Schieb Report

Ausgabe 2020.14

Google Translator als Echtzeitübersetzer

Die Welt wird immer internationaler. Kommunikation findet auch im normalen Umfeld schon lange nicht mehr nur in einer Sprache statt, sondern in vielen verschiedenen. Bei Vor-Ort-Terminen mussten Sie früher für viel Geld einen Simultan-Übersetzer einsetzen, der in Echtzeit zwischen den Teilnehmern übersetzen sollte. Das ist durch die Leistungsfähigkeit der Smartphone-Übersetzer deutlich einfacher geworden!

Wenn Sie ein Android-Gerät verwenden, dann können Sie mit dem kostenlosen Google Übersetzer Übersetzungen per Spracheingabe durchführen. Starten Sie die App, dann wählen Sie die Quell- und die Zielsprache aus. Für Übersetzungen zwischen Englisch, Französisch, Deutsch, Hindi, Portugiesisch, Russisch, Spanisch und Thai steht die Übersetzung durch Spracheingabe zur Verfügung.

Tippen Sie auf **Spracheingabe**, dann können Sie Text in der Quellsprache sprechen und die App übersetzt diesen automatisch in die Zielsprache. Oft ist es aber so, dass Sie ein echte Unterhaltung führen wollen. Da ist es unangenehm, einen Text zu sprechen und dem Gegenüber das Smartphone zum Lesen der Übersetzung hinhalten zu müssen. Viel effektiver geht das, wenn Sie auf **Unterhaltung** tippen. Aktivieren Sie dann unten am Bildschirm

Automatische Spracheingabe. Die App erkennt nun automatisch, in welcher der beiden Sprachen der Text gerade gesprochen wurde, und übersetzt ihn in die jeweils andere Sprache. Die Übersetzung wird dann direkt über die Lautsprecher wiedergegeben.

Verändern der Auflösung des Samsung S20/S20+/S20 Ultra

Der Bildschirm ist eines der wichtigsten Hardware-Elemente eines Smartphones. Darum sind auch die Entwicklungen der Hardware in diesem Bereich besonders schnell und weitreichend. Während lange Zeit die Größe im Mittelpunkt des Interesses standen, ist heute auch die Auflösung, die eine große Rolle spielt. Diese ist nicht immer festgeschrieben: Bei der Samsung S20-Reihe lässt sich diese verändern.

Je höher die Auflösung ist, desto mehr Details können Sie auf dem Bildschirm erkennen. Das hängt natürlich von diversen Faktoren ab: Zum einen von der Auflösung des Quellmaterials: Bei einem Word-Dokument, das in lesbarer Größe dargestellt wird, wirkt sich das kaum auf. Bei einer Webseite, die in der Desktop-Version im Vollbild dargestellt wird, schon eher. Zum anderen ist das menschliche Auge auch nicht unendlich leistungsfähig. Ab einer gewissen Auflösung erkennt es keinen Unterschied mehr.

Hinzu kommt, dass höhere Auflösung auch höheren Stromverbrauch bedeutet, und Sie damit eine Abwägung zwischen Auflösung und Laufzeit des Gerätes vornehmen müssen.

Die Einstellungen für die Auflösung finden Sie unter **Einstellungen** > **Anzeige** > **Bildschirmauflösung**.

Wenn Sie die neue Auflösung anwählen und dann speichern, dann kann es sein, dass die eine oder andere Anwendung, die ihre Inhalte abhängig von der Auflösung des Bildschirms darstellt, geschlossen wird und neu gestartet werden muss.

Hochzeit für Hacker: Hochzeit für Passwortschutz?

In Krisenzeiten wie derzeit gehen Betrüger nicht in Urlaub. Ganz im Gegenteil: Sie nutzen eine aktuelle Krisenlage gerne aus. Etwa, indem sie ungeniert die hohe Aufmerksamkeit für ein Thema für sich ausschlachten.

Experten warnen, dass derzeit viele Betrüger versuchen, mit dem Thema „Corona“ die Leute zu überrumpeln, ihre Zugangsdaten preiszugeben. Sie verschicken Mails mit angeblichen Infos über „Corona“ und fordern so ganz nebenbei zur Eingabe von Logindaten auf. Darauf fallen leider gerade viele herein. Muss das sein und wie kann man sich schützen?

Aktuell wird die beliebte Methode des „Phishings“ reaktiviert: Betrüger – ich würde sie nicht „Hacker“ nennen, den die haben richtig Ahnung und geben sich mitunter wenigstens Mühe – also dreiste Betrüger versuchen arglose Internetbenutzer zu täuschen. Sie schicken ihnen Mails und versprechen wertvolle Informationen zum Thema Corona.

Oder sie bauen Webseiten, die ebenfalls versuchen, mit aktuellen Infos zu punkten. An einer bestimmten Stelle werden die Opfer dann aufgefordert, Zugangsdaten einzugeben, etwa zum Facebook-Konto, zum PayPal-Konto... Wer das macht, gibt seine Daten raus – und wird schon wenig später erleben, dass die Konten gekapert werden. Mit PayPal Geld überwiesen wird. Oder dass auf Rechnung der Opfer Waren bestellt werden...

60% nutzen das aktuelle Passwort mehrfach

Einer aktuellen Studie von Web.de zufolge verwenden 60% der Deutschen immer noch ein und dasselbe Passwort in mehreren Diensten. Bedeutet: Fragt eine Phishing-Mail oder eine Phishing-Seite die Zugangsdaten zu einem eher harmlosen Onlinedienst ab – etwa Facebook oder einen Mini-Onlineshop –. Ist die Chance hoch, dass die Betrüger mit demselben Passwort auch bei PayPal, Amazon oder sogar ins Mail-Konto kommen.

Das wäre dann natürlich besonders fatal, weil so praktisch auf alle anderen Konten zugegriffen werden kann – durch Passwort-Rücksetzen-Funktion. Auf solche Fälle sollten wir alle besser vorbereitet sein.

Passwort-Manager können helfen

Also kommt jetzt die Regel zur Sprache, die wir alle kennen: Kompliziertes Passwort und überall ein anderes. Viele sagen: Das kann sich doch keiner merken...

Richtig: Wichtig ist vor allem, in jedem Onlinedienst ein anderes Passwort zu benutzen. Dazu kann ich nur dringend raten. Überall dasselbe Passwort zu verwenden ist wirklich sträflich gefährlich. Ich rate dazu, gute Passwort-Manager wie 123Password, LastPass oder Dashlane zu benutzen.

Die können wirklich eine Menge heute. Die merken sich alle Passwörter und geben sie automatisch ein. Also ich muss sie mir nicht merken und auch nicht eintippe, das macht die Software für mich. Auf dem Tischcomputer und auf dem Smartphone.

Die Programme beschweren sich sogar, wenn in mehreren Konten dasselbe PW zum Einsatz kommt. Es ist sicherer, einen Passwort-Manager zu benutzen, als Passwörter manuell einzugeben und in mehreren Diensten dasselbe Passwort zu verwenden.

Zwei Faktor Authentifizierung

Trotzdem: Geklaut ist geklaut. Verrate ich aus Versehen mein Paypal-Passwort, dann können die Betrüger doch auch darauf zugreifen.

Richtig. Aber ich kann hier und jetzt meine Zugangsdaten zu Facebook, Twitter, Microsoft, Amazon, Apple und was auch immer verraten – es kommst trotzdem niemand in meine Konten rein. Denn ich verwende praktisch überall die Zwei-Faktor-Authentifizierung.

Die muss man in jedem Dienst einmal einrichten – das geht mittlerweile fast überall. Dann ist neben Benutzername und Passwort auch noch die Eingabe durch einen durch einen Generator erzeugten Code erforderlich. Eine App erzeugt den Code. Das geht blitzschnell, wenn man sich mal daran gewöhnt hat – und macht die Sache ungleich sicherer. Niemand kann diesen Code klauen. Phishing-Mails haben ihren Schrecken verloren. Ich kann nur jedem empfehlen, seine wichtigen Konten damit abzusichern.

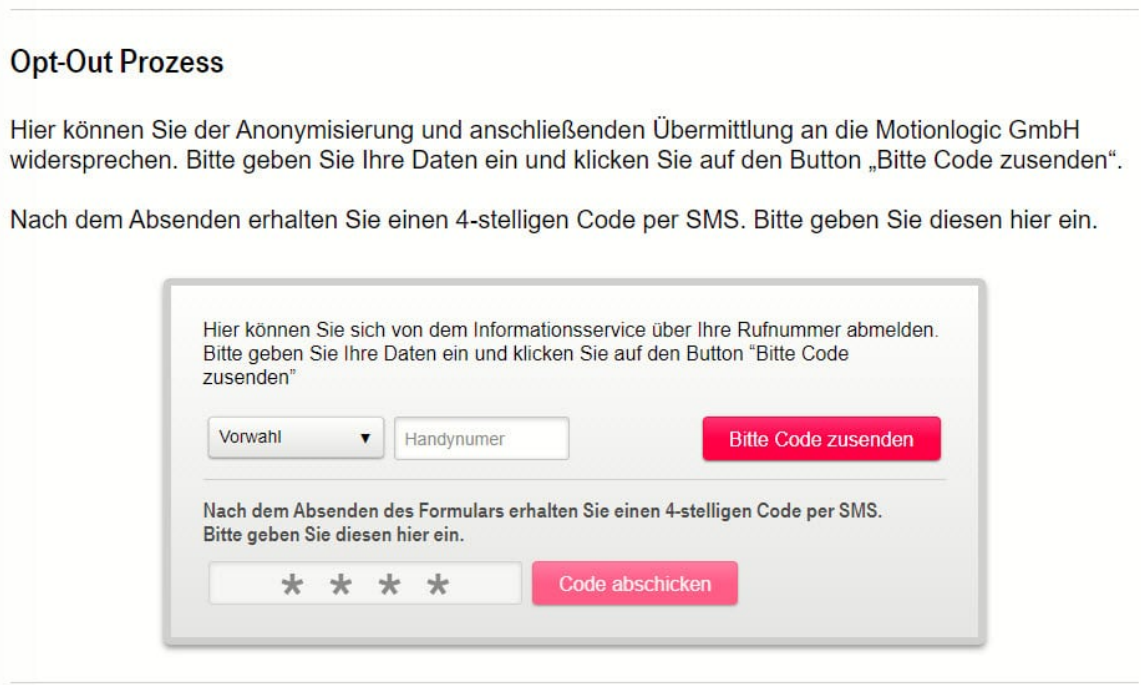
Widerspruch gegen die Telekom-Auswertungen der Mobilfunkbewegungen

Sobald es um die Verarbeitung der eigenen personenbezogenen Daten geht, werden viele Menschen schnell vorsichtig: Die informationelle Selbstbestimmung ist ein hohes Gut und sorgt für ein besseres Gefühl: Sie haben unter Kontrolle, wer was von Ihnen weiß.

