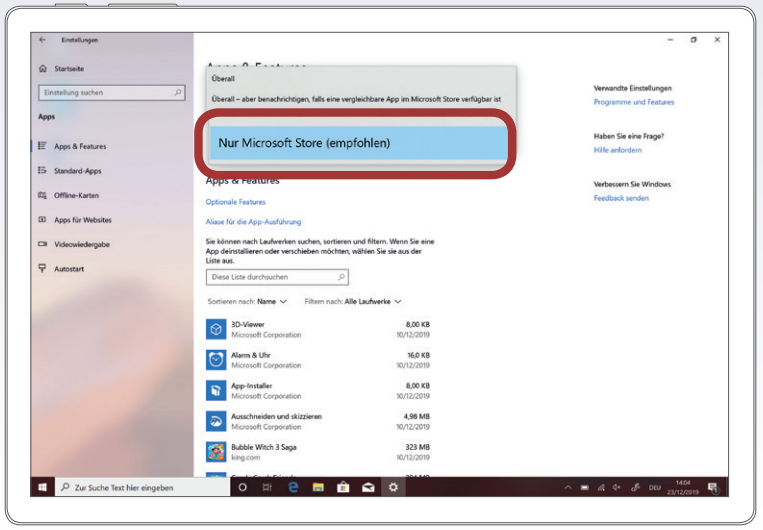




Quellen auswählen

Start ▸ Einstellungen ▸ Apps ▸ Quellen ▸ Nur Microsoft Store

In den Einstellungen kann ausgewählt werden, dass nur Apps aus dem offiziellen Microsoft Store heruntergeladen werden können.



Kein Rückgaberecht für Apps im Microsoft Store

Bevor man im Microsoft Store Apps, Filme oder Musik herunterlädt, sollte man sich sicher sein, dass es sich um das gewünschte Produkt handelt, denn bei Microsoft ist die Rückgabe von Apps, Filmen und Musik nicht möglich. Einige wenige Hersteller bieten zwar kostenlose Testversionen zum Download an, diese sind aber auf eine bestimmte Zeit und/oder Funktionen begrenzt. Immerhin kann man so das Produkt ausprobieren.

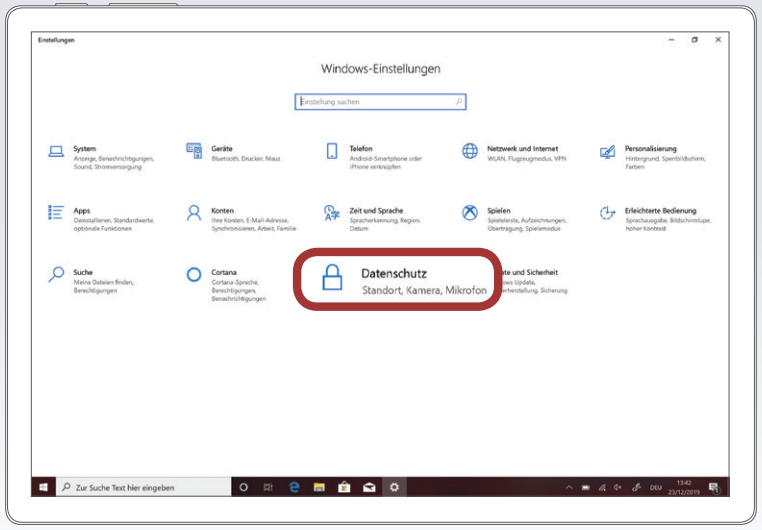
Nicht bedenkenlos allen App-Zugriffsberechtigungen zustimmen

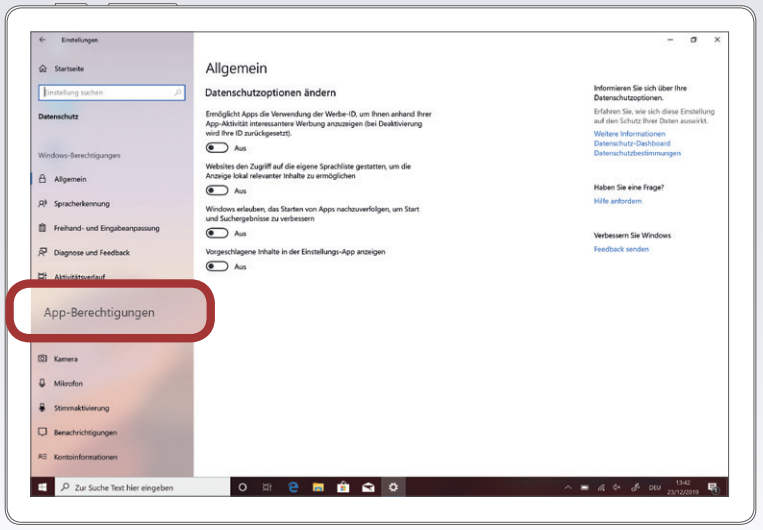
Oftmals ist es aber gar nicht unbedingt eine Sicherheitslücke im engeren Sinne, die von ›bösartigen‹ Apps ausgenutzt wird, um an Daten zu kommen. Vielmehr macht man sich die Unachtsamkeit der Userinnen und User zu Nutze und fordert vom Betriebssystem Berechtigungen an, etwa für den Zugriff auf das Adressbuch, 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

Start ▸ Einstellungen ▸ Datenschutz ▸ App-Berechtigungen

Der Menüpunkt Datenschutz in den Windows-Einstellungen ermöglicht es genau festzulegen, welche Apps auf verschiedene Dienste wie z. B auf den eigenen Standort (Position), Sensoren wie Kamera oder Mikrofon, die Kontoinformationen, die Stimmaktivierung zugreifen können. Es empfiehlt sich, diese Berechtigungen möglichst restriktiv zu setzen.



