Schieb Report

Ausgabe 2018.32

Kein Einschlafen bei zweitem Monitor

Sieht man sich auf einem externen, zweiten Bildschirm einen Film an, schaltet Windows manchmal in den Standby-Modus, wenn man zu lange inaktiv ist. Das lässt sich mit einem eigenen Energie-Plan und einem kleinen Skript leicht ändern.

Zunächst erstellt man zwei Energie-Pläne. Bei einem dieser Pläne sollte der Standby-Modus aktiviert sein. Die Energie-Pläne können erstellt werden, indem [Win]+[R] gedrückt, **powercfg.cpl** eingegeben und mit Klick auf **OK** bestätigt wird. Bei den Einstellungen des einen neuen Plans sollte der Standby-Modus für Akku und Netzbetrieb auf **Nie** gestellt sein.

Im nächsten Schritt finden wir die IDs der beiden Energie-Pläne heraus. Das klappt am einfachsten über die Konsole, indem hier der Befehl **powercfg /l** (kleines L) genutzt wird.

AutoHotkey-Script erstellen

Nun in ein neues Editor-Fenster das folgende Skript einfügen und dabei die beiden GUIDs anpassen – die obere sollte sich auf den Plan beziehen, bei dem der Standby-Modus deaktiviert ist, die untere auf den Energie-Plan mit aktiviertem Standby-Modus.

```
OnMessage(0x219, "MsgMonitor")   MsgMonitor(wParam, lParam, msg)   {
 if (wParam = 7) {   Run, powercfg /s 381b4222-f694-41f0-9685-ff5bb260
df2e   } Else {   Run, powercfg /s 381b4222-0001-2222-3333-00000000000
0   }   MsgBox check %wParam% and %lParam% and decide to run programs
```

```
with %msg%  }  ;wParam: 7 lParam: 0 monitor connected  ;wParam: 32772
lParam: 8977536 should be on disconnected
```

Zum Schluss dieses Skript mit der Endung **.ahk** speichern. Es lässt sich dann mit der Freeware AutoHotkey ausführen. Wer die Automatik ständig aktiv haben möchte, setzt das Skript einfach in den Autostart. Ab sofort wechselt Windows den Energie-Plan automatisch, je nachdem, ob ein externer Monitor angeschlossen ist oder nicht.

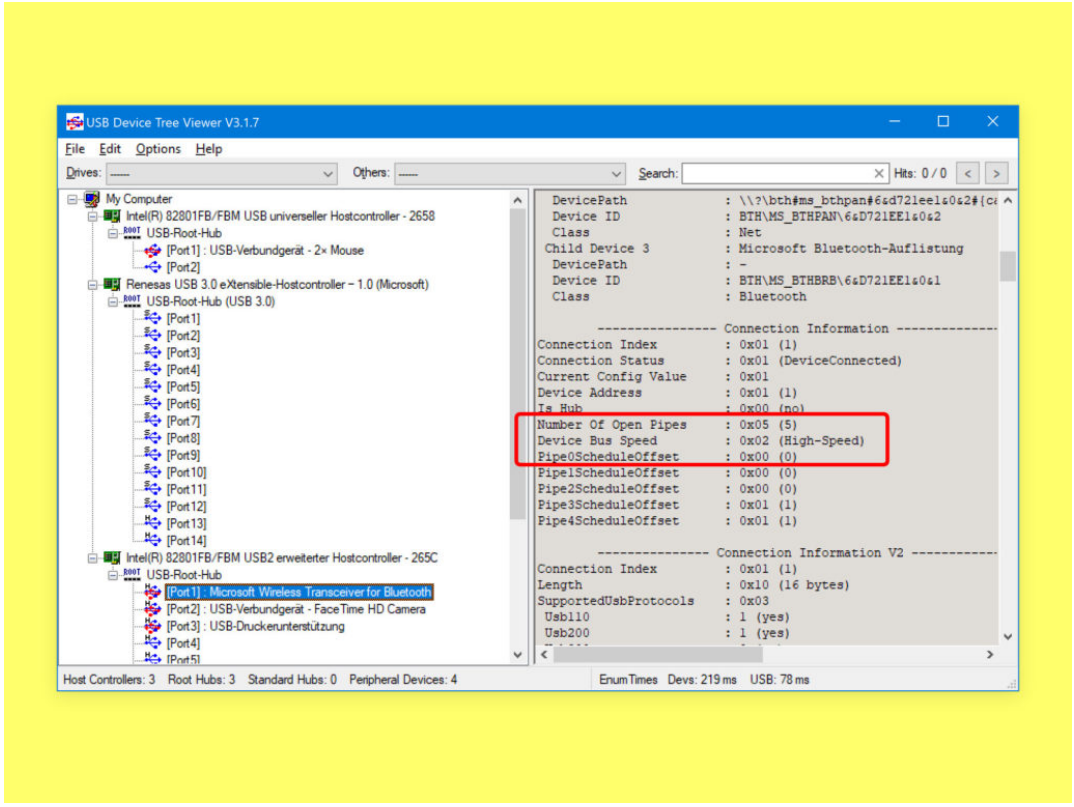
USB-Version ermitteln

An vielen Computern unterstützen nicht alle USB-Anschlüsse den neuesten Standard. Schließt man dann ein Gerät, etwa eine externe Festplatte, an einen Port an, der nur einen älteren Standard unterstützt, wie z.B. USB 2.0, wird das Gerät langsamer. Welche USB-Version bei einem bestimmten Anschluss möglich ist, lässt sich mit einem kostenlosen Tool ermitteln.

Für Klarheit sorgt der sogenannte USB Device Tree Viewer. Den gibt's zum Gratis-Download. Nach dem Start erscheinen alle verfügbaren USB-Ports in einer Liste. Dabei gibt es wie gesagt oft Anschlüsse, die den neueren USB 3.x-Standard unterstützen, andere hingegen bieten nur die langsamere Geschwindigkeit von USB 2.0.

Die maximal mögliche Version und damit Geschwindigkeit für einen bestimmten Port lässt sich über die rechte Seite des Fensters von USB Device Tree Viewer abrufen. Hier findet sich die gesuche Info unter dem Bereich **Connection Information, Device Bus Speed**:

- Erscheint hier die Angabe Super-Speed, bezieht sich das auf USB 3.0.
- High-Speed steht für USB 2.0.
- Full-Speed zeigt an, dass es sich um einen sehr alten und damit lahmen USB 1.1-Anschluss handelt.



Digitalcourage kämpft gegen Staatstrojaner

Auch der Staat setzt Trojaner ein - die heißen dann Bundestrojaner oder Staatstrojaner. Einige Bürgerrechtler, Netzaktivisten und Journalisten setzen sich nun dafür ein, dass der Staat gar keine Staatstrojaner mehr verwenden darf. Gut - oder schlecht?

Der Verein Digitalcourage will gemeinsam mit anderen Bürgerrechtlern und Journalisten eine Klage vor dem Bundesverfassungsgericht einreichen. Polizei und Behörden setzen regelmäßig Trojaner ein. Die werden dann Staatstrojaner oder Bundestrojaner genannt.

Das Bundesverfassungsgericht soll die Rechtmäßigkeit prüfen und klare Grenzen ziehen, wann und wie der Staat Schnüffel-Software einsetzen darf. Den Klägern gehen die eingeräumten Rechte beim Bundestrojaner zu weit. Sie sehen rechtliche Probleme - und sorgen sich um die IT-Sicherheit ganz allgemein.

Hoher technischer Aufwand

Seit etwa einem Jahr gibt es ein Gesetz, das klar regelt, in welchen Situationen so ein Trojaner eingesetzt werden darf. Etwa, um akute Terrorgefahr abzuwehren oder schwerste Kriminalität zu bekämpfen. In solchen Fällen dürfen Polizei und Behörden gezielt Trojaner auf die Geräte von Verdächtigen aufbringen - um sie abzuhören oder relevante Daten abzugreifen.

Mir persönlich erscheint es logisch, dass der Staat diese Möglichkeit haben muss. Das ist zwar ein Eindringen in die Privatsphäre, aber in die von Menschen, die uns alle (höchstwahrscheinlich) bedrohen.