Nun sind wir gerade in einer besonderen Situation, und da werden besondere Maßnahmen ergriffen. So beispielsweise die Weitergabe von Mobilfunkdaten von der Telekom an das Robert Koch-Institut. Wir zeigen Ihnen, was Sie dagegen tun können - wenn Sie das wirklich wollen.

Die Idee ist einfach: So gut wie jeder Mensch hat ein Mobiltelefon, vom einfachen Telefonknochen bis hin zum High End-Smartphone. Bewegt er sich, reist er, dann bewegt sich auch das Gerät.

Diese Bewegungen kann der Netzbetreiber auswerten und daraus eine Aussage ableiten, ob die Menschen eher zuhause bleiben oder weiterhin wild durchs Land reisen. Eine solche Auswertung macht Sinn, und sie nutzt nur anonymisierte Daten. Das RKI bekommt keine Informationen, welcher Benutzer, welche natürliche Person sich hinter einem Datenpunkt verbirgt.



Nichts desto Trotz: Wenn Sie nicht an dieser Auswertung teilnehmen möchten, dann können Sie dies auf der offiziellen Opt-Out-Seite einen Antrag dazu stellen.

QNAP-Netzlaufwerke ohne Qfinder verfügbar machen

Wenn Sie ein QNAP-NAS einsetzen, dann verbinden Sie wahrscheinlich die Netzlaufwerke, die darauf sind, mit dem Mac. Damit können Sie dann wie auf eine lokale Festplatte auf die Dateien drauf zugreifen. Die Software, mit der Sie die Verbindung herstellen, ist der kostenlose Qfinder von QNAP selbst. Den aber immer wieder zu starten und die Verbindung manuell herzustellen, ist unnötiger Aufwand. Wir zeigen Ihnen, wie es einfacher geht.

MacOS sieht hier das Anlegen eines Alias vor. Wenn Sie mit der rechten Maustaste auf das gemountete Laufwerk klicken, dann können Sie über **Alias erzeugen** eine Verknüpfung anlegen. Über die können Sie dann die Verbindung wieder herstellen. Der Nachteil: Sie haben dann das Laufwerk und das Alias parallel auf dem Schreibtisch.

Einfacher ist es, wenn Sie beim Mounten des Laufwerkes im Qfinder den Haken bei **Bereitgestellte Ordner zu "Favoriten" im Finder hinzufügen** setzen. Damit wird ein Eintrag im Favoritenbaum des Finder angelegt. Wenn Sie den Mac neu starten, dann ist die Verbindung zum NAS nicht hergestellt. Ein einfacher Klick auf den Favoriten stellt diese dann her. Auf dem Schreibtisch haben Sie dann nur einen Eintrag für das Netzlaufwerk.

Corona-Krise: Amazon ist der Profiteur

Corona zwingt die Wirtschaft derzeit in die Knie. Nicht nur bei uns in Deutschland, sondern weltweit. Unzählige Arbeitnehmer werden in Kurzarbeit geschickt. Viele, viele Läden müssen wochenlang schließen. Restaurants sowieso. Massenhaft Betriebe und Menschen bangen nun um ihre Existenz.

Doch im fernen Seattle sitzt ein Mann, der davon mächtig profitiert: Jeff Bezos, Gründer und Chef von Amazon. Sein Online-Portal explodiert aktuell regelrecht: Die Menschen bestellen wie verrückt bei Amazon. Mehr denn je. Und sorgen so bei Amazon für neue Umsatzrekorde.

Explodierender Aktienkurs

Allein in den USA will Amazon 100.000 Menschen einstellen, um dem explodierenden Bedarf decken zu können. Die Aktie hat innerhalb weniger Tage um 100 Milliarden Dollar an Wert zugenommen.

Klar, denn die Umsätze sprudeln nicht nur jetzt und aktuell, sondern auch in Zukunft. Durch die Corona-Krise gewinnt Amazon Marktanteile, die teilweise bleiben werden. Denn die Menschen gewöhnen sich immer mehr an den Online-Einkauf.

Krise ruiniert andere Unternehmen

Vor allem aber werden es viele Unternehmen im Einzelhandel nicht schaffen. Die Krise ruiniert sie. Sie machen dicht. Auf diese Weise entsteht dann später noch mehr Notwendigkeit, online einzukaufen.

Weil es schlicht zu wenige Fachgeschäfte gibt - noch weniger als ohnehin schon! -, in denen die Menschen alles Notwendige einkaufen könnten. Amazon profitiert also in mehrerlei Hinsicht von der Krise. Jetzt - und in Zukunft.

Der explodierende Aktienkurs zeigt es: Die Börse geht davon aus, dass Amazon enorm wächst. Durch konsequente Verdrängung. Viele Mitbewerber werden verdrängt. Platt gemacht.

Politik hat nicht an Konsequenzen gedacht

Allerdings trifft Amazon diesmal nicht die volle Schuld. Die Politik schließt die Geschäfte - natürlich aus gutem Grund. Aber ohne sich ausreichend Gedanken zu machen, welche Konsequenzen das hat.

Vielleicht wäre es eine gute Idee, die ganz großen Online-Shoppingportale zu besteuern. Um einen Finanzausgleich hinzubekommen. Wo die einen profitieren, lässt sich doch das Leid der anderen zumindest wirtschaftlich etwas ausgleichen.

Gezielt online einkaufen - bei den Kleinen

Eine Lenkung wäre wünschenswert. Ein Lastenausgleich. Fairness. Doch das wird wohl eher nicht passieren. Deshalb sollten **wir** darüber nachdenken, wo wir online einkaufen.

Wann immer möglich, sollten wir das in den Geschäften tun, die aktuell unter der Krise zu leiden haben. Viele Einzelhändler verkaufen derzeit online, um noch größeren Schaden zu vermeiden.

Also: Lieber vor Ort einkaufen - und liefern lassen. Da, wo es möglich ist.

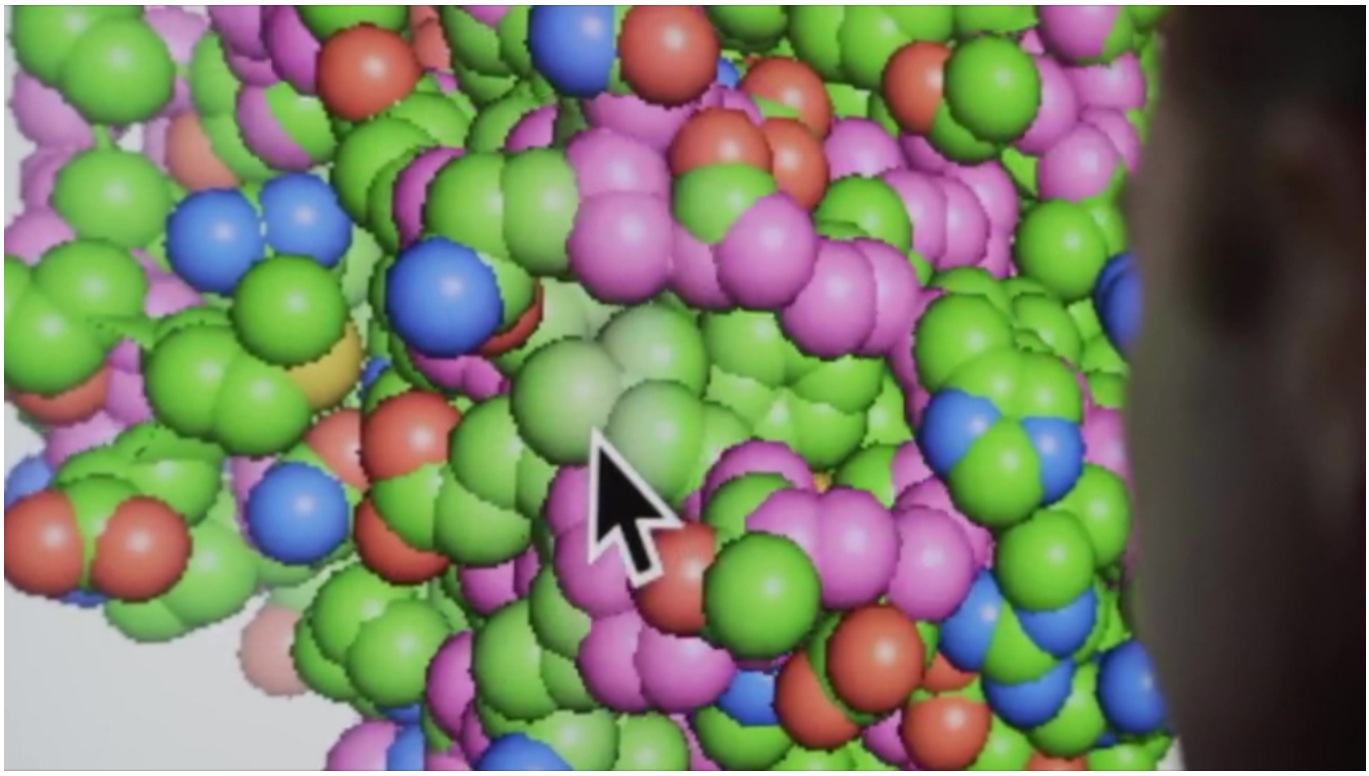
Digitale Lösungen im Zeitalter von Corona: Hackathon und mehr

Der Corona-Krise mit Kreativität begegnen: Das ist augenblicklich eine der großen Herausforderungen. In allen Bereichen des Lebens. Aber wie lassen sich digitale Lösungen nutzen, um sich dem Virus entgegenzustemmen? Das ist eine Frage, die die Bundesregierung tatsächlich gestellt hat. Sie hat einen Hackathon veranstaltet. Eine Art Bewerbungs-Session. Hier konnte jeder seine Ideen präsentieren. Im Netz unter dem Hashtag #WirvsVirus zu finden. Rund 43.000 Leute haben mitgemacht. Welche digitalen Ansätze gibt es?