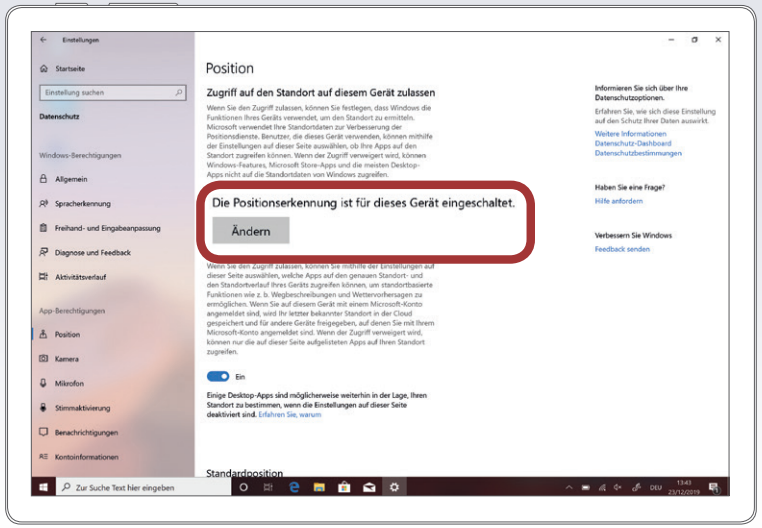


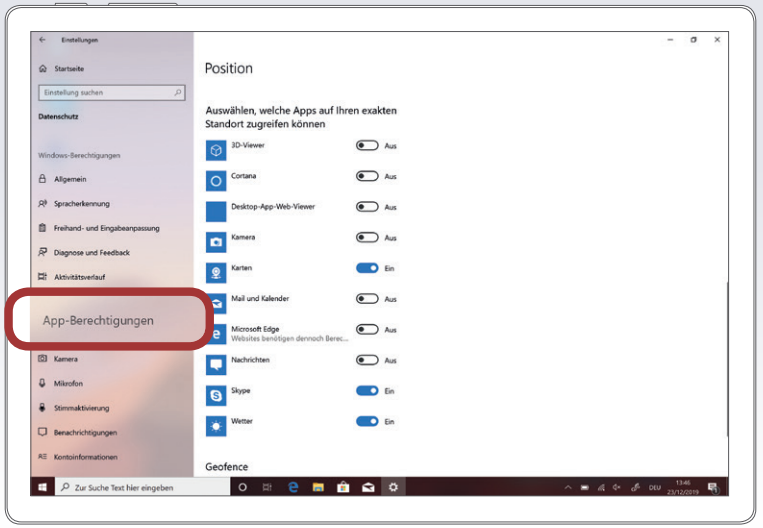
Datenschutzeinstellungen

Beispiel: Zugriff auf den eigenen Standort einschränken

Einstellungen ▸ Einstellungen ▸ Datenschutz ▸ App-Berechtigungen ▸ Position ▸ einzelne Apps auswählen und ändern

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.

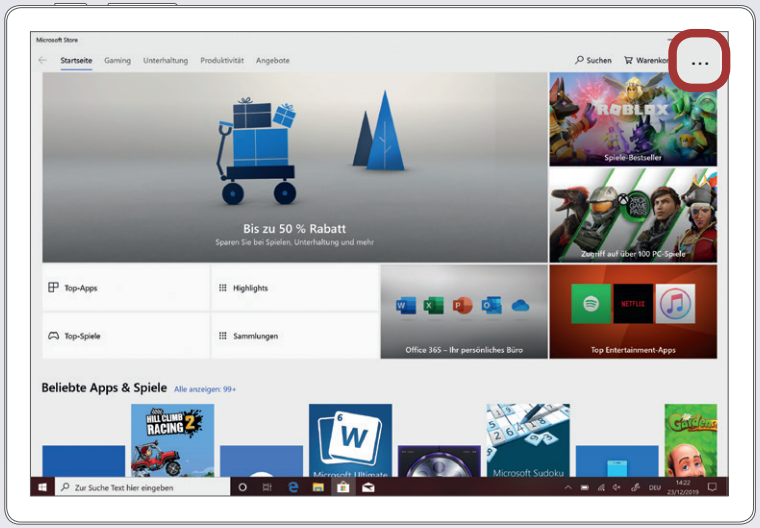


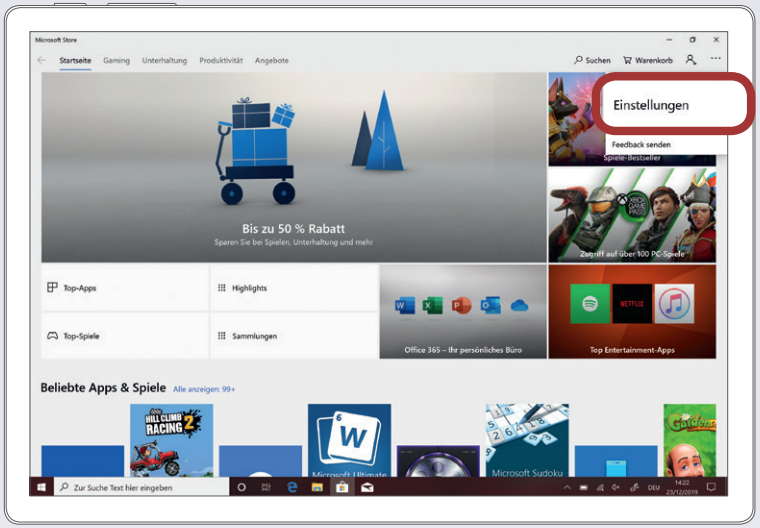


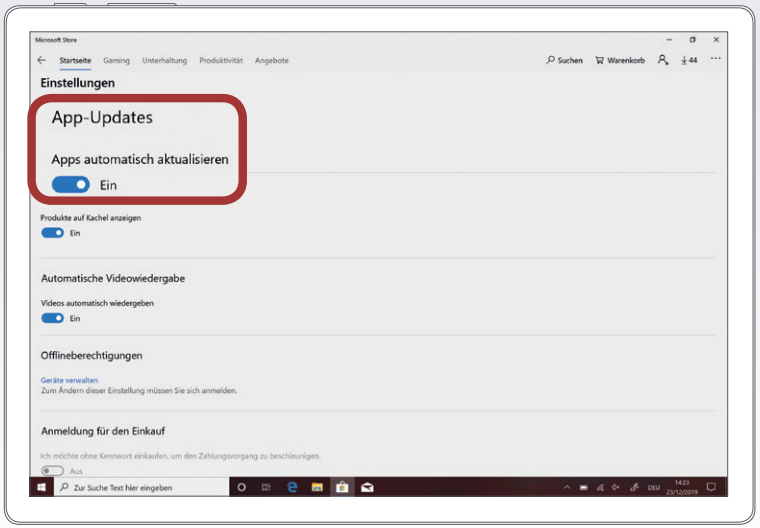
Keine automatischen App-Aktualisierungen & nur WLAN für Aktualisierungen

Microsoft Store ▸ Mehr ▸ Einstellungen ▸ App-Updates ▸ Aus

Werden App- Updates angeboten, kann es durchaus sein, dass weitere oder neue Nutzungsrechte von der App verlangt werden. Es empfiehlt sich daher auch bei Updates auf neue Zugriffsrechte zu achten und diese wiederum nach deren Sinnhaftigkeit oder Notwendigkeit zu hinterfragen.
Möchten Nutzerinnen und Nutzer nicht manuell nach neuen App-Updates suchen müssen, kann die ›Benachrichtigungsfunktion‹ aktiviert werden. Diese informiert, wenn ein neues Update bereitsteht. Entscheiden sich Nutzerinnen und Nutzer für die automatische Aktualisierung, sollte die Funktion ›nur über WLAN‹ aktiviert werden; ansonsten können solche Hintergrundaktualisierungen das eigene Datenvolumen strapazieren und im schlimmsten Fall Zusatzkosten verursachen.