Gellinger / Pixabay[/caption]

Ein Problem wäre es, wenn Staatstrojaner nahezu beliebig oder häufig eingesetzt würden. Das BKA beteuert, das sei nicht der Fall. Und ich finde das glaubwürdig. Denn der technische Aufwand ist hoch, einen Staatstrojaner aufzubringen und die Daten auszuwerten.

Der Aufwand ist deshalb hoch, weil die Beamten genau wissen müssen, welches Gerät abgehört werden soll. Sie müssen das Betriebssystem kennen und die eingesetzte Software. Sie nutzen Sicherheitslücken aus, um den Trojaner an den Start zu bringen - so wie Kriminelle das auch machen.

https://soundcloud.com/user-999041145/so-funktionieren-staatstrojaner

Sicherheitsrisiko für uns alle

Und genau das ist der springende Punkt: Weil Staatstrojaner Sicherheitslecks benötigen (anders kriegt man sie nicht in die Geräte), hat der Staat kein vitales Interesse, solche Lecks zu stopfen (oder stopfen zu lassen, etwa, indem Hersteller verpflichtet werden, bekannt gewordene Lecks zu schließen). Im Gegenteil: Der Staat hat ein Interesse daran, die selbst genutzten Sicherheitslecks eben **nicht** zu schließen. Was Tür und Tor für andere Kriminelle öffnet.

Dieser Aspekt trifft zweifellos zu. Es wird interesant zu erfahren, wie die Verfassungsrichter urteilen: Sind Spähaktionen per Staatstrojaner eine "Verletzung der Menschenwürde", wie einige der Kläger argumentieren (was ich nicht denke, wenn wirklich sehr gezielt gespäht wird) - und muss der Staat nicht Sorge dafür tragen, dass Sicherheitslecks nach Bekanntwerden geschlossen werden?

[caption id="attachment_759322" align="alignnone" width="1030"]

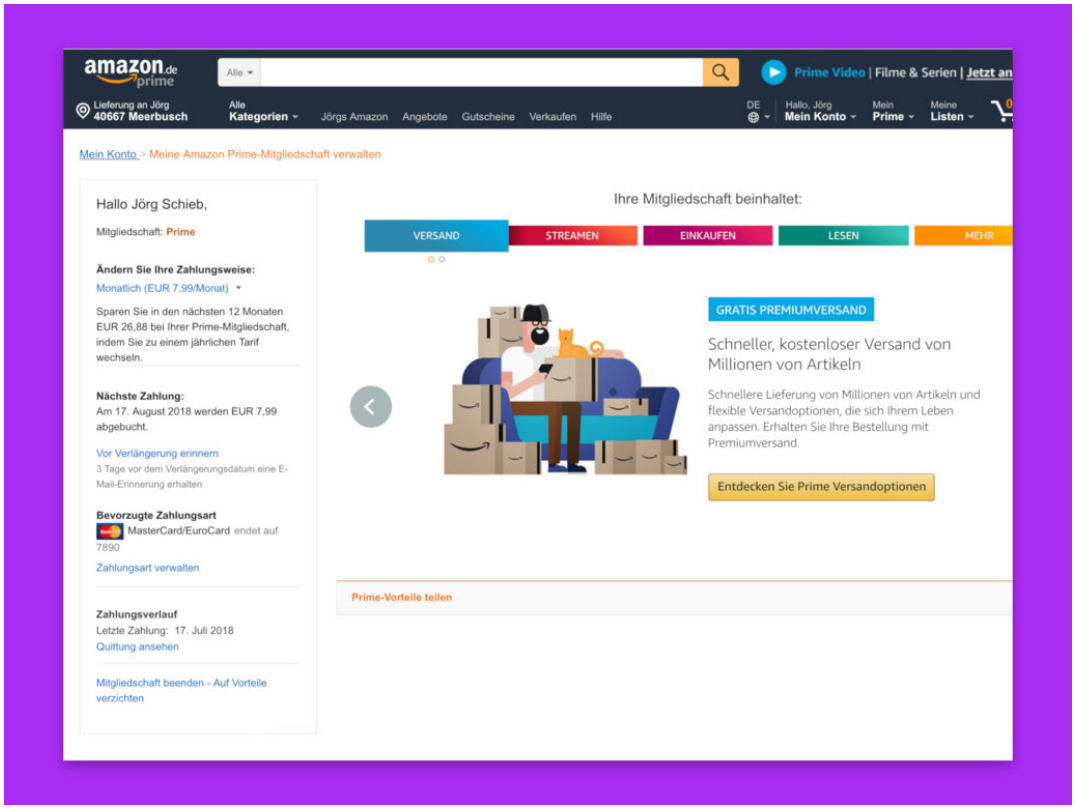
Amazon Prime: Abo-Details einsehen

Mit Amazon Prime können Viel-Besteller sich jede Menge Kosten für den Versand von Waren des Online-Händlers sparen. Abgeschlossen ist die Prime-Mitgliedschaft schnell – nur ein paar Daten eintragen, schon ist man fertig. Wer die Abo-Details aber im Nachhinein abrufen oder ändern will, muss die passende Seite erst suchen.

Die Details einer Amazon Prime-Mitgliedschaft lassen sich wie folgt einsehen und verändern:

1. Zunächst im Browser amazon.de aufrufen.
2. Jetzt folgt, falls nötig, oben rechts ein Klick auf **Anmelden**.
3. Nun rechts oben mit der Maus auf den Eintrag **Mein Prime** klicken.
4. Auf der erscheinenden Landing-Seite mit den Prime-Leistungen ganz nach unten scrollen.
5. Unterhalb des Kastens **Mehr Vorteile mit Prime** auf den Link **Meine Prime-Mitgliedschaft verwalten** klicken.

In der Spalte auf der linken Seite erscheinen jetzt die Abo-Details, unter anderem mit der Angabe, ob es sich um ein monatliches oder ein Jahres-Abo handelt, sowie mit der Info, mit welchem Zahlungsmittel Amazon Prime bezahlt wird. Schließlich steht ganz unten auch die Option bereit, das Prime-Abo zu beenden.



HEIF/HEVC: Das steckt hinter dem neuen Bildformat auf dem iPhone

Wer sein iPhone viel zum Filmen und Fotografieren nutzt, wird vielleicht schon mal über die Abkürzungen HEIF oder HEVC gestolpert sein. Das neue Bildformat bietet einige Vor-, aber auch verschiedene Nachteile.

Fotos und Videos nehmen auf dem iPhone schnell viel Speicherplatz ein. Zum Glück entwickeln sich aber nicht nur Smartphones und Kameras rasant weiter, sondern auch Dateiformate. Wer seinen Speicher etwas schonen will, hat seit iOS 11 die Möglichkeit, auf das Format HEIF für Fotos oder HEVC für Videos zu wechseln.

HEIF / HEVC steht für "**High-Efficiency Image Formate** bzw. **High Efficiency Video Coding"**.

Im Gegensatz zum altbekannten JPEG, werden HEIF-Fotos bis zu **50% effizienter komprimiert,** ohne dabei an Bildqualität zu verlieren. Auch das Videoformat MPEG-4 (auch bekannt als H.264) hat mit H.265 einen verbesserten Videocodec erhalten, der es ermöglicht Speicherplatz zu sparen, ohne Qualität einzubüßen.

Mehr Speicherplatz auf Kosten von Kompatibilität

HEIF und HEVC klingen erstmal nach einer sinnvollen Einstellung. Sollte man also immer auf das neue Bildformat setzen und JPEG und MP4 komplett ignorieren?

Nur bedingt, denn HEIF/HEVC werden längst nicht von allen Programmen unterstützt. Wer also sichergehen will, dass seine Bilder und Videos vom iPhone auf jeden Fall auch auf anderen Geräten wiedergegeben werden können, sollte doch zum unkomprimierten Format greifen.

Wer seine Fotos ohnehin nur auf iPhone oder iPad abspielt und Speicher sparen will, kann bedenkenlos zu HEIF und HEVC greifen. Außerdem sollte es nicht allzu lange dauern, bis die Formate auch mit anderer Software kompatibel sind.