Anscheinend ist Deutschland sehr kreativ: 43.000 Teilnehmer – eine Menge.

Es gibt sehr viele Ideen, wie sich mit Hilfe von Apps Dinge organisieren lassen. Zum Beispiel Nachbarschaftshilfe: Wer möchte gerne helfen, für andere einkaufen – und wir ist auf solche Hilfe angewiesen? Dafür gibt es Online-Lösungen. Eine Art schwarzes Brett. Es gibt aber auch Vorschläge für ein zentrales Register für Beatmungsgeräte in Deutschland. Damit jederzeit klar ist, wo noch Geräte verfügbar sind – und wo es knapp wird.

Auch elektronische Kulturangebote stehen hoch im Kurs: Da praktisch der gesamte Kulturbetrieb lahm liegt, bieten viele an, Veranstaltungen, Konzerte oder Aufführungen online zu streamen oder abrufbar zu machen. Da braucht es geeignete Werkzeuge, um so etwas auffindbar zu machen. Aber auch zur Unterstützung des Medizinbetriebs gibt es viele Vorschläge. Expertem aus den unterschiedlichsten Bereichen prüfen nun, welche der Ideen womöglich sogar konkret umgesetzt oder gefördert werden können.



Tracken zur Eindämmung

Darunter sind auch Vorschläge, wie sich die Epidemie selbst eindämmen lässt. Etwa Tracking-Systeme, wie wir sie aus Asien kennen.

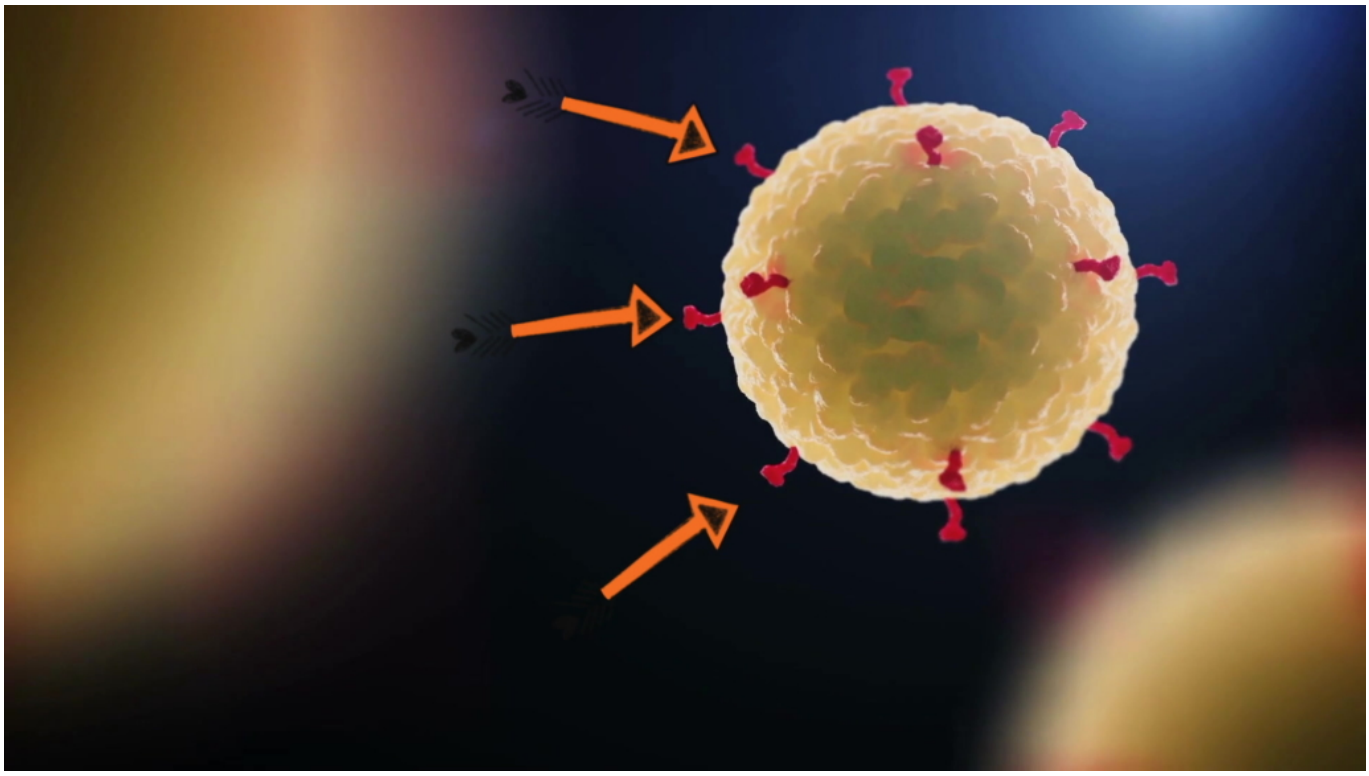
In Asien wurden solche Tracking-Apps aber mitunter verordnet. Bei uns in Deutschland genießt der Datenschutz ein hohes Ansehen. Deswegen müssen andere Lösungen her. Eine App, die sich GeoHealth nennt, ist da ein schönes Beispiel: Hier können Infizierte eine "Datenspende" machen und ihre Bewegungsdaten der letzten 14 Tage abliefern. Komplett freiwillig.

Die Daten werden anonymisiert gespeichert und können helfen, Infektionsketten nachzuvollziehen oder auszuschließen. Jeder Bürger kann prüfen, ob es zu Kontakten mit Infizierten gekommen sein kann. Die App soll die nächsten Tage online gehen und crowd-finanziert sein. Sich mehr oder weniger durch Spenden finanzieren. Funktioniert aber nur dann gut, wenn möglichst viele mitmachen.

Auf dem eigenen Rechner der Forschung helfen

Im Fokus der der Medizin und Wissenschaft steht natürlich die Bekämpfung des Virus an sich. Die Forschen arbeiten mit Hochdruck an Medikamenten und suchen nach einem Impfstoff für Corona. Auch da gibt es Möglichkeiten zu helfen.

Wer das Virus verstehen will, muss Simulationen im Computer durchführen. Das kostet wahnsinnig viel Rechenzeit. Konkret suchen die Forscher nach einem passenden Protein, das in der Lage ist, sich an den sogenannten "Spikes" des Corona-Virus anzudocken – so wie es ein Antikörper auch macht. Denn dann kann das Virus nicht mehr in Körperzellen eindringen, sich nicht mehr vermehren und auch keinen Schaden anrichten. Aber wie sieht dieses Protein genau aus? Es gibt verschiedene Möglichkeiten, da zu helfen.



Wer mag, kann bei Folding@home eine App laden und unbenutzte Zeit auf dem eigenen Rechner zur Verfügung stellen. Die wird dann genutzt, um nach passenden Proteinen zu forschen. Wenn Hunderttausende mitmachen, sind das gigantische Rechenkapazitäten – und das liefert den Forschern möglicherweise die sehnlich erwartete Antwort. Jeder kann mitmachen. Und man verpflichtet sich zu nichts, denn die gespendete Rechenkapazität kann jederzeit angehalten oder beendet werden.

Wie wär's mit einer Server-Spende liebe Profiteure?

Noch besser wäre es natürlich, gleich Supercomputer oder sowas einzusetzen.

Allerdings sind Rechenkapazitäten sehr teuer. Ich finde: Die Profiteure der aktuellen Situation – Konzerne wie Amazon, Google, Microsoft – dürften gerne erhebliche Kapazitäten aus ihren Rechenzentren kostenlos der Forschung zur Verfügung stellen. Das würde so richtig helfen.

TIPP: Hier gibt es zwei wertvolle Guides zum Thema Home Office und Microsoft Office kostenlos zum Download.

Ausgezeichnete Podcasts

Zum ersten Mal wurde in diesem Jahr der "Deutsche Podcast Preis" vergeben. Eine hervorragende Idee - und irgendwie auch allerhöchste Zeit. Denn es gibt nicht nur immer mehr Podcasts, sondern auch viele wirklich gute. Einigen davon sind jetzt offiziell ausgezeichnet!

Podcast liegen schon länger im Trend. In Zeiten von Corona werden sie besonders gerne und häufig konsumiert - wie so viele online erreichbare Angebote und Sendungen.

Während Video-Streaming-Anbieter in Europa ihre Bandbreiten reduzieren, um die Netz-Infrastruktur zu entlasten, ist das bei Podcasts nicht nötig: Audio ist in punkto Bandbreite deutlich genügsamer. Selbst 60 Minuten Podcast in bester Qualität "verbrauchen" weniger Bandbreite als ein paar Minuten Streaming in 4K.

Über 700 Einreichungen - und am Ende sieben Preise

Nur was hören? Die Auswahl ist mittlerweile riesig, auch bei uns in Deutschland. Die Inhalte sind bei Podcasts extrem verschieden: Von unterhaltsam bis nachdenklich, von Laien-Podcast bis zum technisch perfekt gemachten Podcast, der mühelos über einen Radiosender gehen könnte, ist heute so ziemlich alles dabei.

Jetzt gibt es auch einen Deutschen Podcast-Preis: Am Donnerstag (28.03.2020) wurden die besten Podcasts nun offiziell in sechs Kategorien ausgezeichnet.

Geplant war eine große Gala - schon vor einer Woche -, doch Corona hat den Planern einen Strich durch die Rechnung gemacht. Deshalb hat der Deutsche Podcastpreis entschieden, den Preis online zu vergeben.

Eine knapp 55-minütige Sendung, in der Ariana Baborie und Micky Beisenherz Nominierte und Gewinner vorstellen und die verdienten Sieger küren. Also keine Gala light zum Angucken, sondern - stilecht! - als Verleihungs-Podcast.