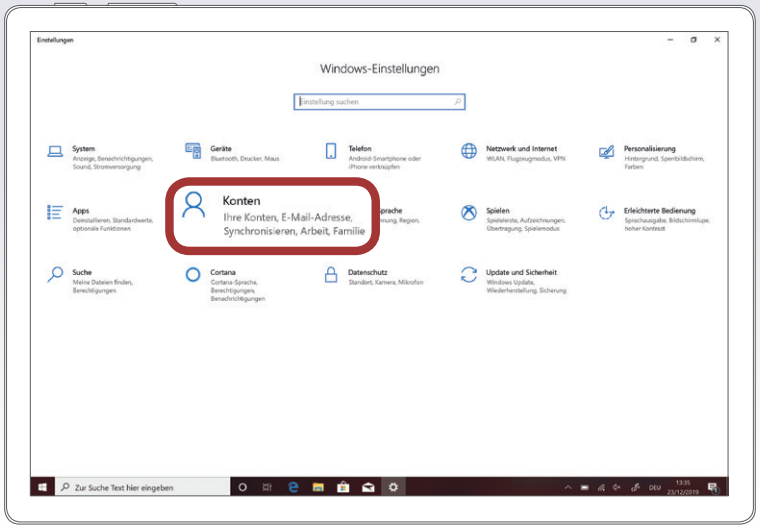


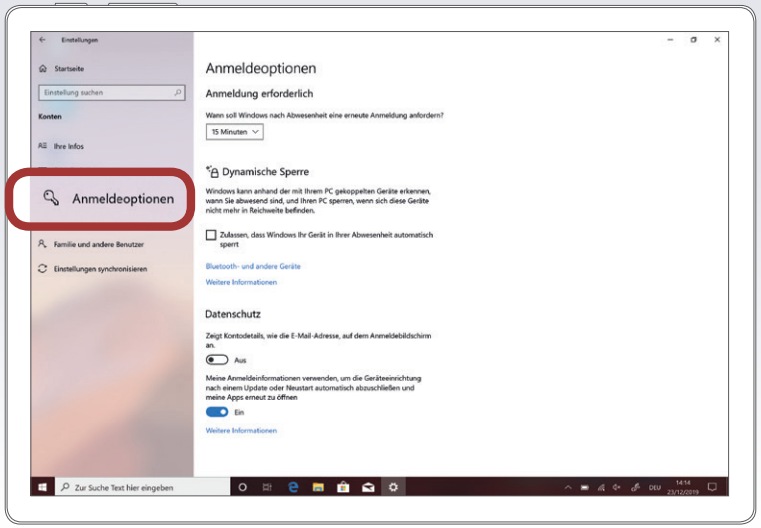
Datenschutzeinstellungen

Kontodetails auf dem Anmeldebildschirm verbergen

Start ▸ Einstellungen ▸ Konten ▸ Anmeldeoptionen ▸ Datenschutz

Bei der Anmeldung am Gerät zeigt Windows die E-Mail-Adresse an, dies kann deaktiviert werden.

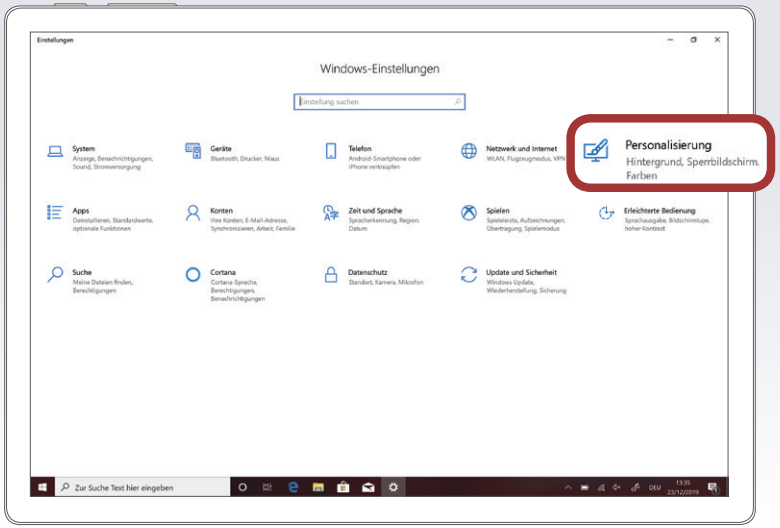


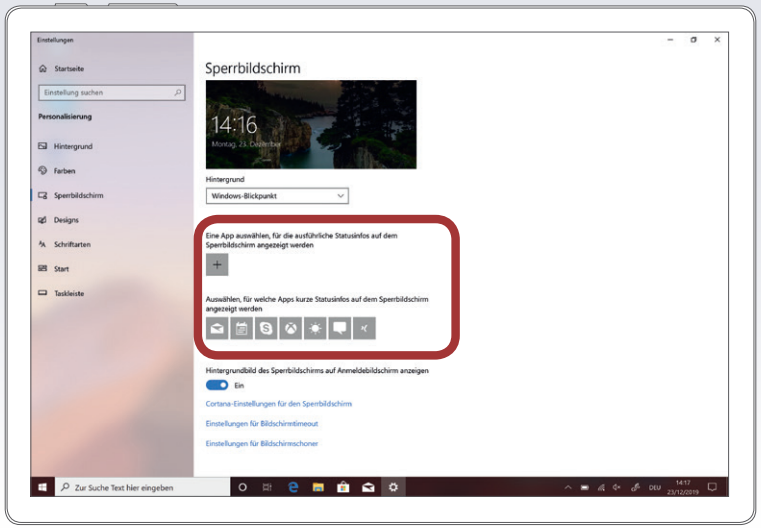


App-Inhalte am Sperrbildschirm anzeigen

Einstellungen ▸ Personalisierung ▸ Sperrbildschirm ▸ Apps auswählen

Sie können selbst definieren, welche Inhalte von welchen Apps am Sperrbildschirm angezeigt werden sollen und welche nicht.