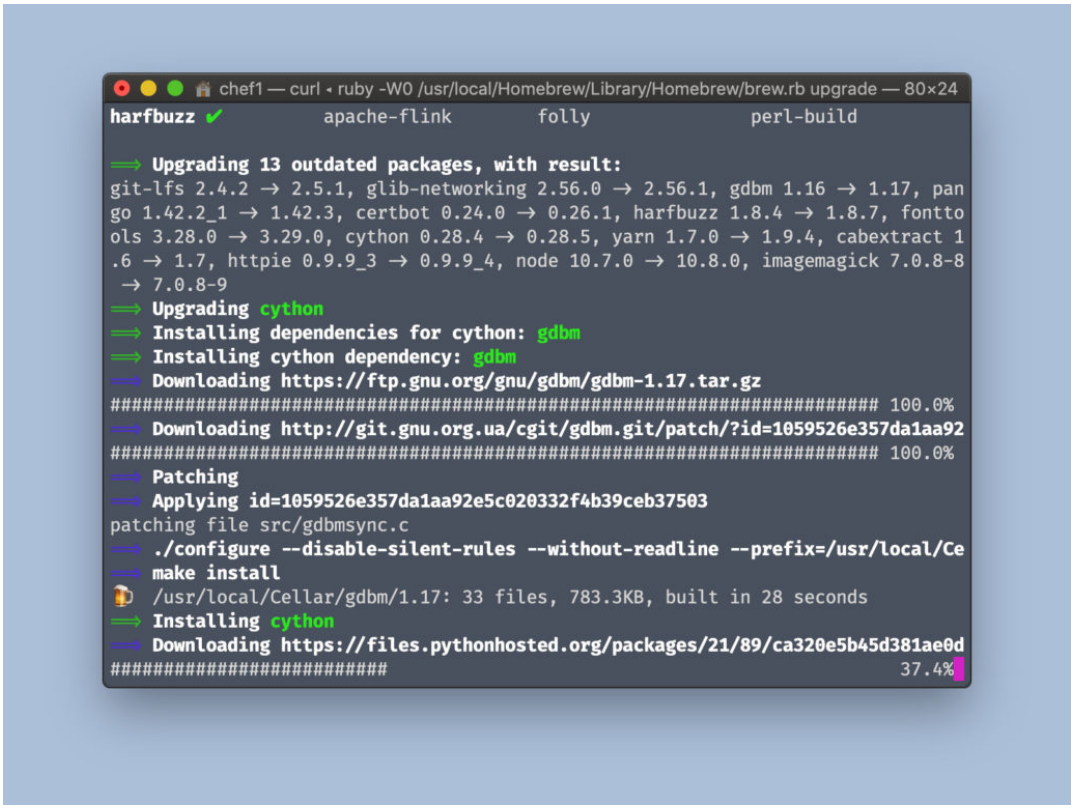
Homebrew: Nur ein Paket updaten

Unix-Nutzer schätzen die einfache Aktualisierung von Programmen über einen Paket-Manager. Mit Homebrew gibt es ein ähnliches System auch für macOS. Das Problem: Installiert man Updates, werden alle Pakete auf einmal auf den neuesten Stand gebracht. Braucht man nur das Update für ein einzelnes Programm, hilft ein Trick weiter.

Um mit Homebrew nur ein einzelnes Paket zu updaten, geht man wie folgt vor:

1. Zunächst ein neues Fenster des Terminals öffnen – etwa per Spotlight-Suche.
2. Jetzt den Befehl **brew update** eintippen. Dadurch werden alle neuen Pakete geladen.
3. Mithilfe des Kommandos **brew upgrade paketname** [Enter] lässt sich das gewünschte Paket jetzt gezielt auf den neuesten Stand bringen.

Tipp: Wer herausfinden möchte, welche Pakete installiert sind, tippt einfach den Befehl **brew list** ein. Diese Liste lässt sich bei Bedarf auch nach einzelnen Paketen filtern – nach dem Schema **brew list | grep paketname**.

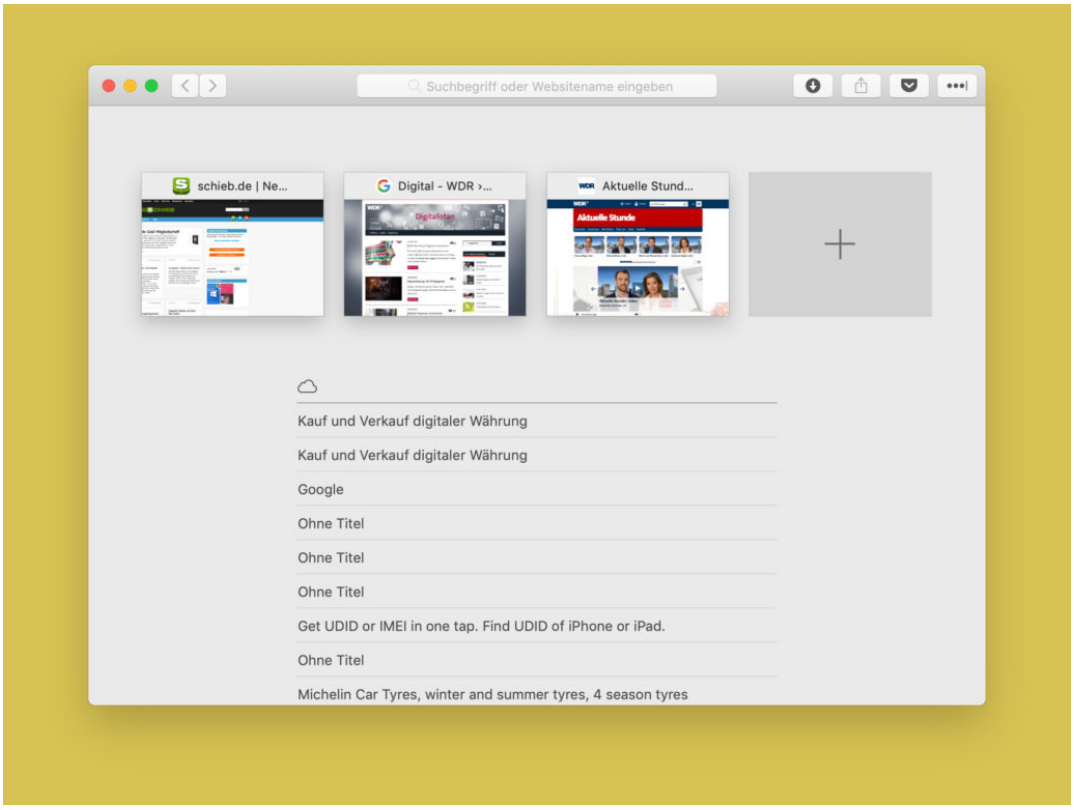


Übersicht über offene Safari-Tabs

Wer viele Webseiten gleichzeitig geöffnet hat, verliert schnell den Überblick. Denn anhand der Seiten-Titel auf den einzelnen Tabs sind manchmal kaum Rückschlüsse auf den Inhalt möglich. Einfacher wird’s mit der Tab-Vorschau des Safari-Browsers.

Die Übersicht über sämtliche offenen Website-Registerkarten in Safari lässt sich mit einer einfachen Geste auf dem Trackpad des MacBooks aufrufen. Wir zeigen, wie das geht:

1. Zunächst Safari starten, etwa per Klick auf das Symbol des Programms unten im Dock des Macs.
2. Jetzt ein paar Webseiten in Tabs laden.
3. Nun zwei Finger auf dem Trackpad aufeinander zu bewegen, was einer Zoom-Out-Geste entspricht.
4. Nach einem Augenblick wird die aktuell im Vordergrund offene Webseite so verkleinert, dass sie neben den anderen geöffneten Tabs als Vorschau bzw. Miniatur-Ansicht dargestellt wird.
5. Ein Klick auf ein beliebiges dieser Thumbnails bewirkt, dass der Safari-Browser die zugehörige Webseite mit ihrem Tab in den Vordergrund holt.



Doppelte Dateien auf dem Mac finden

Festplattenspeicher will gut genutzt werden. Besonders doppelt vorhandene Dateien sollte man da auf jeden Fall vermeiden, um den wertvollen Speicherplatz nicht an Karteileichen zu verschwenden.

Es ist auf jeden Fall immer gut, von sehr wichtigen Dateien ein Backup oder eine Kopie zu haben. Unnötige doppelte Dateien will hingegen niemand auf dem Computer haben.