Die Gewinner sind:

- **Bestes Talk-Team**
  Paardiologie
- **Beste*r Interviewer*in**
  Deutschland 3000
- **Beste Produktion**
  Talk-O-Mat
- **Publikumspreis:**
  Gemischtes Hack
- **Bestes Skript / Beste*r Autor*in**
  Das allerletzte Interview
- **Beste*r Newcomer*in**
  Paardiologie
- **Beste journalistische Leistung**
  Zeit Verbrechen

Publikumspreis? Verzichtbar - weil ohnehin unfair

So wie der Grimme Online Award (GOA) kennt auch der Deutsche Podcast-Preis einen **Publikumspreis**. So wirklich fair ist diese Kategorie niemals. Denn natürlich hat immer der/die Nominierte mit der ohnehin größten Fan-Schar automatisch die größten Chancen.

Klickbefehl an die Crowd - und: Preis gesichert. Deshalb ist ein Publikumspreis in meinen Augen nicht wirklich aussagekräftig, ja sogar überflüssig. Lieber eine weitere Kategorie aufmachen, in der faire Chancen für alle bestehen.

Die Preise zeigen: Einen eindeutigen Trend gibt es nicht. Es wurden Podcasts prämiert, die gut unterhalten (Gemisches Hack), die fesseln und packen (Zeit Verbrechen), aber mit Talk-O-Mat ein Podcast, der überrascht - denn hier treffen zwei Prominente im "Blind Date" aufeinander, was mir persönlich sehr gut gefällt. Die jeweils geladenen Gäste wissen vorher nichts voneinander und springen ins kalte Wasser.

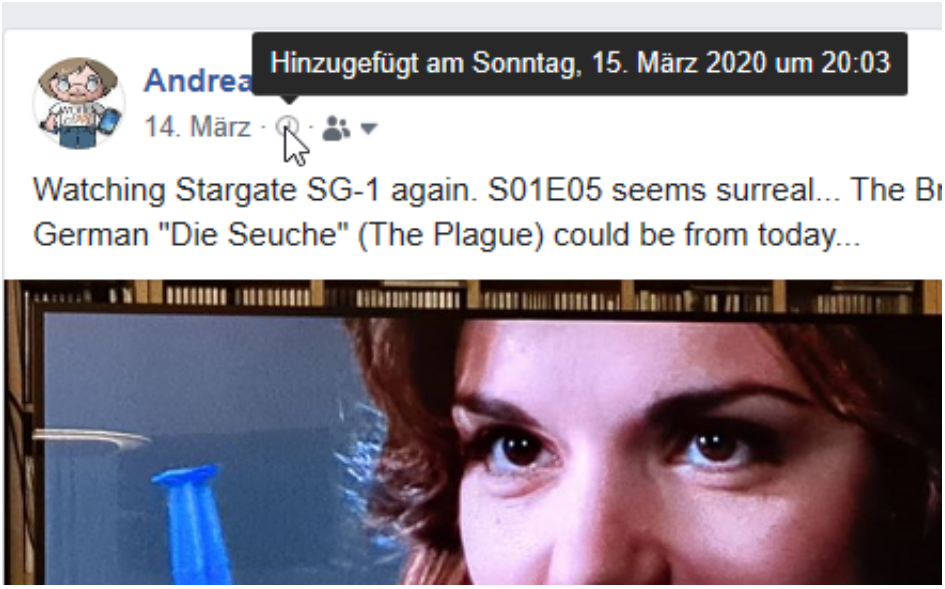
Ansonsten: Klasse, dass es endlich einen Deutschen Podcast-Preis gibt. Eine 148-köpfige Crowd-Jury hatte die schwierige Aufgabe, die besten Podcasts zu finden und zu küren. So ein Preis ist immer ein Ansporn für alle, selbst Podcasts machen, alles zu geben. Die Qualität steigt, das Angebot wird breiter. Gut für alle. Vor allem für all jene, die gerne Podcasts hören.

Vorsicht bei Propheten: Facebook und das Beitragsdatum

In Zeiten von Unsicherheit und Krisen hat eine dunkle Seite der Menschen Hochkonjunktur: Das Geschäft mit der Angst. Das zeigt sich unter anderem auch bei Meldungen in den sozialen Netzwerken wie Facebook, wo dann plötzlich auf Prophezeiungen von vor Jahren verwiesen wird, in denen die Krise schon vorhergesagt wurde. Wir zeigen Ihnen, wie das funktioniert und wie sie das erkennen können.

Normalerweise zeigt Facebook das Datum des Posts direkt unter dem Namen des Postenden an. Beim Schreiben haben Sie keine Möglichkeit, ein abweichendes Datum anzugeben. Nun kann es aber sein, dass Sie nachträglich ein Ereignis einstellen müssen. Dann posten Sie den Beitrag, klicken dann auf die drei Punkte rechts und auf **Datum ändern**.

Sie können nun ein beliebiges Datum (und auf Wunsch auch eine Uhrzeit) in der Vergangenheit eingeben, und schon ändert sich die Datumsangabe im Beitrag. Das bleibt allerdings nicht ohne Folgen: In einem solchen Fall erscheint neben dem Datum ein Uhrsymbol.



Halten Sie die Maus auf das Uhr-Symbol, dann bekommen Sie das ursprüngliche Datum angezeigt. Das ist unveränderlich und entlarvt einen Versuch, einen falschen Eindruck zu erwecken.

Sicherheitstipps für Windows-Benutzer im Jahr 2020

Derzeit arbeiten mehr Menschen im Home Office und vernetzt als jemals zuvor. Eine Hochzeit für Betrüger und Cyberkriminelle, denen so mehr potenzielle Opfer zur Verfügung stehen. Sie versuchen mit allen Tricks, die Menschen in Fallen zu locken.

Pishing-Mails, Identitätsdiebstahl, Datenmissbrauch, Cyberattacken: Die Liste möglicher Online-Verbrechen und Betrügereien wird immer länger. Mit der zunehmenden Nutzung von Computern nehmen die Sicherheitsbedrohungen sprunghaft zu. Das stellt nicht nur Unternehmen, sondern auch Privatnutzer vor neue Herausforderungen.
Auch wenn Sie sich mit der Frage Ihrer Online-Sicherheit ausführlich beschäftigt haben, ändern sich die Zeiten schnell: Online-Kriminelle werden immer geschickter und wenden bei ihren Betrugsversuchen die neuesten Techniken ein.

Wer glaubt, durch regelmäßige Windows-Updates allein gut geschützt zu bleiben, der täuscht sich: Erst vor kurzem hat Microsoft einen Sicherheitshinweis veröffentlicht, der über eine ungepatschte Schwachstelle im SMB-Protokoll informiert. Eine große Gefahr, da dieses Leck beispielsweise zur Verbreitung wurmartiger Viren führen kann. Diese Sicherheitsanfälligkeit wurde als „Eternal Darkness“ und „GMBGhost“ bezeichnet.

Ein Sicherheits-Update zum Schließen dieser Schwachstelle ist erst einige Zeit später gekommen. Was zeigt: Man kann sich nicht darauf verlassen, dass die Patches immer rechtzeitig ausgeführt werden.

Daher: Nur wer seine Schutzmaßnahmen regelmäßig auf den neuesten Stand bringt, bleibt auf der sicheren Seite.

Deshalb hier einige Tipps, wie Sie Ihren Computer als Windows-Benutzer schützen und die Risiken im Netz minimieren.

1. Sichere Kennwörter verwenden

Ein sicheres Kennwort schafft ein grundlegendes Sicherheitsniveau und kann somit den Diebstahl persönlicher Daten verhindern. Ihr Kennwort muss mindestens aus 8 Zeichen bestehen und eine Kombination aus Groß- und Kleinschreibung enthalten. Viele Benutzer schreiben Ihre Kennwörter auf, einige verwenden dafür sogar Aufkleber, die neben dem Monitor angebracht werden.

Das ist allerdings nicht empfehlenswert, da die Kennwörter leicht ausspioniert werden können. Außerdem sollten Sie beim Erstellen eines Kennworts nicht Ihren Namen, Spitznamen, Familienmitglieder oder Haustiere angeben, da solch ein Kennwort leicht zu erraten ist.

2. Browser-Verkehr verschlüsseln

Datenverschlüsselung spielt eine wichtige Rolle und macht Ihre Messaging, Speicher- und File-Sharing-Dienste sicher.

Die sogenannte E2E (End-to-End)-Verschlüsselung sorgt dafür, dass die versendeten Inhalte auf dem ganzen Weg vom Absender zum Empfänger verschlüsselt und somit geschützt bleiben. Nur der finale Empfänger hat das Recht die Inhalte zu entschlüsseln.

Dafür ist der Einsatz von VPN-Software notwendig. VPN steht für „virtuelles privates Netzwerk“ und macht eine „getunnelte“ und somit eine sichere und anonyme Datenübertragung möglich. Windows-Benutzer können so eine Lösung zum Beispiel zur Verschlüsselung des Browser-Verkehrs ein VPN für Windows PC verwenden.

3. Zwei-Faktor-Authentifizierung verwenden

Die Zwei-Faktor-Authentifizierung, auch als MFA (Multi-Faktor Authentifizierung) bekannt, ist ein Vorgang, bei dem der Zugriff zu einem Account nur in zwei oder mehreren separaten Schritten

möglich ist. Sie kennen es bestimmt von Ihrer Bank: um sich zum Online-Banking anzumelden, passieren Sie mehrere unterschiedliche Schritte, um Ihre Identifikation nachzuweisen.

Die einfachste und bekannteste Kombination ist „Benutzername und Kennwort“, aber es gibt inzwischen schon komplizierte und somit auch sicherere Authentifizierungsmethoden. Die Multi-Faktor-Authentifizierung ist eine wirksame Maßnahme zum Schutz Ihres Accounts und soll auf jeden Fall akzeptiert und verwendet werden.

4. Vor Phishing-Angriffen schützen

Über gefälschte Webseiten, E-Mail mit Links oder Anhängen versuchen die Internet-Betrüger mit verschieden Tricks an Ihre persönlichen Daten zu kommen. Diese illegale Datenbeschaffung wird im EDV-Jargon als Phishing bezeichnet.