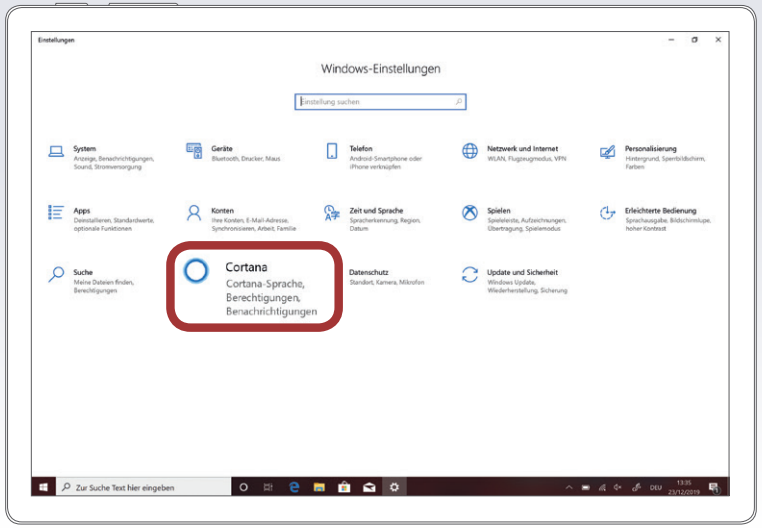


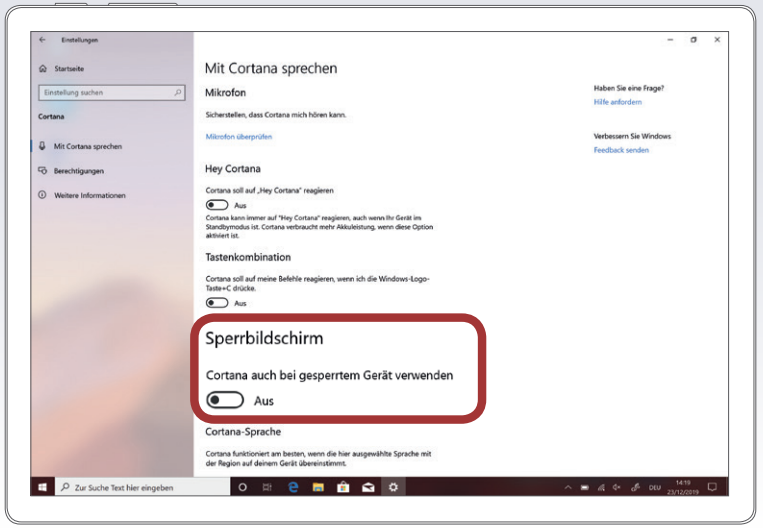


Cortana am Sperrbildschirm ausblenden

Start ▸ Einstellungen ▸ Cortana ▸ Mit Cortana sprechen ▸ Sperrbildschirm ▸ Aus

Auch das sprachgesteuerte Assistenzsystem Cortana können Sie am Sperrbildschirm ein- oder ausblenden.





Wenn das Tablet intensiv genutzt wird, viele Apps heruntergeladen oder auch Online-Banking verwendet werden, sollten Nutzerinnen und Nutzer die Aktivierung einer Sicherheits-App andenken.

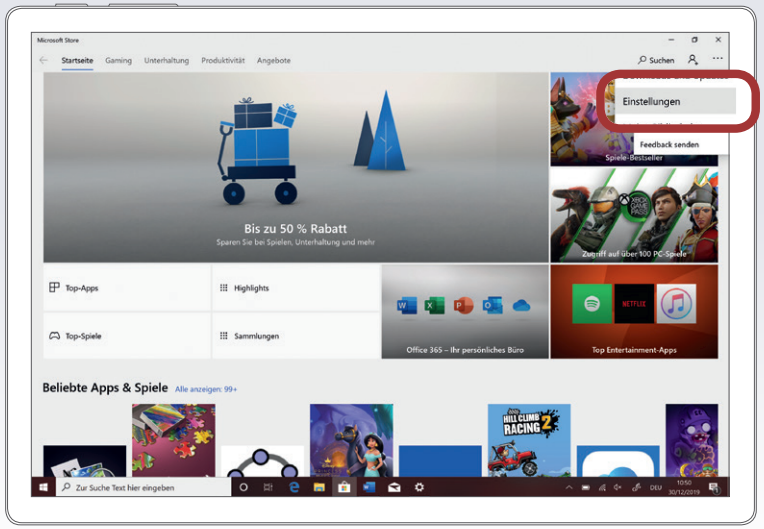
Virenschutzprogramme durchsuchen das Tablet nach Infektionen aller Art (Viren, Würmer und Trojaner) und blockieren und beseitigen diese wenn möglich. Bei Windows ist der Windows Defender Antivirus bereits vorinstalliert. Wer darüber hinaus einen Virenscanner kaufen möchte, sollte das Produkt auf die persönlichen Bedürfnisse abgestimmt auswählen.

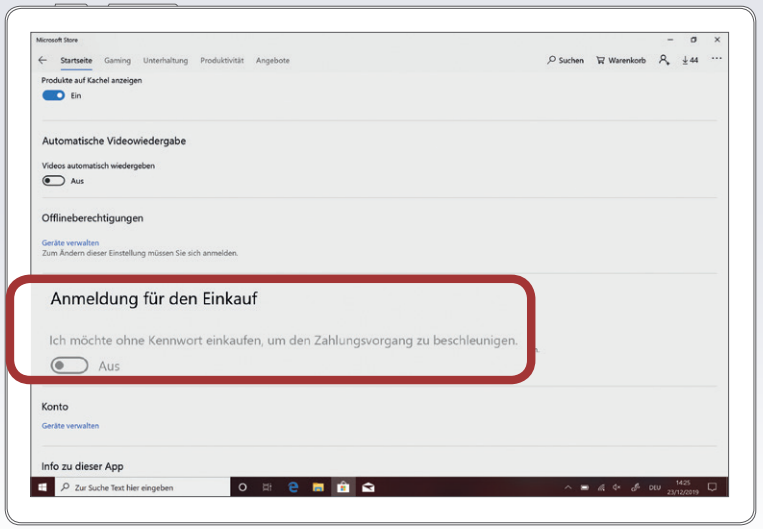
Kostenfalle In-App-Käufe

Bei manchen Apps (z. B. Spielen) besteht die Möglichkeit, in den Anwendungen Guthaben oder Punkte zu kaufen, ohne den klassischen Bestellvorgang zu durchlaufen (›In-App-Käufe‹) wodurch die Gefahr unbeabsichtigt Geld auszugeben, steigt. In-App-Käufe können zu einer 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.

Microsoft Store ▸ Mehr ▸ Einstellungen ▸ Anmeldung für den Einkauf ▸ Ich möchte ohne Kennwort einkaufen um den Zahlungsvorgang zu beschleunigen.

Um diese versehentlichen Käufe zu verhindern, gibt es im Microsoft Store die Möglichkeit, Käufe nur nach vorheriger Passwort-Eingabe zu ermöglichen. Dazu muss die Standardeinstellung geändert werden.