Wer den Überblick über seine Dateien verloren hat, kann beispielsweise das Tool **Duplicate File Finder Remover** nutzen, um doppelte Dateien und Ordner auf der Festplatte zu finden und anschließend zu löschen.

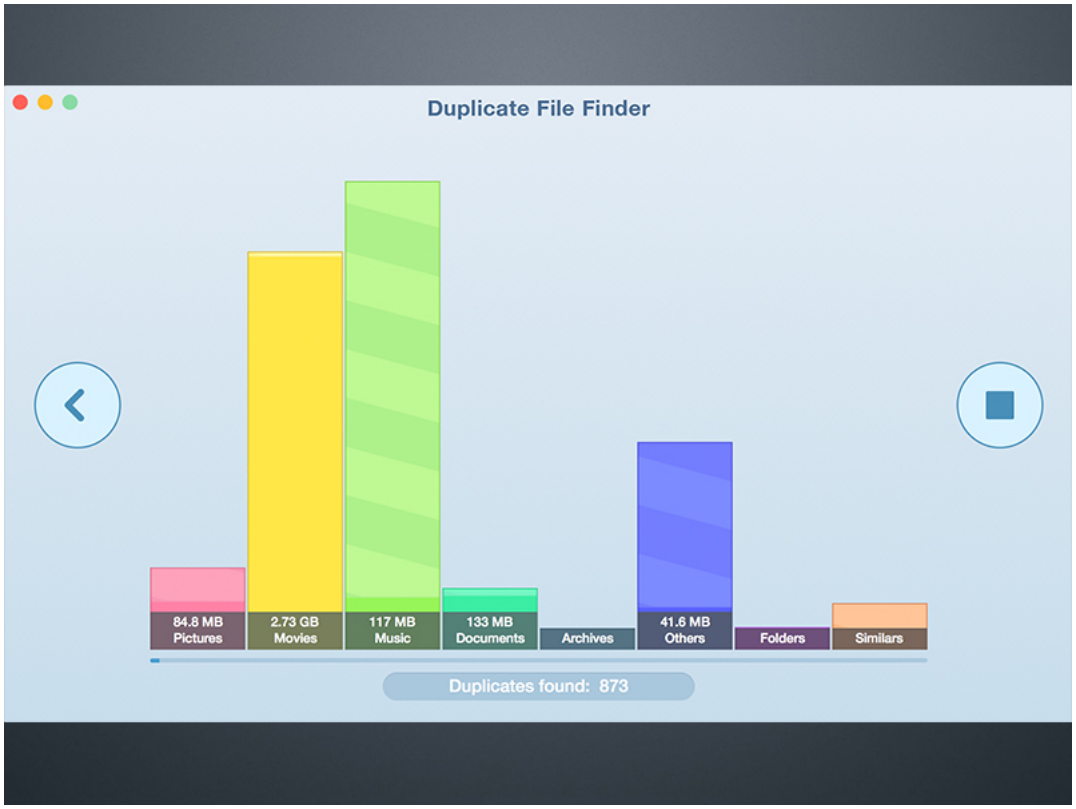
Ist das Programm aus dem App Store installiert, kann es auch direkt losgehen. Wer seine **komplette Festplatte** nach Duplikaten scannen will, kann das über einen Klick auf **Scan Home Folder** tun. Das Programm sucht anschließend nach Dateien auf der Festplatte, die denselben Dateityp und Dateinamen aufweisen.

In einer Übersicht werden nun alle gängigen Dateitypen (Dokumente, Videos, Bilder, Musik, etc.) aufgelistet, von denen Duplikate gefunden wurden. Außerdem wird hier direkt angegeben, wie viel Speicherplatz die doppelten Dateien einnehmen und in welchem Ordner sie sich genau befinden.

Software leistet auch kostenlos sehr gute Dienste

Einige der Funktionen, wie das Löschen der doppelten Dateien über das Programm, sind leider nur in der kostenpflichtigen Pro-Version verfügbar. Trotzdem macht auch die kostenlose Software einen sehr guten Job beim Finden der Dateien. Da die Dateipfade direkt angegeben werden, kann man also einfach direkt in den entsprechenden Ordner gehen, um die Dateien manuell zu löschen.

Ist nur ein Schritt mehr und kostenlos. Ein weiteres sehr nützliches Feature: Anstatt die komplette Festplatte zu scannen, lassen sich auch spezifische Ordner festlegen, in denen nach Duplikaten gesucht werden soll. Da spart einiges an Zeit und ist viel präziser, als eine allumfassende Suche.



Fotos vom Handy übertragen

Wer auf dem Handy viele Fotos oder andere Dateien gespeichert hat und diese ohne Zeitverlust auf den Computer kopieren will, hat dazu verschiedene Möglichkeiten. Das Problem: Soll die Übertragung per WLAN oder Kabel stattfinden, geht das oft nur lahm vonstatten. Da gibt es eine einfachere Lösung.

Die praktischste Methode nutzt einfach den sogenannten USB On The Go-Modus. Unterstützt ein USB-Stick diesen Modus, lässt er sich direkt – etwa über einen Micro-USB-Anschluss – mit dem Smartphone verbinden. Danach können über die Datei-App des mobilen Geräts Dateien und Ordner vom internen Speicher auf das USB-Laufwerk kopiert oder verschoben werden.

Eine Alternative zu diesen On The Go-Sticks ist ein sogenanntes On The Go-Kabel. Es sieht aus wie eine USB-Verlängerung – das eine Ende kommt in den Anschluss des Handys, ans andere Ende lässt sich ein ganz normaler USB-Stick oder eine Festplatte anschließen. Dabei aber auf das Dateisystem achten. Denn mobile Geräte unterstützen oft nur das FAT-, nicht aber das NTFS-Dateisystem, das bei Windows-Datenträgern oft zum Einsatz kommt.

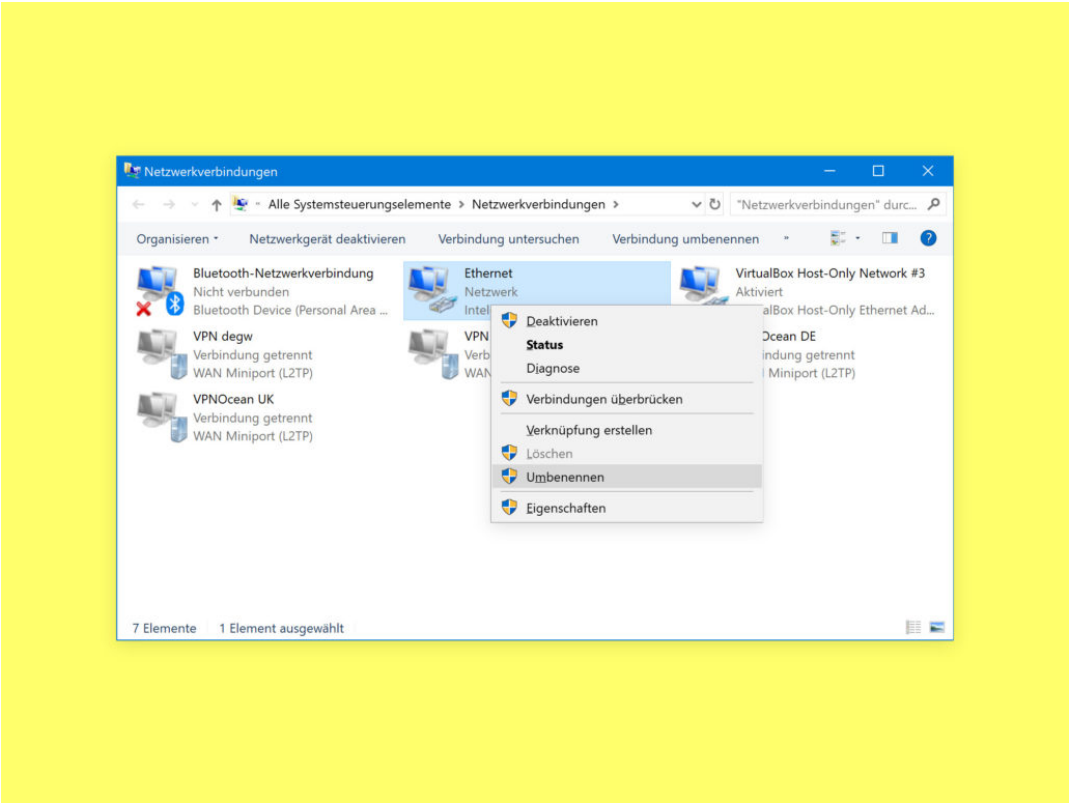
Netzwerke umbenennen

Verbindungen zu Netzwerken bekommen in Windows automatisch Namen zugewiesen – „Ethernet 1“, „WLAN 3“ und so weiter. Kein Wunder, dass man hier nicht wirklich Durchblick bekommt. Besser, man vergibt für die Netzwerk-Interfaces sprechende Namen.