Um sich vor Phishing zu schützen, sind einige Vorsichtsmaßnahmen gefragt. Öffnen Sie keine Links in unbekannten und unerwarteten E-Mails und laden Sie keine Anhänge herunter.

Auch beim Surfen ist Vorsicht geboten: oft begegnet man den gefälschten Links auch auf bekannten und auf den ersten Blick vertrauenswürdigen Seiten.
Das gleiche betrifft das Streaming oder Herunterladen von Inhalten aus unsicheren Quellen.

Auch hier können Sie über die Links auf unsichere Seiten weitergeleitet werden.

5. Regelmäßig aktuelle Patches und Updates installieren

Online-Kriminelle programmieren Viren, die Schwachstellen in Betriebssystemen, Webbrowsern und Softwareanwendungen leicht finden können. Wenn ein Benutzer eine bestimmte Website besucht oder eine Anwendung aufmacht, wird das Gerät infiziert. Deswegen ist es wichtig, die neuesten Patches und Updates von Microsoft zu installieren, um Ihren Computer vor solchen Bedrohungen zu schützen. Alternativ können Sie einfach automatische Updates aktivieren.

Die Aktualisierung der Online-Sicherheitssoftware in Echtzeit ist sehr wichtig, um die Sicherheit vor neuer und komplizierter Malware, Viren und Trojanern zu gewährleisten. Daher wird fast jede Online-Sicherheitssoftware automatisch aktualisiert, ohne dass Benutzer eingreifen

müssen.

6. Führen Sie regelmäßige Scans durch

Windows verfügt über ein integriertes Online-Sicherheitssystem, in dem Sie die den Zeitraum für die Scans einstellen können. Das regelmäßige Scannen hilft beim, die Gefahren und unsichere Systemeinträge rechtzeitig zu erkennen und deren schädliche Wirkung zu verhindern.

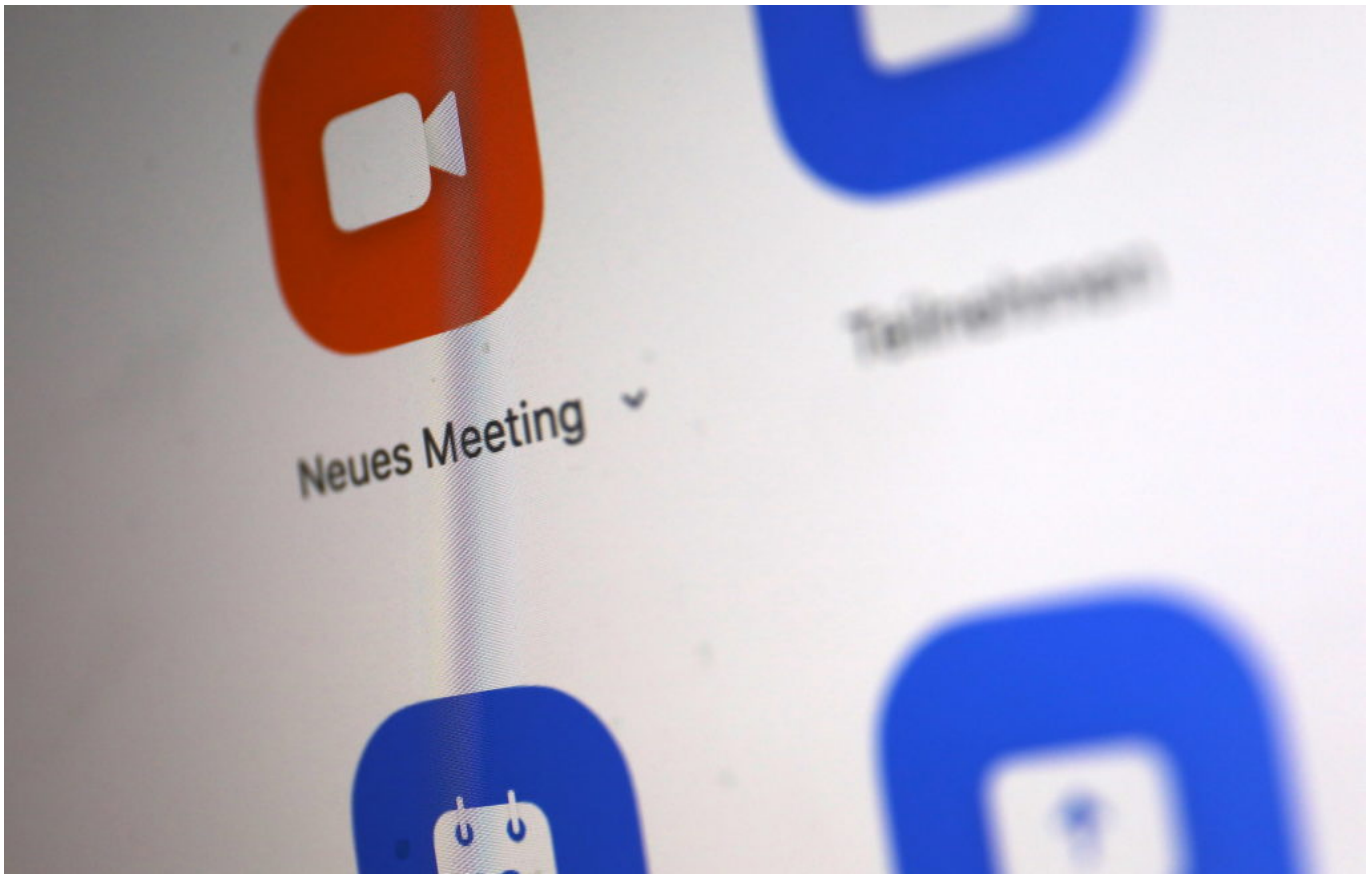
Denken Sie daran, Ihre Schutzmaßnahmen regelmäßig zu aktualisieren und sich über die Neuigkeiten zu informieren. Es lohnt sich auf jeden Fall präventiv zu handeln um den Schaden und damit verbundene hohe Kosten zu vermeiden.

Und es hat Zoom gemacht: Video-Chats unsicher

Schnell mal eine VIdeokonferenz einrichten oder mit Kollegen plaudern? Viele greifen da reflexartig zu Skype. Dabei gibt es viele interessante Alternativen. Vor allem Zoon erfreut sich gerade riesiger Beliebtheit. Doch wie sich zeigt, hat die populäre Video-App erhebliche Sicherheitslücken. Mehrere!

Videokonferenzen? Hat es schon immer gegeben - aber so viele wie gerade waren es wohl noch nie. Nun nutzen auch die vielen Menschen im Corona-Home-Office häufiger als sonst Video-Chat-Systeme, etwa in Microsoft Teams, Skype, GotoMeeting oder Zoom. Sie kommen via Internet mit Kolleginnen und Kollegen ins Gespräch.

Aber es sprechen auch Ärzte mit ihren Patienten übers Netz. Oder Lehrerinnen und Lehrer mit ihren Lernenden. Yoga in der Zoom-Konferenz: Früher undenkbar, heute fast Standard.

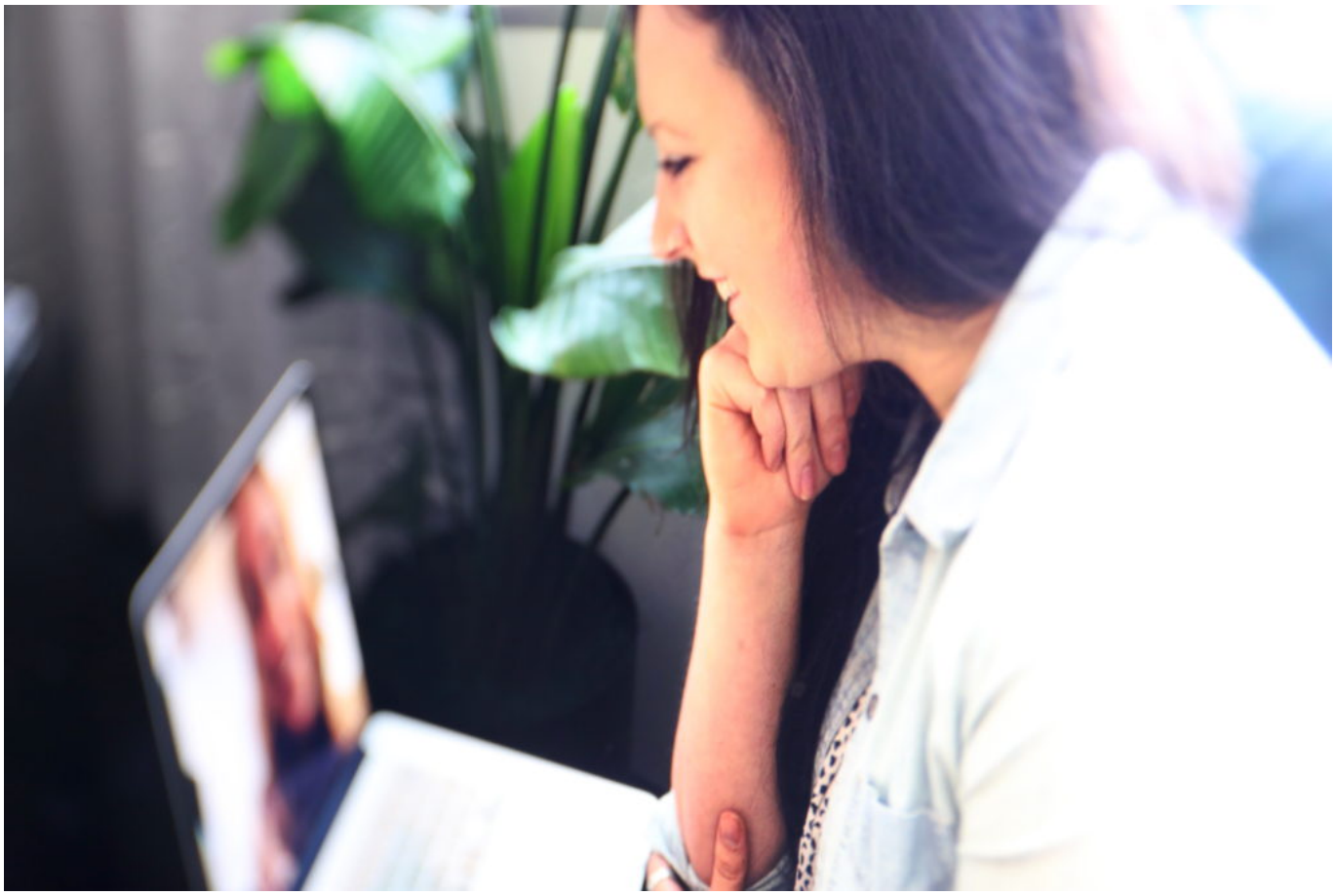


Rasantes Wachstum bei Zoom

Ein großer Profiteur dieses Booms ist der Anbieter Zoom aus Kalifornien. Die Zahl der monatlichen Nutzer bei diesem praktischen Video-Chat-Dienst ist in den letzten Tagen um rasante 190 Prozent gestiegen. Ein regelrechter Boom! Es scheint, als nutze alle Welt gerade Zoom.