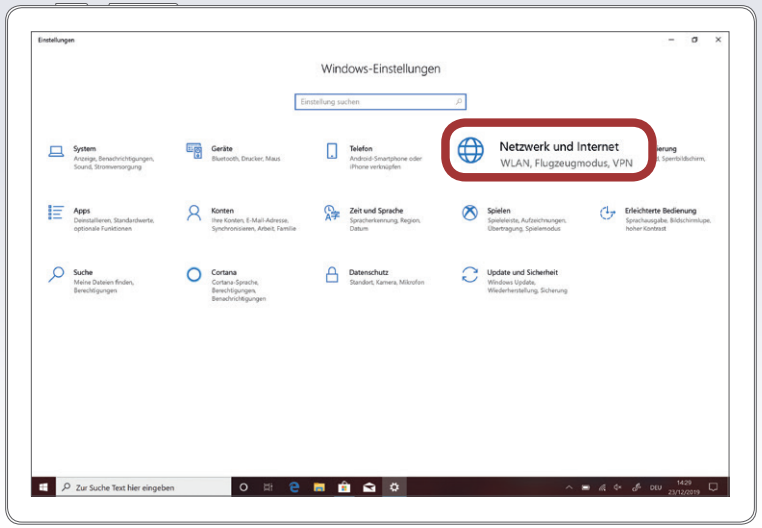
Kostenfalle Datentarife

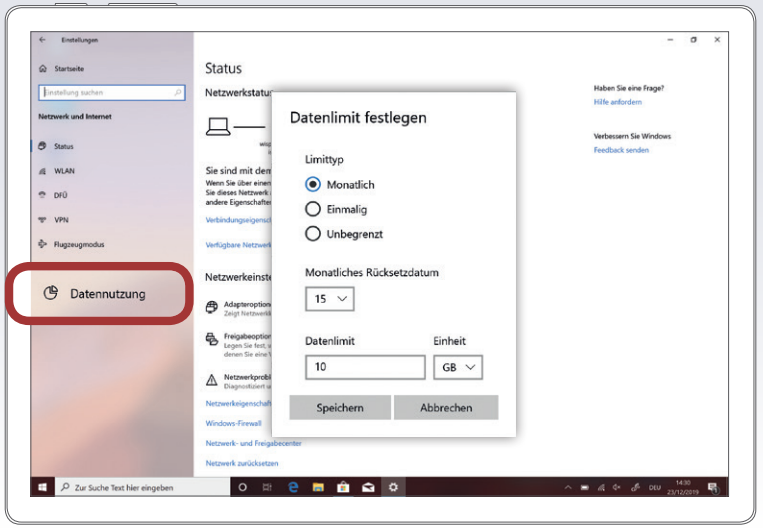
Viele Nutzerinnen und Nutzer von Smartphones und Tablets haben Verträge mit einem limitierten Internet- Paket, pro Monat können sie somit nur ein bestimmtes Datenvolumen verbrauchen. In vielen Fällen wird nach dem Überschreiten dieses Limits die Internetverbindung gedrosselt, in einigen wird jedes weitere Megabyte extra abgerechnet – und das kann teuer werden. Es empfiehlt sich daher, den eigenen Verbrauch im Auge zu behalten.

Viele Tablets haben integrierte Funktionen, um den Datenverbrauch zu messen und auch Limits einzustellen. Alternativ kann eine App zur Kontrolle des Datenvolumens heruntergeladen werden; die meisten Mobilfunkanbieter bieten solche Apps zur Volumen- und Kostenkontrolle an. Jedoch sollte bei allen Lösungen beachtet werden, dass diese Programme keine endgültige Genauigkeit haben. Ist das Datenlimit beinahe erreicht, sollten Nutzerinnen und Nutzer im Zweifelsfall lieber auf weiteren Datenverbrauch verzichten, um so Extrakosten zu vermeiden. Zur Reduktion des Datenverbrauchs empfiehlt es sich auch, Hintergrundsynchronisationen auszuschalten.

Datenlimit festlegen

Einstellungen ▸ Netzwerk und Internet ▸ Datennutzung ▸ Netzwerk auswählen ▸ Limit festlegen

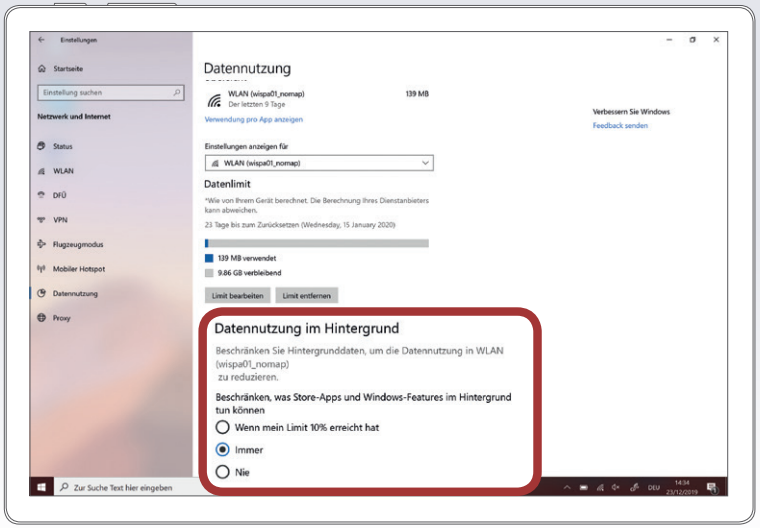




Kostenfalle Datentarife

Datennutzung im Hintergrund beschränken

Einstellungen ▸ Netzwerk und Internet ▸ Datennutzung ▸ Netzwerk auswählen ▸ Datennutzung im Hintergrund ▸ Immer



Roaming

Um zusätzliche Kosten im Ausland zu vermeiden, kann das Roaming deaktiviert werden.

Im Juni 2017 wurden Roaminggebühren innerhalb der EU mit Ausnahmen abgeschafft. Das bedeutet, dass Mobilfunkbetreiber innerhalb Europas keine zusätzlichen Gebühren für Anrufe, SMS und Datenvolumen innerhalb der EU sowie in Norwegen, Liechtenstein und Island verrechnen dürfen. Konkret bedeutet das, dass Anrufe, die aus dem EU-Ausland getätigt werden, nicht mehr kosten dürfen als jene, die im Inland erfolgen. Freieinheiten (Freiminuten und -SMS), die durch das Bezahlen einer Grundgebühr zur Verfügung stehen, können auch im EU-Ausland genutzt werden. Das gilt ebenso für Datenpakete, hier kann der Betreiber aber eine eingeschränkte Nutzung vorgeben. Von inkludierten fünf GB dürften dann z. B. nur zwei GB auch im EU-Ausland genutzt werden. Außerhalb der EU kann es aber zu erhöhten Kosten kommen: Preise für Datendienste sind zum Teil extrem hoch: EUR 15,– bis EUR 20,– pro MB. Laut Roaming-VO muss eine Schutzgrenze bei EUR 60,– (auch in Drittstaaten) eingerichtet sein. Dieser Grenzwert kann jedoch geändert werden.