Um Netzwerke in Windows einen verständlicheren Namen zu geben, geht man wie folgt vor:

1. Zuerst gleichzeitig die Tasten [Windows]+[R] drücken.
2. Jetzt den Befehl **ncpa.cpl** eintippen und mit Klick auf **OK** bestätigen.
3. Nun kann die betreffende Verbindung, die einen neuen Namen erhalten soll, mit der rechten Maustaste angeklickt werden.
4. Hier findet sich der gesuchte **Umbenennen**-Befehl.

Tipp: Auf die gleiche Weise lassen sich nicht nur Ethernet-, also kabelgebundene Netzwerk-Verbindungen mit einem neuen Namen ausstatten, sondern auch WLAN-Verbindungen.

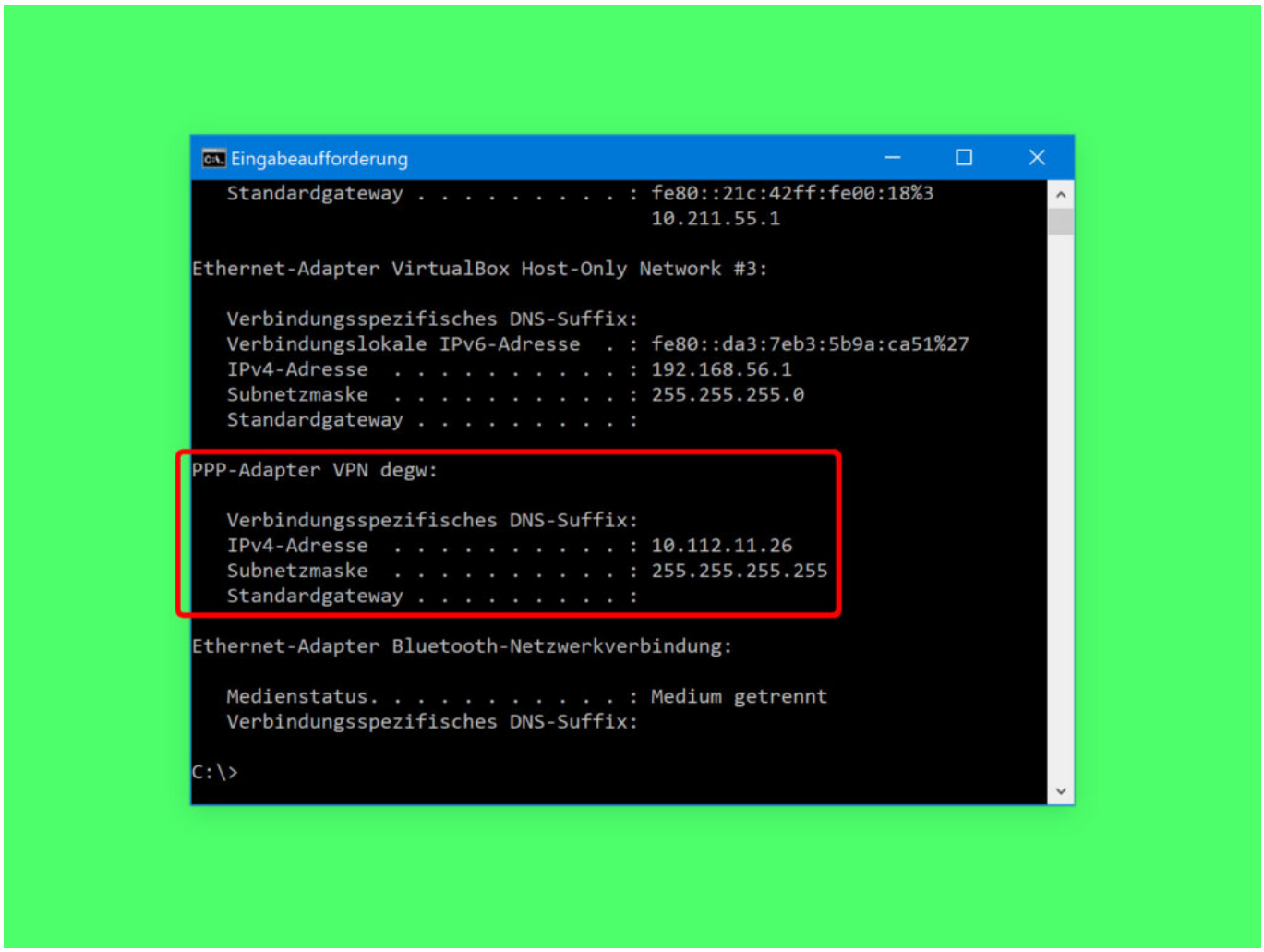


IP-Adresse einer VPN-Verbindung

Wer auch in offenen WLANs geschützt unterwegs sein oder auf Firmen-Ressourcen zugreifen will, braucht eine VPN-Verbindung, also einen sicheren Tunnel. Innerhalb dieses Tunnels erhält der Nutzer auch eine eigene IP-Adresse, die ihn im Intranet kennzeichnet. Welche das ist, lässt sich leicht nachsehen.

Linux- und Mac-Nutzer können die IP-Adresse der VPN-Verbindung über das Terminal einsehen – einfach ein neues Konsolen-Fenster öffnen und hier den Befehl **ifconfig** eintippen. Unter den verschiedenen Netzwerk-Schnittstellen erscheint auch eine, die sich auf das PPP-Protokoll bezieht. Im Beispiel ist das **ppp0** – darunter wird die zugehörige IP-Adresse angegeben und lässt sich ablesen.

In Windows geht das ähnlich einfach: Zunächst eine Verbindung zu dem betreffenden VPN-Netzwerk herstellen. Dann ein neues Fenster der Eingabe-Aufforderung öffnen, etwa, indem zuerst auf den Start-Button geklickt, dann **cmd** getippt und auf das erste Resultat geklickt wird. Nun den Befehl **ipconfig** („ip“, nicht „if“) eintippen und mit Druck auf [Enter] bestätigen. Auch hier wird ein Eintrag für die IP-Konfiguration der PPP-Verbindung sichtbar.