Weil es so einfach ist: App installieren oder im Browser starten - fertig. Nur einer muss die App benutzen, alle anderen können einfach im Browser mitmachen. Einfach. Bequem. Kostenlos. Nur wer mehr als 40 Minuten oder in größeren Gruppen plaudern will, muss für den Dienst überhaupt zahlen.

Doch nun häufen sich Berichte über erhebliche Sicherheitslecks. So haben sich Nutzer beim FBI gemeldet, weil in Zoom-Schalten von Lehrern und Schülern plötzlich pornografische Inhalte zu sehen waren. Oder Hassbotschaften mit Hakenkreuz. Offensichtlich ist es Fremden gelungen, sich in bestehende Konferenzen einzuklinken und mitzumachen.



Konferenzsystem nicht gut abgesichert

Denn das Startup hat sein Konferenzsystem nicht genügend abgesichert. Es ist unverantwortlich, dass sich Fremde einfach so Zugang verschaffen können... Das ist zwar der Einfachheit des Systems geschuldet, müsste aber deutlich besser abgesichert sein.

Immerhin: Nutzer können sich schützen, indem der "Gastgeber" (Host) eines Video-Chats jeden Gast manuell in den Chat holt. Dann kann zumindest ein solches "Zoom Bombing" nicht passieren.

Ausspioniert über die Handy-Kamera

Aber das ist längst nicht alles. Es gibt erhebliche Bedenken, was die Datensicherheit anbelangt. Auf iOS-Geräten hat die App Daten an Facebook geschickt, etwa über Modell, freien Speicher und Display-Größe - selbst bei Usern, die gar nicht Mitglied sind bei Facebook.

Außerdem war es auf Apple-Geräten aufgrund schlampiger Programmierung möglich, die Kamera im Handy zu aktivieren und die User ausspionieren. Selbst wenn die App nicht aktiv ist, ja sogar selbst nachdem sie deinstalliert wurde.

Am Ende nur Lippenbekenntnisse

In den USA kümmern sich Staatsanwaltschaft und FBI um die krassesten Fälle. Natürlich beeilt sich das Unternehmen zu unterstreichen, wie wichtig ihm Datenschutz und Privatsphäre seien. Es würden keine Nutzerdaten verkauft etc.

Aber am Ende sind das nur Lippenbekenntnisse. Wäre es wirklich so, wäre es nicht so solch eklatanten Sicherheitsverstößen gekommen. Auch andere Chat-Systeme wie Skype fallen immer wieder durch Sicherheitsprobleme auf.

Es braucht dringend eine Art TÜV für Apps

Das zeigt: Auch wenn man den Eindruck hat, bei einem Video-Chat "unter sich" zu sein - es entspricht keineswegs immer den Tatsachen. Video-Chats sind alles andere als eine sichere Sache!

Es braucht meiner Ansicht nach dringend eine Art TÜV für derlei sensible Apps: Denn wer möchte vertrauliche Gespräche führen mit dem Risiko, abgehört oder ausgeschnüffelt zu werden? Niemand!

Werkzeuge für Homeoffice für unter 10€

Corona zwingt viele Menschen ins Home Office. Derzeit arbeiten mehr Menschen von zu Hause als jemals zuvor. Doch nicht alle bekommen die nötige Sofware vom Arbeitgeber gestellt. Einige Anbieter verkaufen wichtige Software derzeit sogar zu Sonderpreisen.

Ob Quarantäne oder Kontaktverbot: Viele arbeiten im Augenblick von zu Hause und lernen die Möglichkeiten der Digitaisierung besser kennen. E-Mails von Kunden beantworten, mit Kolleginnen und Kollegen in Kontakt stehen, die Software im Konzern nutzen, Daten beaebeiten oder Video-Konferenzen abhalten: Die Bandbreite der Möglichkeiten ist riesig. Viele Mitarbeiter müssen sich erst mal einarbeiten und die Besonderheiten kennenlernen.

Microsoft Office - das Online-Abo Office 365 soll übrigens ab 21. April 2020 Microsoft 365 heißen! - bietet viele Möglichkeiten, um im Team an Dokumenten zu arbeiten. Gemeinsam mit Kollegen Texte erfassen und bearbeiten, Zahlen und Listen in Excel durcharbeiten, Powerpoint-Dokumente erstellen oder Präsentationen halten: Mit Office kein Problem.

Microsoft Office 2019 nur 29,50€!

Microsoft Office muss ich niemand erklären – alle kennen die Büro-Software und die meisten brauchen sie auch. Wer sein Büropaket auf den neuesten Stand bringen will oder muss, kann einfach auf Office 2019 upgraden – und auch das vergleichsweise kostengünstig.

Mit dem Gutscheincode **WD50L** erhalten Kunden bei Keysworld ein Office.Upgrade für 29,50€.

Windows 10 für 8,67€!

Sobald Sie sich mit einem Microsoft-Konto bei einem Windows-10-PC anmelden, werden die individuellen Konfigurationseinstellungen und Benutzerprofilinformationen automatisch übernommen. Auch persönliche Daten in der Cloud – mit einer Kombination aus Microsoft OneDrive und Box – müssen der Benutzer nicht manuell übertragen, sondern das passiert beim Upgrade automatisch.

Windows 7 und ältere Versionen sollten im Home Office nicht zum Einsatz kommen. Sie sind angreifbar. Anbieter wie Keysworlds bieten derzeit Sonderkonditionen an, damit Menschen im Home Office sich günsitg ausrüsten können. Ein Upgrade auf Windows 10 soll demnach nur 8,67€ kosten. Dazu bei einer möglichen Bestellung den Rabattcode **TLIZ35** nutzen.

Der Gutscheincode **WD50L** sollte für 50% Rabatt sorgen.

- Office 2019 Professional Plus (1PC): 29,50€
- Windows 10 Pro + Microsoft Office 2019 Pro: 35,00€

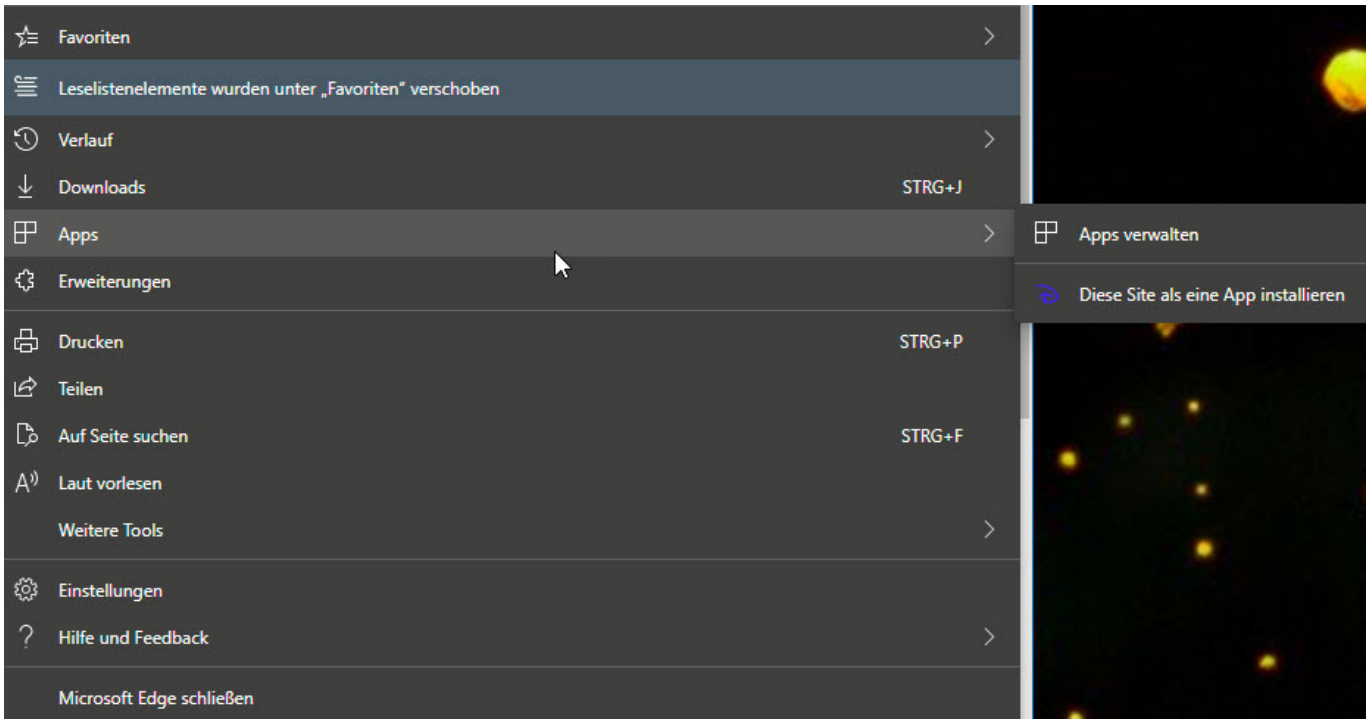
Auf viele andere Produkte gibt es 38% Rabatt. Hier denPromo-Code **TLIZ35** nutzen.