ACHTUNG

Der Schutz durch die Roaming-VO gilt nicht auf Schiffen oder in Flugzeugen, die zum Teil eigene Mobilfunknetze (technisch gesehen via Satellit realisiert) anbieten.

Am besten schaltet man vor Aufenthalten außerhalb der EU zumindest die Roamingdienste und die Mobilbox für das Hinterlassen von Nachrichten direkt beim Netzbetreiber via App oder Telefonhotline aus. Roamingdienste können zwar auch am Endgerät selbst deaktiviert werden, direkt beim Betreiber ist aber die sicherere Variante. Beachten Sie, dass nicht bei allen Tarifen Roaming möglich ist.

WLAN, Bluetooth und mobile Hotspots

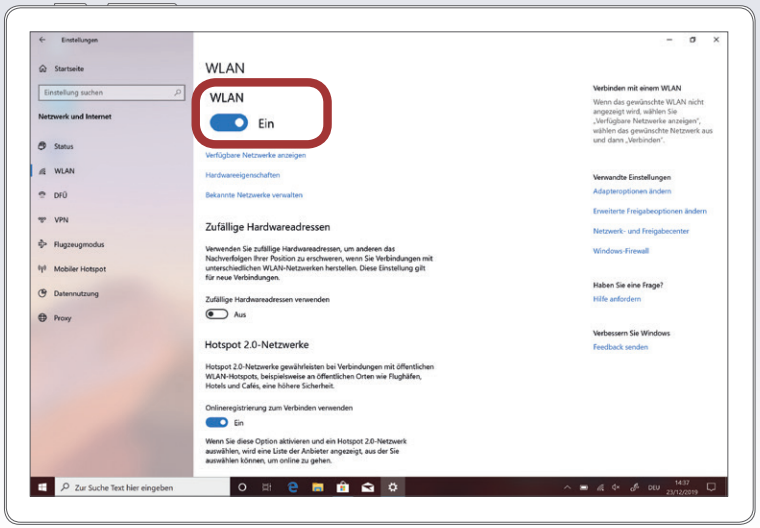
›Home is where your wifi connects automatically‹: Wenn sich das Tablet selbstständig mit verfügbaren WLANs verbindet, ist das zwar praktisch und bequem, kann aber unter Umständen ein Sicherheitsrisiko darstellen. Drahtlose Schnittstellen sollten nur für die unmittelbare Verwendung aktiviert werden.

WLAN, Bluetooth und sonstige drahtlose Schnittstellen stellen potentielle Angriffspunkte dar. Die WLAN- und Bluetooth-Funktion sollte deshalb nur dann eingeschaltet 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

Einstellungen ▸ Netzwerk und Internet ▸ WLAN ▸ Aus

In den Einstellungen auf Netzwerk & Internet tippen. Unter WLAN werden die verfügbaren Netzwerke angezeigt und die WLAN-Funktion kann abgeschaltet werden. Zudem sollte konfiguriert werden, dass sich das Tablet nicht automatisch mit offenen WLAN-Netzen verbindet. Diese sind oft nur mangelhaft gesichert und ermöglichen bei einem Angriff das Mitlesen des gesamten Netzwerkverkehrs.

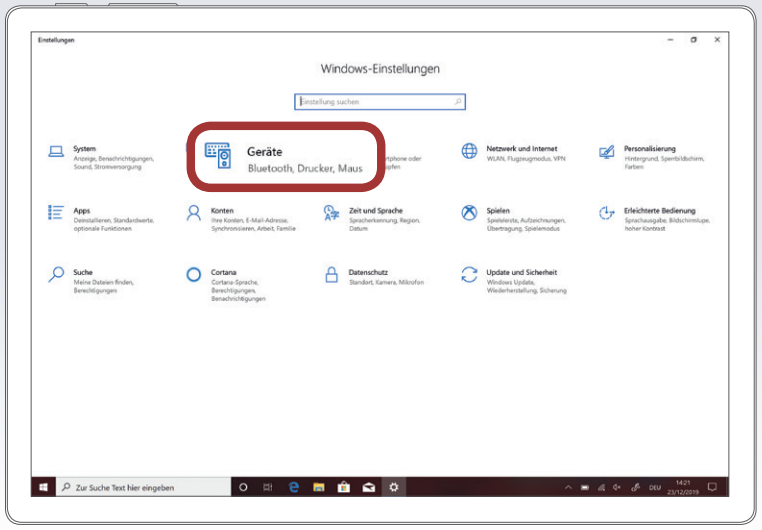


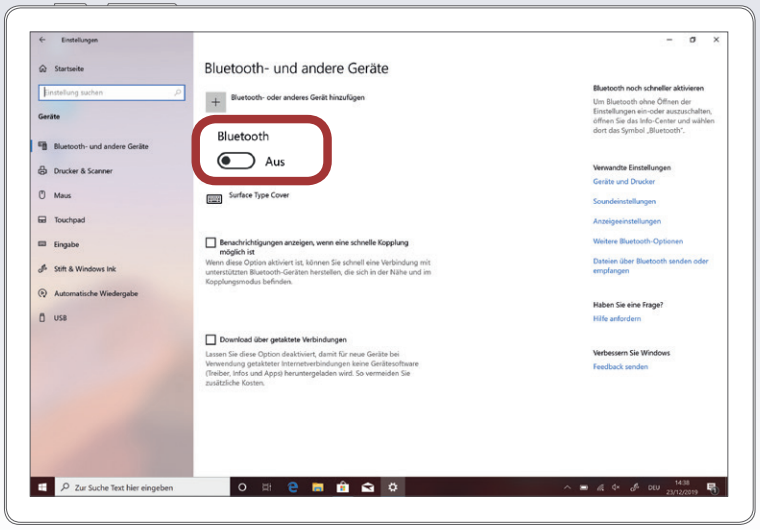
TIPP

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.