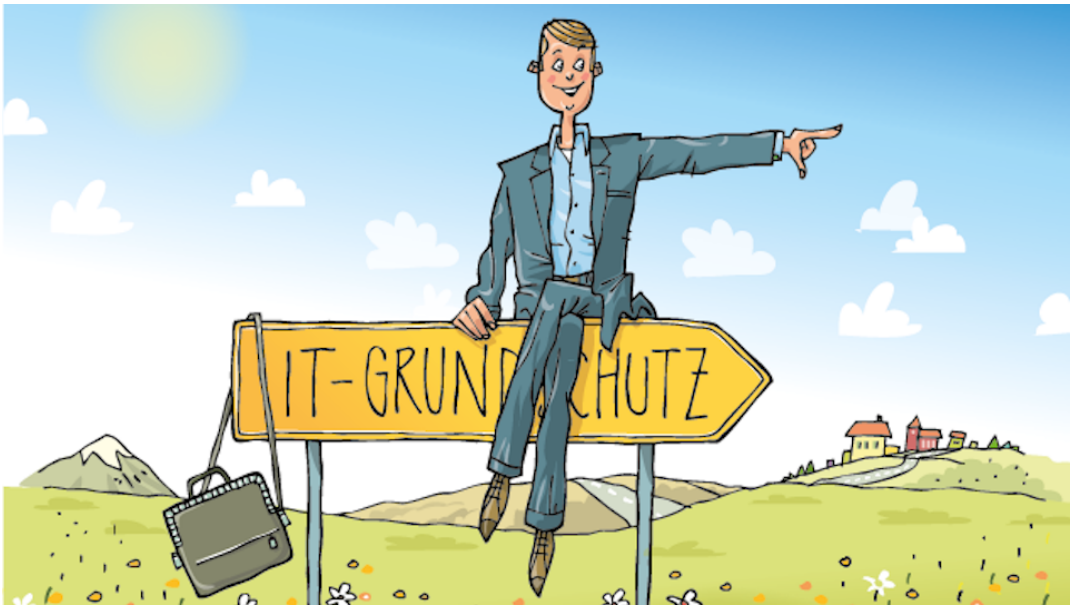

Eingabeaufforderung
Standardgateway . . . . . : fe80::21c:42ff:fe00:18%3
10.211.55.1
Ethernet-Adapter VirtualBox Host-Only Network #3:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::da3:7eb3:5b9a:ca51%27
IPv4-Adresse . . . . . : 192.168.56.1
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . :
PPP-Adapter VPN degw:
Verbindungsspezifisches DNS-Suffix:
IPv4-Adresse . . . . . : 10.112.11.26
Subnetzmaske . . . . . : 255.255.255.255
Standardgateway . . . . . :
Ethernet-Adapter Bluetooth-Netzwerkverbindung:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
C:\>

BSI mit eigenem Online-Kurs: Fit fürs Netz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) müht sich redlich, die Öffentlichkeit in Sachen IT-Sicherheit aufzuklären. Für Behörden ist das BSI erste Anlaufstelle. Jetzt hat die Behörde einen durchaus empfehlenswerten Online-Kurs auf den Weg gebracht, der wichtiges Know-how anschaulich vermittelt.

Es vergeht kein Tag, an dem nicht neue Sicherheitsrisiken bekannt werden: Eine Sicherheitslücke hier, ein Bug (Fehler) dort, eine neue Schwachstelle ganz woanders. Software ist nun mal fehleranfällig - und wir setzen heute überall Software ein. Im PC, im Tablet, im Smartphone, in der Smartwatch, im Auto, im Digitalen Assistenten, im Küchengerät ...

Das erhöht das Risiko, über solche Sicherheitslücken zu stolpern. Es ist nicht das Internet an sich, das uns all die Probleme bringt, es sind die vielen Programmier- und Denkfehler, die sich in den Programmen verbergen.



Kostenloses Online-Seminar

Deshalb ist es wichtig, einige Regeln zu beachten - das gilt vor allem in Unternehmen, Institutionen und Behörden. Es nutzt aber nichts, wenn nur die IT-Experten im Haus die Regeln kennen. Idealerweise wissen alle, was zu beachten ist. Wie sich Hackangriffe vermeiden lassen und Phishing-Angriffe ins Leere laufen. Kurz: Wie ein IT-System, wie Hard- und Software idealerweise genutzt und eingestellt werden, um Sicherheitsrisiken einzudämmen.

Da empfehle ich den neuen Online-Kurs des BSI (Bundesamt für Sicherheit in der Informationstechnik): Hier lernt man in einem gut gemachten, kostenlosen Seminar die Sicherheitsempfehlungen der IT-Experten aus dem BSI kennen.

Ihr könnt Euch damit vertraut machen und daraus ziehen, was für Euch nützlich ist. Ein

gelungener Kurs, in den jeder mal die Nase stecken sollte. Ihr erfahrt zum Beispiel, wie Ihr einen IT-Grundschutz-Check durchführt. Schön, dass das BSI dem Kurs auch auflockernde Illustrationen und Cartoons spendiert hat.

https://soundcloud.com/user-999041145/so-funktionieren-staatstrojaner

Trojaner nutzen Sicherheitslücken aus

Schlau machen schützt besser als jede Firewall

Am Ende jeder Lerneinheit gibt es Prüfungsfragen. Wer nicht so auf Online-Seminare steht, kann auch alles als PDF herunterladen. Schwerpunkt des Online-Kurses ist die Anwendung in Wirtschaft und Verwaltung. Wem das zu dröge ist, kann auch auf andere Weise einsteigen. Die Redaktion vom Internet ABC zum Beispiel bietet Eltern, Lehrern und Großeltern einen guten Infobereich, in dem sich Besucher mit den Basics der Internetwelt vertraut machen und auch einiges über Risiken und Gefahrenabwehr lernen können.

Sich selbst fit zu machen hilft mehr, als jede Schutz-Software oder Firewall!

So funktioniert die Verwaltung im Online-Shop reibungslos

Auch in einem Online-Shop fallen zahlreiche betriebswirtschaftliche Prozesse und administrative Aufgaben an, die es zu bewältigen gilt. Denn hat sich ein solcher erst einmal auf dem Markt etabliert, so gehen jeden Tag zahlreiche Bestellungen ein, die bearbeitet werden müssen. Spätestens dann, wenn der Web-Shop viele Kunden oder zahlreiche verschiedene Produkte im Sortiment hat, wird es kompliziert. Wer dann nicht auf computergestützte Hilfe setzt, der verliert schnell den Überblick.

Wer als Online-Shop-Betreiber zufriedene Kunden haben möchte, der sollte vor allem auf schnelle Lieferung setzen. Denn nur so kann ein Web-Shop der Konkurrenz standhalten. Dafür ist es jedoch essentiell, dass alle Waren immer ausreichend vorrätig sind.

[caption id="attachment_759373" align="alignnone" width="500"]


Free-Photos / Pixabay[/caption]

Übersichtliche Warenwirtschaft

Hat man nur eine kleine Produktpalette und wenig Kunden, so mag das zu Beginn auch ohne ein entsprechendes Programm möglich sein. Doch spätestens, wenn der Kundenstamm wächst oder sich die Produktpalette erweitert, ist es ohne computergestützte Hilfe kaum noch möglich, den Überblick zu behalten.

Dann kann ein professionelles Wawi-System für eine übersichtliche Warenwirtschaft sorgen. Denn dieses zeigt an, wenn Waren zuneige gehen und nachbestellt werden müssen. Damit

sind Lieferengpässe und unzufriedene Kunden passé. Daneben kann ein Shop-Betreiber ebenfalls mithilfe des Systems seine Bestellungen verwalten.

Selbst diejenigen, die auf mehreren Plattformen ihre Waren verkaufen, behalten mit einer solchen Lösung den Überblick. Denn über ein Warenwirtschaftssystem lassen sich sämtliche Bestellungen abrufen und bearbeiten. So erhält jeder Kunde seine bestellte Ware zeitnah und vollständig.

[caption id="attachment_759374" align="alignnone" width="500"]

TheDigitalArtist / Pixabay[/caption]

Lieferscheine und Rechnungen einfach erstellen

Zu den täglichen Aufgaben eines Online-Shop-Betreibers zählt nicht nur das Versenden der georderten Waren, sondern ebenfalls das Erstellen von Lieferscheinen und Rechnungen. Zwar ist es nicht Pflicht, einen Lieferschein im Paket beizulegen, jedoch ist dies für beide Seiten