- Windows 10 Professional (1PC): 8,67€

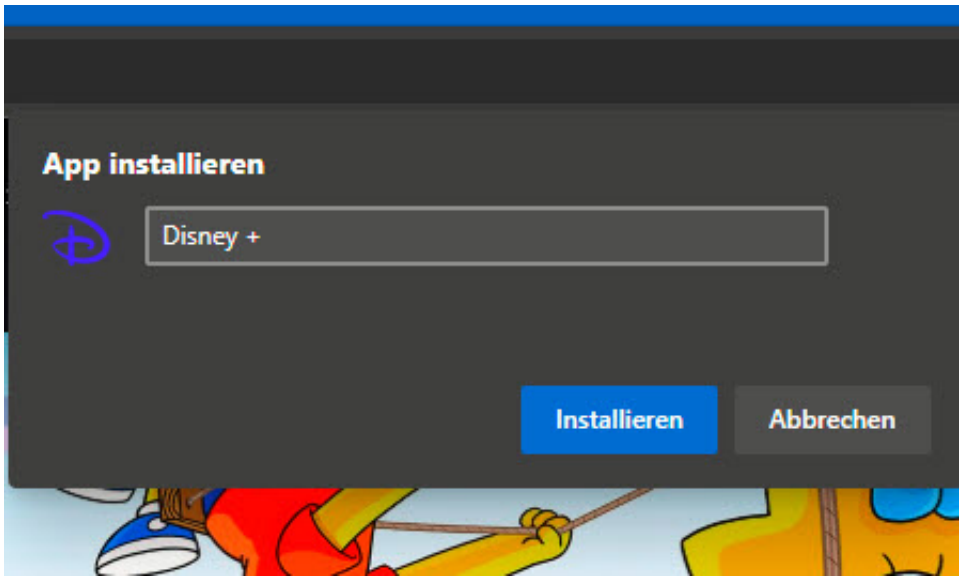
Disney + App selber bauen für Windows 10

Windows 10 war mal gestartet, um mit der Kachelwelt die Desktops abzulösen. Das hat sich mit der Zeit immer mehr als gescheiterter Versuch der Touch-Fähigkeit herausgestellt. Von Version zu Version von Windows 10 ist Microsoft immer weiter davon weggegangen, und das haben auch die App-Anbieter übernommen. Immer mehr Windows Store-Apps werden zurückgezogen, neue Apps gar nicht mehr angeboten. Das trifft auch Disney +. In wenigen Schritten können Sie das aber selber machen!

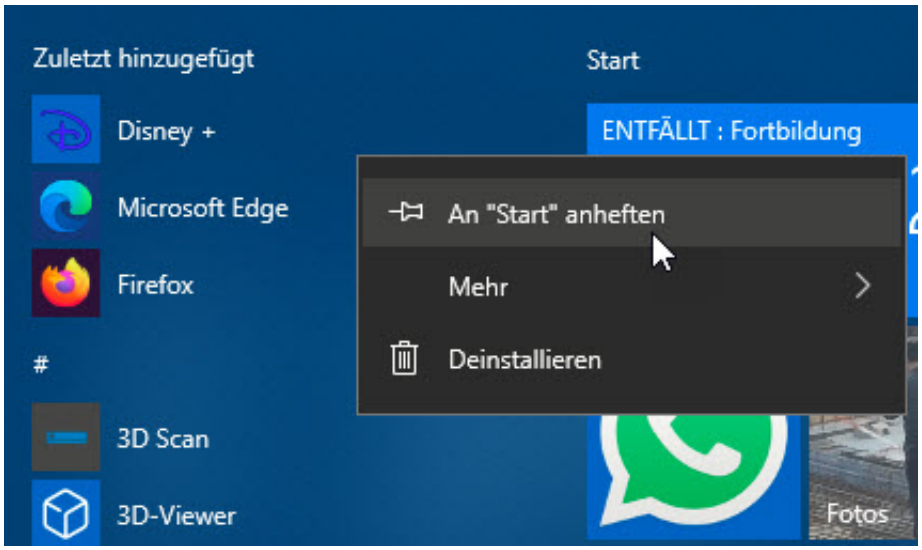
Das Zauberwort heißt hier "Progressive Web Apps", abgekürzt PWA. Das ist am Ende nichts anderes als das Erzeugen einer App aus einer Webseite, die dann aus dem Startmenü startbar ist und wie eine App aussieht und reagiert. Das geht mit Chrome und dem neuen Microsoft Edge, den Sie hier herunterladen können.



Rufen Sie die Disney +-Webseite auf, dann klicken Sie oben rechts auf die beiden Punkte, dann auf **Apps** > **Apps verwalten** > **Diese Site als eine App installieren**. Geben Sie der neuen App einen sprechenden Namen. Windows 10 öffnet die neue App nun direkt.



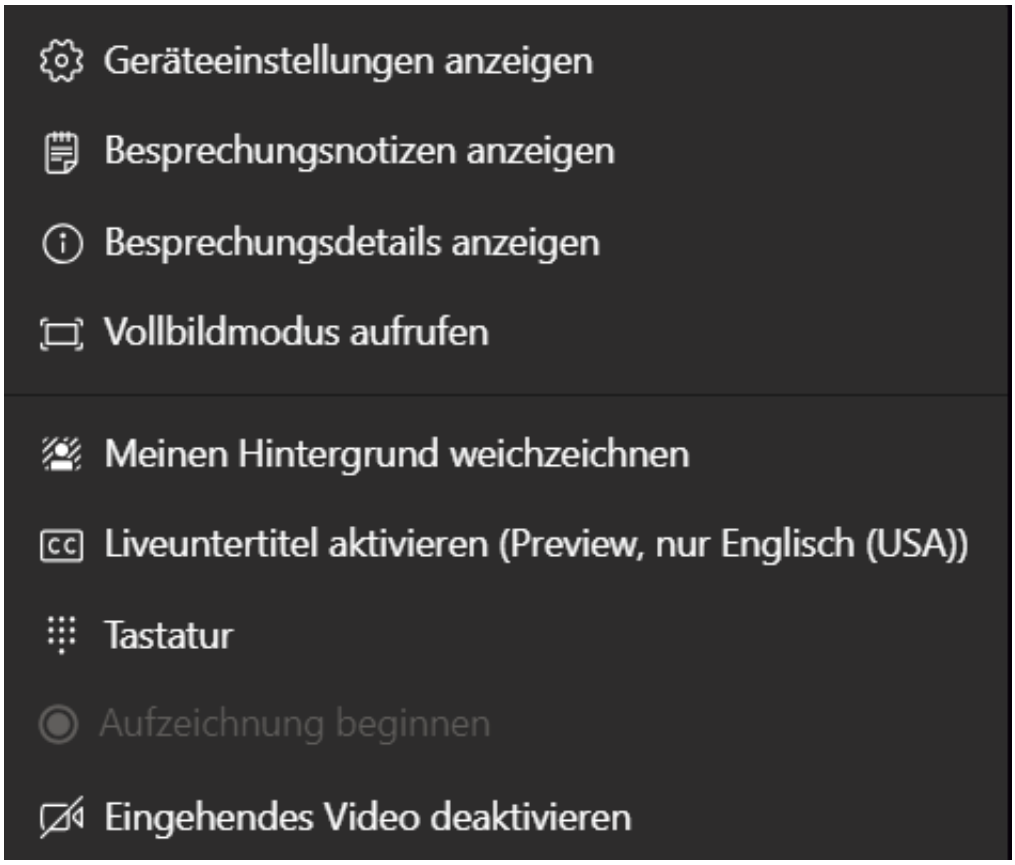
Für Windows ist die PWA-App tatsächlich eine echte App, darum finden Sie sie im Startmenü auch in der Liste der zuletzt installierten Apps unter **Zuletzt hinzugefügt**. Klicken Sie mit der rechten Maustaste hinein und dann auf **An "Start" anheften**. Schon haben Sie eine neue Kachel im Startmenü. Einen Unterschied zu einer echten App können Sie gar nicht mehr erkennen.



Netiquette in Teams: Schlabberlook ade!

In Zeiten des Corona-Virus entscheiden sich immer mehr Unternehmen, vom persönlichen vor-Ort-Termin auf eine virtuelle Terminplanung umzusteigen. An einem PC oder Mac irgendwo in einer sicheren Umgebung per Videokonferenz teilzunehmen ist meist nicht spürbar ineffizienter. Microsoft Teams ist eines der verbreiteten Systeme. Wenn Sie einige einfache Maßnahmen beherzigen, dann klappt es auch mit der Videokonferenz!

Zu allererst: Eine Videokonferenz ist immer noch eine firmeninterne Veranstaltung. Auch wenn Sie zuhause auf der Couch sitzen, gilt eine gewisse Netiquette. Wenn die Kamera verwendet werden sollte, sollten Sie besser nicht Ihr liebstes Schlabber-T-Shirt tragen, sondern - zumindest obenrum im Erfassungsbereich der Kamera - vernünftig gekleidet sein.



Auch der Erfassungsbereich der Kamera an sich ist ein Thema: So aufgeräumt wie Ihr Büro oder Wohnzimmer auch sein mögen, der Hintergrund ist meist nicht im Fokus. Ob es nun das Trucker-Babe im Poster oder das vollkommen chaotische Aktenregal ist: Drehen Sie die Kamera so, dass der Hintergrund möglichst neutral ist. Bei Teams können Sie dazu noch ein technisches Hilfsmittel nutzen. Klicken Sie mit der Maus auf die drei Punkte in der Übersichtsleiste. Im sich öffnenden Menü klicken Sie auf **Meinen Hintergrund weichzeichnen**. Dann wird der Hintergrund um Ihren Kopf so verzerrt, das keine Details mehr sichtbar sind.

Herausfinden der Windows-Version

Viele Artikel rund um neue Funktionen oder Fehlerbehebungen in Windows erwähnen immer wieder die Versionsnummer: "In 1909 hat Microsoft das geändert" oder "Wenn Sie noch 1809 haben, dann...". Diese Versionsnummer war bei früheren Windows-Versionen noch direkt in der Systemsteuerung ablesbar. In Windows 10 versteckt sie sich ein wenig tiefer. Wir zeigen Ihnen, wo Sie sie finden!