Bluetooth deaktivieren

Einstellungen ▸ Geräte ▸ Bluetooth ▸ Aus





Verkaufen, Verschenken & Verborgen

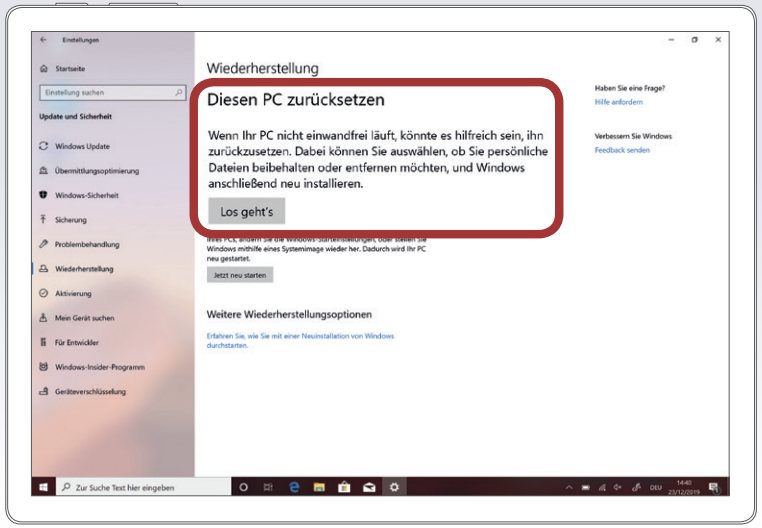
E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem Tablet sind sehr viele persönliche Daten gesammelt. Soll das Gerät weitergegeben oder verkauft werden, sollte es unbedingt auf den Werkszustand zurückgesetzt und alle Daten sollten gelöscht werden.

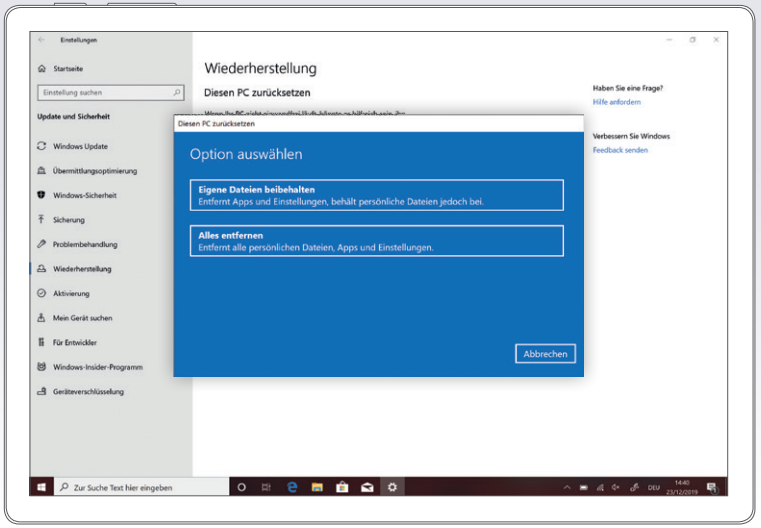
E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem Tablet sind sehr viele persönliche Daten gesammelt. Soll das Gerät weitergegeben oder verkauft werden, sollte es unbedingt auf den Werkszustand zurückgesetzt und alle Daten sollten gelöscht werden. Um die Weitergabe persönlicher Daten zu verhindern, 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). Daten, die noch benötigt werden, sollten vor der Zurücksetzung auf den Werkszustand auf einem anderen Datenträger gesichert werden.

Auf Werkszustand zurücksetzen

Einstellungen ▸ **Update und Sicherheit** ▸ **Wiederherstellung** ▸ **Diesen PC zurücksetzen**

Mit dieser Funktion werden alle persönlichen Inhalte (Apps, Bilder, Musik, Videos, Konten, etc.) vom Gerät entfernt und das Tablet wird auf Werkseinstellungen zurückgesetzt.





›Mein Gerät suchen‹: Das iPad finden, sperren und löschen

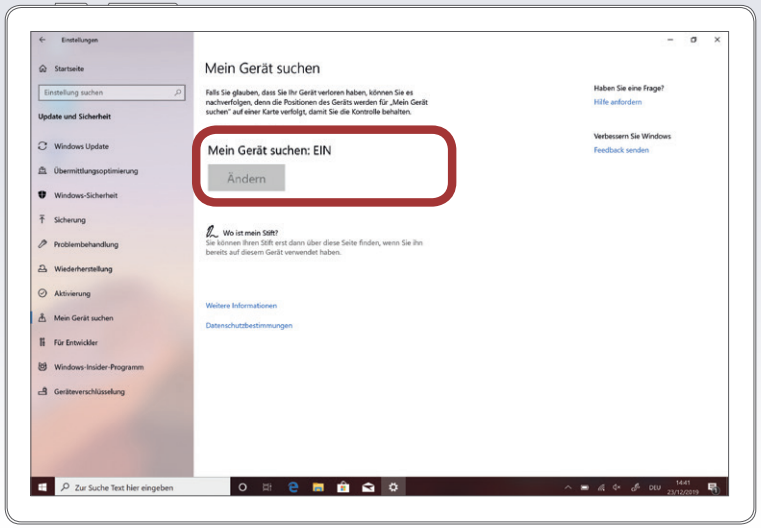
Die meisten Tablets bieten die Möglichkeit, es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen. Windows unterstützt dies im Rahmen der Funktion ›Mein Gerät suchen‹. Ist diese Funktion aktiviert, kann das Tablet über das Microsoft-Konto geortet, 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).
Bei Diebstahl und Verlust sollte auch sofort der Netzbetreiber informiert werden, damit die SIM-Karte gesperrt wird. In den meisten Fällen haften die Nutzerinnen und Nutzer bis zur Mitteilung an den Netzbetreiber für anfallende Kosten. Ebenso schnell wie möglich sollte eine Diebstahlsanzeige erstattet werden.

Zur Vorbereitung der Verlust- oder Diebstahlsanzeige: IMEI – International Mobile Equipment Identity, zu den Vertragsunterlagen zu Hause oder den Reiseunterlagen geben. IMEI ist eine 15-stellige Nummer, mittels derer ein GSM/UMTS/LTE Endgerät wie ein Tablet weltweit identifiziert werden kann. IMEI steht auf der Verpackung des Geräts oder kann (vorbereitend) auch über die Surface App, die Einstellungen des Geräts oder am Gerät selbst gefunden werden: https://support.microsoft.com/de-at/help/4036293/surface-find-the-serial-number-on-surface

Aktivierung von Mein Gerät suchen

Einstellungen ▸ Update und Sicherheit ▸ Mein Gerät suchen



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.