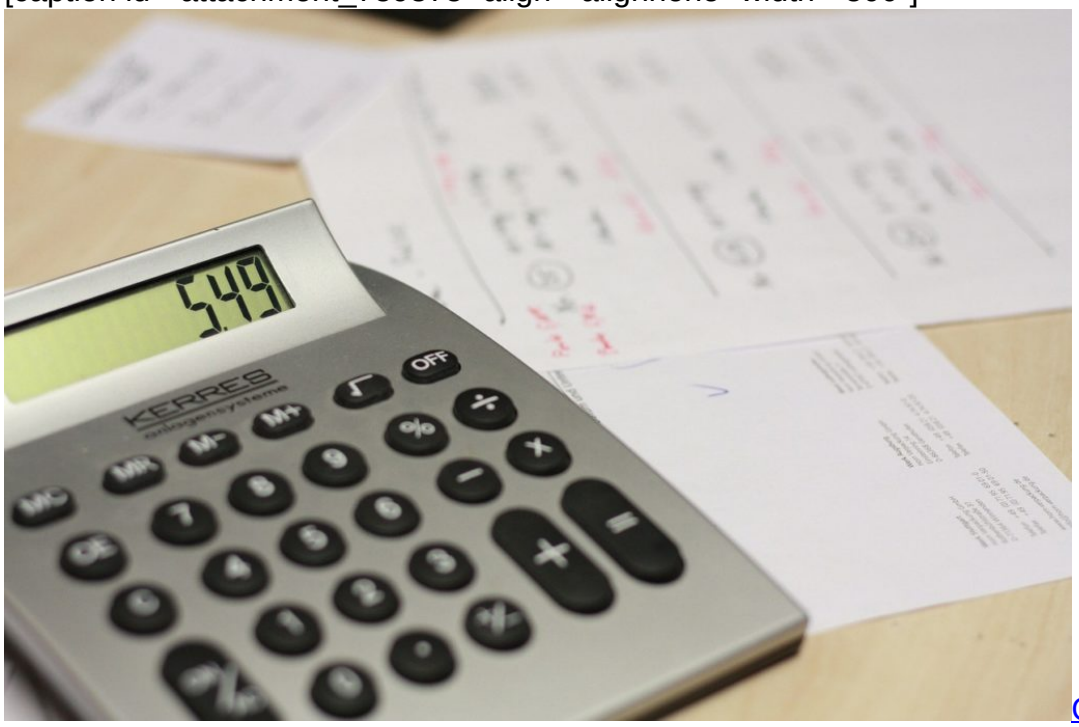
nützlich. Durch die Auflistung der gelieferten Produkte ist eine bessere Übersichtlichkeit gewährleistet.

Denn ein Lieferschein erleichtert es dem Kunden, die Sendung auf Vollständigkeit zu überprüfen. Ist eines der georderten Produkte erst zu einem späteren Zeitpunkt lieferbar, so kann das ebenfalls auf dem Schein vermerkt werden. Wer ein Muster für den Lieferschein als Vorlage verwendet, der spart zusätzlich Zeit. Dank diesem ist er im Handumdrehen erstellt.

Das Schreiben von Rechnungen ist eine weitere Aufgabe, die Online-Shop-Betreiber erledigen müssen. Diese müssen gesetzlichen Richtlinien entsprechen und folgende Aspekte beinhalten:

- Rechnungsdatum
- Spätestes Zahlungsdatum
- Name und Adresse des Rechnungsstellers
- Name und Adresse des Rechnungsempfängers
- Rechnungsnummer
- Produktumfang
- Auslieferungsdatum
- Netto-Betrag
- Umsatzsteuer

Auch für dies Erstellung von Rechnungen gibt es spezielle Vorlagen, dank denen keine wichtigen Angaben vergessen werden.

[caption id="attachment_759375" align="alignnone" width="500"]


Cobanams / Pixabay[/caption]

Saubere Buchführung

Weiterhin ist jeder Selbstständige dazu verpflichtet, Bücher zu führen. Wer teure Nachzahlungen vermeiden möchte, der sollte alle Geschäftsvorfälle sauber auflisten. Dies ist nicht nur wichtig für die Vorlage bei der Finanzbehörde, sondern hilft dem Online-Shop-Betreiber ebenfalls, einen Überblick über seine Finanzen zu behalten.

Zwar ist es möglich, diese Aufgabe an einen Buchhalter oder Steuerberater auszulagern, jedoch können sich das vor allem kleinere Shops oftmals nicht leisten. Doch mithilfe einer professionellen Software ist es auch für diejenigen mit wenig Erfahrung in diesem Bereich kein Problem, selbst Bücher zu führen.

Damit sich nicht am Ende des Geschäftsjahres ein riesiger Berg an Belegen angehäuft hat, ist es ratsam, diese Arbeit regelmäßig zu erledigen. So behält man den Überblick und kann bei möglichen Problem direkt reagieren.

EuGH: Auch Schüler dürfen sich nicht frei im Internet bedienen

Der Europäische Gerichtshof musste entscheiden, ob für Schulen und Schüler "entspanntere" Regeln beim Urheberrecht gelten. Nein, es gelten dieselben (strengen) Regeln haben die Richter des EuGH entschieden. Damit ist klar: Es muss etwas passieren, damit das Internet als Recherchemedium an Schulen gefahrlos genutzt werden kann - und die Rechteinhaber gleichzeitig nicht leer ausgehen.

Der vom EuGH verhandelte Fall ist quasi ein Klassiker und eignet sich meiner Meinung daher perfekt für eine Verhandlung vor dem Europäischen Gerichtshof (EuGH): Eine Schülerin findet im Internet ein Foto der spanischen Stadt Córdoba und fügt diese Aufnahme (sogar unter Angabe der Quelle) in ihr Referat ein.

Später erscheint die Arbeit samt Foto auf der Webseite der Schule (Gesamtschule Waltrop). Der Berufsfotograf, der das Foto gemacht hat, klagt nicht nur auf Unterlassung und Schadenersatz, weil seine Urheberrechte verletzt wurden, sondern berechnet der Schule auch noch die üblichen Anwaltsgebühren. Ein (leider) ziemlich alltäglicher Vorgang.

Schüler nutzen das Internet - achten aber nicht immer das Urheberrecht

Europaweite Regelung wäre am besten

Der Bundesgerichtshof hat den Fall bereits verhandelt und ihn nun dem EuGH vorgelegt. Das ist gut so, denn solche Fälle regelt man am besten europaweit einheitlich. Klar, streng

genommen hat die Schülerin die Urheberrechte verletzt - spätestens, als das Foto auch auf der Webseite erschienen ist. Nur: Wie herzlos muss man sein, eine Schule/Schülerin zu verklagen, anstatt froh und stolz zu sein, dass die eigene Arbeit dort wahrgenommen wird und zu sehen ist? Oder einfach darum zu bitten, das Foto wieder zu entfernen...

Doch das ist eine Charakterfrage und keine juristische. Der Jurist will wissen: Was geht und was geht nicht. Fakt ist: Schulen in Europa sind chronisch klamm. Das ist zweifellos ein politisches Armutszeugnis. Niemand käme aber auf die Idee zu verlangen, dass Stuhlhersteller Schulen ihre Stühle kostenlos zur Verfügung stellen oder dass Lehrer kostenlos unterrichten. Also sollten auch Urheber nicht leer ausgehen, wenn ihre Arbeit in Schulen genutzt wird. Jedenfalls nicht grundsätzlich. Allerdings sollten auch keine Honorare wie in der Wirtschaft erwartet werden.

[caption id="attachment_759334" align="alignnone" width="500"]

jarmoluk / Pixabay[/caption]

Befreit die Schulen - und bezahlt die Rechteinhaber

Es gibt nun den Vorschlag, Schulen generell von der Verpflichtung freizustellen. Sie sollen beim Gebrauch von Texten, Videos, Fotos etc. keine Lizenz bezahlen müssen. Das geht in die richtige Richtung, denke ich. Besser und richtig fände ich allerdings, wenn für die Schulen in eine Art europäischen Kulturtopf eingezahlt wird - von den Staaten, selbstverständlich. Das Geld wird fair auf die Rechteinhaber verteilt (Autoren, Musiker, Fotografen). Dafür dürfen sich die Schulen frei bedienen - und müssen keine juristischen Konsequenzen befürchten. So hätten alle etwas davon.

Der Europäische Gerichtshof (EuGH) hat anders entschieden (hier das Urteil): Es gibt keine Ausnahmen beim Urheberrecht - auch nicht für Schulen. Daher ist vorher um Erlaubnis zu fragen und ggf. eine Lizenz zu zahlen. Das Gericht hat juristisch konsequent entschieden. Jetzt sollte die Politik ran - und das Recht neu regeln. Schließlich möchte man medienkompetente Kinder haben. Das Urheberrecht neu regeln, bitte!

Was sollten Bildbearbeitungsprogramme heute können?

Bilder sind heute omnipräsent. Egal ob in Printmedien, Internetzeitungen oder in Chats: überall Bilder. Von Fotos und der Interaktion mit Bildern leben vor allem die sozialen Netzwerke. Hier werden täglich Millionen Bilder hochgeladen, getauscht oder geliked.