Die Versionsnummer von Windows teilt sich in zwei Teile auf: Die **Version** an sich gibt die Ausbaustufe von Windows an, im Normalfall die Version des Feature-Updates (von Microsoft mittlerweile halbjährig ausgerollt. Dazwischen gibt es aber immer wieder Updates. Diese ändern die Versionsnummer nicht, sondern die zweite Angabe, den **Build**. Es gibt zwei Versionen, sich diese Angaben anzeigen zu lassen.

Gehen Sie in die **Einstellungen**, dann klicken Sie auf **System** > **Info**. Im zweiten Infoblock unter Windows-Spezifikationen sehen Sie dann Version und Betriebssystembuild. Ganz nebenbei sehen Si darüber dann auch alle relevanten Informationen zu Ihrem PC, wie den Prozessor, den Hauptspeicher und vieles mehr.

Alternativ drücken Sie gleichzeitig die Tasten **Windows** + **R** und geben Sie im Eingabefeld **winver** ein. Hier bekommen Sie dann nur die Versions- und Buildinformationen angezeigt.


Info
Windows 10
Microsoft Windows
Version 1809 (Build 17763.1098)
© 2018 Microsoft Corporation. Alle Rechte vorbehalten.
Das Betriebssystem Windows 10 Pro und die zugehörige Benutzeroberfläche sind durch Marken- und andere rechtsabhängige bzw. bestehende gewerbliche Schutz- und Urheberrechte in den Vereinigten Staaten und anderen Ländern geschützt.
Dieses Produkt ist unter den Microsoft-Softwarelizenzbedingungen lizenziert für:
Benutzername
Unternehmensname
OK

Herausfinden des Gerätetyps bei iPad, MacBook, Surface

Besonders die Geräte der Betriebssystemhersteller wie Apple und Microsoft haben ein stabiles Element: Sie sehen sich zwischen den Modellreihen oft sehr ähnlich. Das macht es dem Benutzer nicht ganz einfach, anhand des Geräts in der Hand herauszufinden, um welches Modell es sich handelt. Sie müssen aber nur wissen, wo Sie nachschauen müssen!

Bei Apple gestaltet sich das Ganze recht einfach, wenn macOS läuft. Egal ob auf einem MacBook oder einem iMac: Klicken Sie auf den Apfel oben links im Finder, dann auf **Über diesen Mac**. Unter der Angabe des Betriebssystems sehen Sie alle relevanten Daten des Geräts, unter anderem auch die Modellbezeichnung.

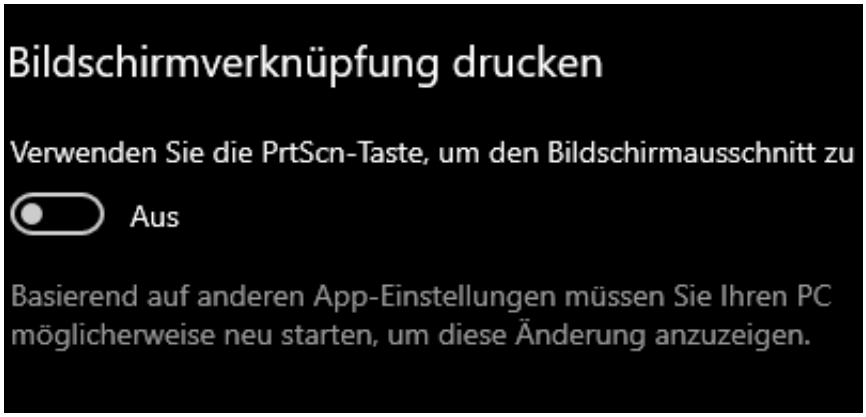
Bei iPhones und iPads tippen Sie auf **Einstellungen** > **Allgemein**, dann finden Sie unter Modellname das Modell des Gerätes. Was aber, wenn das Gerät nicht mehr an geht? Dann brauchen Sie gute Augen! Jedes der Geräte hat eine eigene Modellbezeichnung, die Sie ganz winzig auf der Rückseite finden. Suchen Sie den Bereich, wo Sie Schriftzeichen erkennen. Mit einer Lupe (oder der Kamera Ihres Smartphones, mit der Sie dann das Bild vergrößern können) können Sie unter Model die Bezeichnung finden. Mit der Suchmaschine Ihrer Wahl finden Sie ohne großen Aufwand heraus, um welches Gerät es sich handelt.

Das selbe Verfahren können Sie bei den Microsoft Surface-Geräten anwenden: Unter dem Kickstand, dem ausklappbaren Ständer, finden Sie ebenfalls die Modellnummer, die Google & Co. dann schnell in eine Modellbezeichnung umwandeln.

Wenn das Screenshot-Programm nicht funktioniert

Wenn Sie mit Windows arbeiten, dann werden Sie immer mal wieder Bildschirmfotos machen müssen, um bestimmte Dinge zu veranschaulichen. Ob es nicht funktionierende Dinge und Fehlermeldungen sind, Abbildungen, über die Sie reden möchten: Einfacher als ein Bildschirmfoto zu machen geht es nicht. Dafür wird in den meisten Fällen die Taste **Druck** oder **PrntScr** auf der Tastatur verwendet. Was aber, wenn die nicht will?

In einfachsten Fall können Sie das Snipping tool von Windows, das auf jedem Windows 10-Rechner vorinstalliert ist, nutzen. Wenn Ihnen das nicht reicht, dann gibt es kostenlose Programme wie GreenShot und professionelle Lösungen wie SnagIt. Welche Lösung Sie tatsächlich einsetzen ist relativ egal, zum Aktivieren müssen Sie eine Taste drücken. **Druck** oder **PrntScr** bieten sich hier an und werden meist vorkonfiguriert. Allerdings hat Windows eine eigene Funktionalität, die hier stören kann.



Unter **Einstellungen** > **Erleichterte Bedienung** > **Tastatur** können Sie ganz unten aktivieren, dass Windows intern die Bildschirmausschnitt-Funktion über diese Taste startet. Ist das der Fall, dann steht diese Taste nicht für andere Programme zur Verfügung. Schalten Sie die Funktion aus, dann funktionieren die Drittanbieter-Programme immer noch nicht. Starten Sie sie neu, oder de- und reinstallieren Sie sie, um die Zuweisung der Taste hinzubekommen.

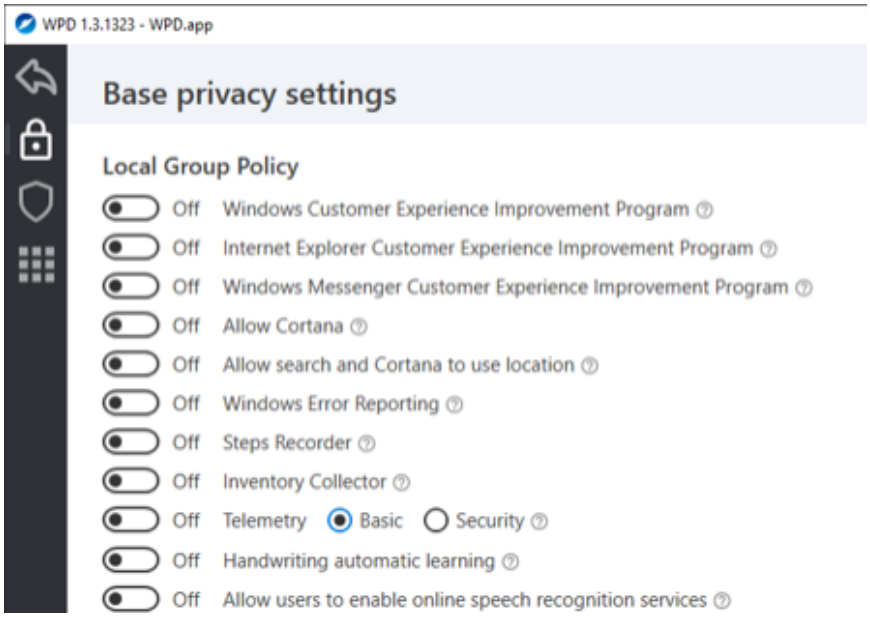
Sehr viel komfortabler funktioniere Screenshots mit Spezialprogrammen. Sie bieten deutlich mehr Möglichkeiten. Wer sogar Screencasts braucht, also nicht nur ein "Foto" des aktuellen Bildschirms, sondern ein kleines Video - etwa, um einen Ablauf zu demonstrieren, einen Videoguide herzustellen oder ein Webinar anzubieten -, der kann zum Beispiel den Screen Recorder von Movavi auspobieren. Hier lassen sich komortabel Screen-Casts erstellen - und bei Bedarf auch gleich besprechen, mit Musik versehen und schneiden. Einfach kostenlos ausprobieren!

Optimierung der Datenschutzeinstellungen unter Windows 10

Die Datenschutzeinstellungen des Betriebssystems sind für immer mehr Anwender interessant. Im Hintergrund laufen so viele Prozesse, die unter anderem der sogenannten Telemetrie, also der Aufnahme der "Systemgesundheit" dienen. Microsoft versucht. anonym so viel wie möglich Daten von Ihrem PC zu erhalten, um frühzeitig auftretende Fehler zu erkennen und in kommende Updates ausnehmen zu können. Im System selbst hat Microsoft viele Optionen weggestrichen. Wir zeigen Ihnen, wie Sie diese trotzdem nutzen können!

Viele Datenschutzeinstellungen sind von Microsoft in die Gruppenrichtlinien verfrachtet worden. Diese sind eigentlich das Handwerkszeug der Administratoren. Normalanwender beschäftigen sich damit eher wenig. Dafür gibt es aber eine kleine Freeware, mit denen Sie die Datenschutz-Einstellungen von Windows 10 viel feiner beeinflussen können als im Standard.

Das Windows Privacy Dashboard (WPD) können Sie kostenlos hier herunterladen. Unter "Datenschutz" finden Sie die wichtigsten Group Policies und können diese ein- und ausschalten. Wenn Sie nicht sicher sind, was eine Einstellung bewirkt, dann klicken Sie auf das kleine Fragezeichen neben ihrem Namen. Die App zeigt Ihnen dann einen kurzen Hilfetext als Erklärung an.



Mit der App werden Sie Windows nicht komplett datenschutzkonform machen und die Datensammlung nicht komplett verhindern. Sie können aber zumindest einen großen Schritt dahin machen!