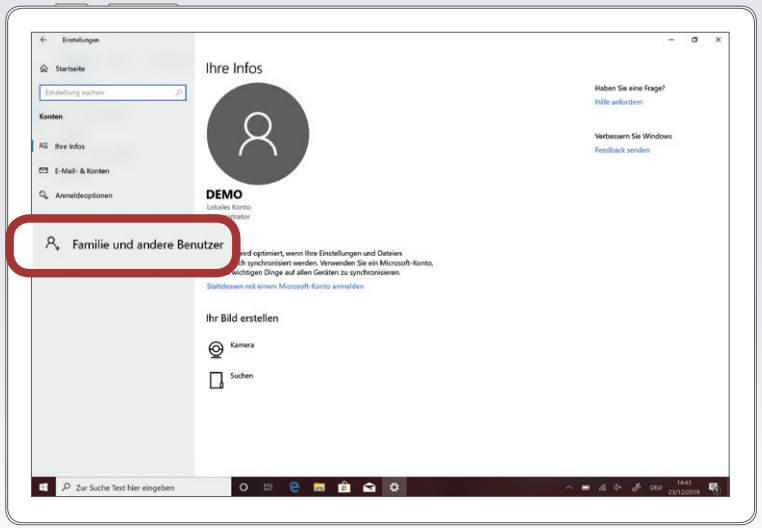
Erziehungsberechtigte sollten allerdings bedenken, dass Medienerziehung nicht an Software delegiert werden kann. Eine allzu penible Überwachung sämtlicher Aktivitäten ist zudem pädagogisch wenig sinnvoll: Sie verleitet zum Einschreiten, wo Kinder eigentlich gut allein zurechtkommen und steht einer vertrauensvollen, 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.

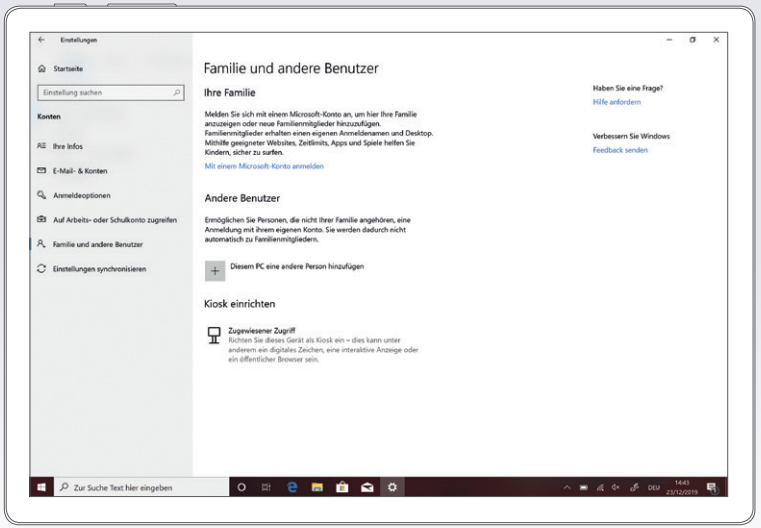
Ein Kinderkonto anlegen

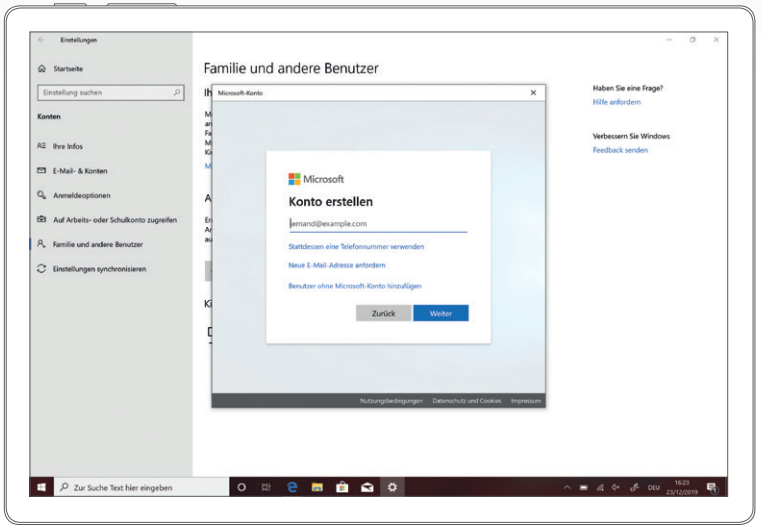
Einstellungen ▸ Konten ▸
Familie und weitere Benutzer ▸
Familienmitglied hinzufügen ▸ Kind hinzufügen ▸
Eingabe der E-Mail-Adresse des Kindes

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-Gerät, auf dem es sich anmeldet.

Ist der E-Mail-Adresse des Kindes 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 freigeschaltet und kann zur Anmeldung auf dem Tablet benutzt werden.





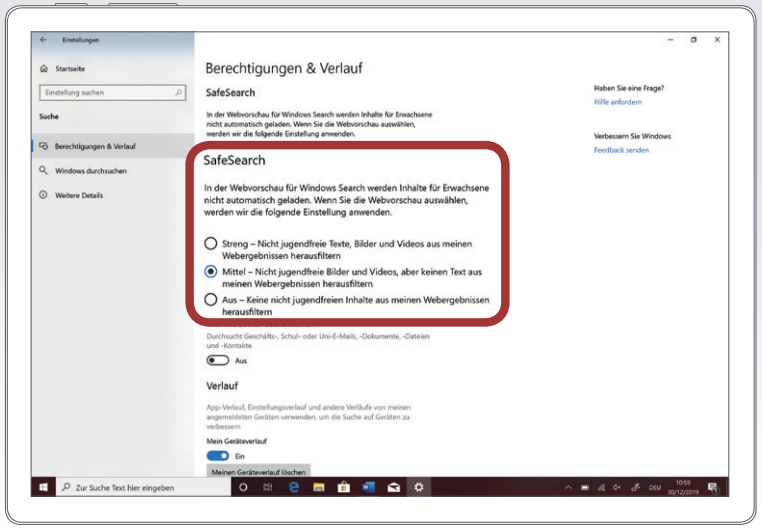


Einrichten von Family Features – das kindersichere Tablet

SafeSearch aktivieren

Einstellungen ▸ Suche ▸ Berechtigungen & Verlauf ▸ SafeSearch ▸ Streng/Mittel/Aus

Die Funktion Safesearch verhindert, dass nicht jugendfreie Inhalte in den Suchergebnissen angezeigt werden. Sie werden blockiert.



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.

Notizen

Notizen

TIPP

In unserer Broschüre »Technischer Kinderschutz im Internet« stellen wir weitere Möglichkeiten vor und geben Informationen, wie Kinder bei ihren ersten Erfahrungen im Internet unterstützt werden können.
Sie kann auf www.ispa.at/technischerschutz kostenlos heruntergeladen werden.

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.

Die Arbeiterkammer Niederösterreich bietet Ihnen Beratung rund um die Themen Smartphone, Internet und Digitalisierung an. Mit dem Handy- und Internettarifrechner der AK (handy.arbeiterkammer.at) finden Sie sich leichter im Tarifdschungel zurecht. Weitere Leistungen und Kontakt zur Konsumentenberatung der Arbeiterkammer Niederösterreich finden Sie unter noe.arbeiterkammer.at/konsument

Währinger Straße 3/18, 1090 Wien
Tel.: +43 (0)1 409 55 76 | office@ispa.at
www.ispa.at | twitter.com/ispa_at
facebook.com/ISPA.InternetserviceProvidersAustria