Wie stark die Bildernutzung inzwischen in die Gesellschaft vorgedrungen ist, zeigen Statistiken zu Instagram. Laut Brandwatch teilen die Nutzer der Plattform jeden Tag etwa 80 Millionen Fotos/Bilder. Kein Wunder, dass inzwischen mehr als 40 Milliarden Bilder auf Instagram geteilt wurden. Fotos landen in den sozialen Medien häufig als Schnappschuss.

Ungestellt und ungeschminkt zeigen die Fotos, was Nutzern gerade gefällt oder sie beeindruckt. Einige Bilder fallen allerdings in eine etwas andere Kategorie. Extrem lebende Farben, schier unglaubliche Lichteffekte und Schattenspiele oder herausragende Kontraste begeistern. Die Bilder scheinen aus einer anderen Welt zu stammen.

Oft trifft dies sogar zu. Es handelt sich zwar um Fotos, die eine reale Situation eingefangen haben. Ein Teil der Atmosphäre ist allerdings im Rechner entstanden – mithilfe eines professionellen Bearbeitungstools.

Bildbearbeitung ist längst nicht mehr nur Profis und absoluten Cracks hinter der Kamera vorbehalten. Gerade der Open Source Gedanke hat in den letzten Jahren auch Hobbyfotografen einige sehr leistungsfähige Werkzeuge mit an die Hand gegeben.

Abbildung 1: Heute lassen sich tolle Effekte auf Bilder legen – mit der richtigen Software kein Problem

Bildbearbeitung versus Bildoptimierung

Was ist Bildbearbeitung? Vereinfacht ausgedrückt handelt es sich hier um die Veränderung von Bildinhalten. Einfaches Beispiel: Beim Fotografieren mit Blitzlicht entsteht bei einer Achsengleichheit von Objektiv und Blitz der sogenannte Rote Augen Effekt. Mithilfe einer Bildbearbeitung kann dieser Aufnahmefehler auf Knopfdruck korrigiert werden. Aber: Es gibt einen Unterschied zwischen der Bildbearbeitung und der Bild-/Fotooptimierung.

Die Bildbearbeitung wie sie heute von der breiten Masse wahrgenommen wird, umfasst nicht nur die Korrektur von Aufnahme- oder Objektivfehlern. Moderne Programme sind in der Lage, durch die Arbeit mit mehreren Bildebenen, ein Foto komplett zu verändern – indem Bildinhalte gelöscht werden oder neu hinzukommen. Digitale Fotoentwicklung orientiert sich in eine etwas andere Richtung. Verändert werden unter anderem:

- Schärfe
- Helligkeit
- Kontrast
- Farbtemperatur

Weitergehende Bearbeitungswerkzeuge fehlen bei vielen reinen Entwicklungsprogrammen. Aber: In diesem Segment ist die Palette durchaus fließend. Achtung: In der digitalen Fotoentwicklung arbeiten Profis und versierte Hobbyfotografen häufig mit sogenannten Rohdaten. Letztere sind mit dem Negativ der klassischen Fotografie vergleichbar. Bilder im Rohdaten-Format erlauben eine erhebliche Bandbreite an Entwicklungsmöglichkeiten. Für eine Bildbearbeitung müssen Fotos im Regelfall aber erst in ein passendes Format umgewandelt werden.

Standard-Funktionen in der Bildbearbeitung

Software zur Bildbearbeitung bringt viele Funktionen mit. Einige Features sollten in jedem Fall dabei sein. Die Korrektur des Rote-Augen-Effekts gehört dazu. Gerade bei Aufnahmen unter ungünstigen Lichtverhältnissen kann es durch hohe ISO-Werte zu unschönem Rauschen kommen. Um diesen Effekt zu eliminieren, ist auf die Rauschreduzierung als Funktion zu achten.

Darüber hinaus sind Funktionen wie:

- Beschneiden
- Kontrastveränderungen
- Helligkeitsanpassungen

wichtige Elemente, die in jedem Fall zur Grundausstattung zählen. Auch die Sättigung sollte anpassbar sein. In der Praxis ist bei der Bildbearbeitung auch der Arbeitsschritt des Neuausrichtens von Vorteil. In der Eile „des Gefechts“ kann der Horizont schnell schief aufgenommen werden.

[caption id="attachment_759305" align="alignnone" width="500"]

geralt / Pixabay[/caption]

Im Hinblick auf die Veränderungen der Farben werden Einsteiger schnell feststellen, dass es zwischen:

- Luminanz
- Sättigung

für die einzelnen Farbtöne signifikante (und auch überraschende) Unterschiede gibt. Und dass sich mit diesem Wissen im Hinterkopf einige beeindruckende Effekte erzeugen lassen. Ein ebenfalls sehr wichtiges Tool im Fundus der Bildbearbeitung sind Freihand- und Lasso Werkzeug, die als Auswahlwerkzeug für spätere Funktionen sehr nützlich sind.

Weitergehende Funktionen in der Bildbearbeitung

Das ganze Bild ein wenig schärfen und rote Augen entfernen – Einsteiger werden diese Funktionen recht schnell beherrschen. Wer etwas tiefer in die Bildbearbeitung eintaucht stößt sehr schnell auf Funktionen wie das Freistellen von Objekten und die Arbeit in mehreren Ebenen. Beim Freistellen werden einzelne Objekte markiert und können anschließen ausgeschnitten und verschoben oder separat bearbeitet werden.

Ein sehr starkes Tool für die fortgeschrittene Bearbeitung ist die Verwendung der Bildebenen. Auf diese Weise können Bilder so optimiert werden, dass störende Elemente nicht mehr im Endergebnis auftauchen.

Nützlich – Anfängern aber nicht unbedingt bekannt – sind die Retuschefunktionen, mit denen sich ganze Bildelemente verschwinden lassen, ohne im fertigen Bild Spuren zu hinterlassen.

[caption id="attachment_759306" align="alignnone" width="500"]


realworkhard / Pixabay[/caption]

Was kostet solche Software heute?

Software wie Adobe Photoshop ist im Bereich der Bildbearbeitung führend – was die Entwicklung neuer Standards und Funktionen angeht. Aus diesem Grund sind solche Tools das Handwerkzeugs der Fotoprofis – und kosten entsprechend Geld. Eine Profi-Suite kann in der Bildbearbeitung (mit allen erdenklichen Modulen) schnell einige hundert Euro kosten. Foto- und Grafikstudios werden mitunter sogar mit einer vierstelligen Summe zu rechnen haben. Für den privaten Anwender sind solche Preise für die Softwarelizenzen natürlich utopisch.

Wer den Anspruch etwas nach unten schraubt, kann sich mit 100 Euro bereits eine recht zuverlässige Toolbox nach Hause holen, um Schnappschüsse oder die Urlaubsfotos ästhetisch aufzubereiten. Es geht noch etwas günstiger. In den letzten Jahren haben sich einige Open Source Varianten – sowohl im Bereich der Bildbearbeitung als auch für die Entwicklung durchgesetzt.

Ein gutes Beispiel ist hier Gimp. Der Vorteil: Enthusiasten entwickeln die Software stetig weiter, fügen neue Funktionen ein – und das Ganze ist auch noch kostenlos. Aber: Nutzer, die keinen Cent ausgeben wollen, müssen im Vergleich mit kostenpflichtigen Tools mit Abstrichen – etwa bei der Funktionalität – leben.

Abbildung 2: Heute besteht eine große Auswahl im Bereich der Bildbearbeitungssoftware. Es ist für jeden Geschmack und jede Preisklasse etwas Passendes dabei.

Fazit: Amateur oder Profi – jeder kann Bilder bearbeiten

Eine gute Bildbearbeitung kann aus einem schlechten Foto keinen erstklassigen Schnappschuss machen. Bildfehler wie fehlende Helligkeit, rote Augen oder der Weißabgleich lassen sich mit vielen Programmen korrigieren. Greifen Hobbyfotografen zum ersten Mal zur Kamera und anschließend zu Maus und Zeichenwerkzeug, beginnt die Reise durch eine neue Welt mit vielen Möglichkeiten. Moderne Bildbearbeitung kann viele Effekte erzeugen, Bilder schärfen und Farben noch intensiver wirken lassen. Dabei muss es nicht zwingend eine professionelle Software sein. Einige Open Source Lösungen sind für Amateure in jedem Fall interessant.

Bildquellen:

Abbildung 1: @ Soorelis (CC0-Lizenz) / pixabay.com

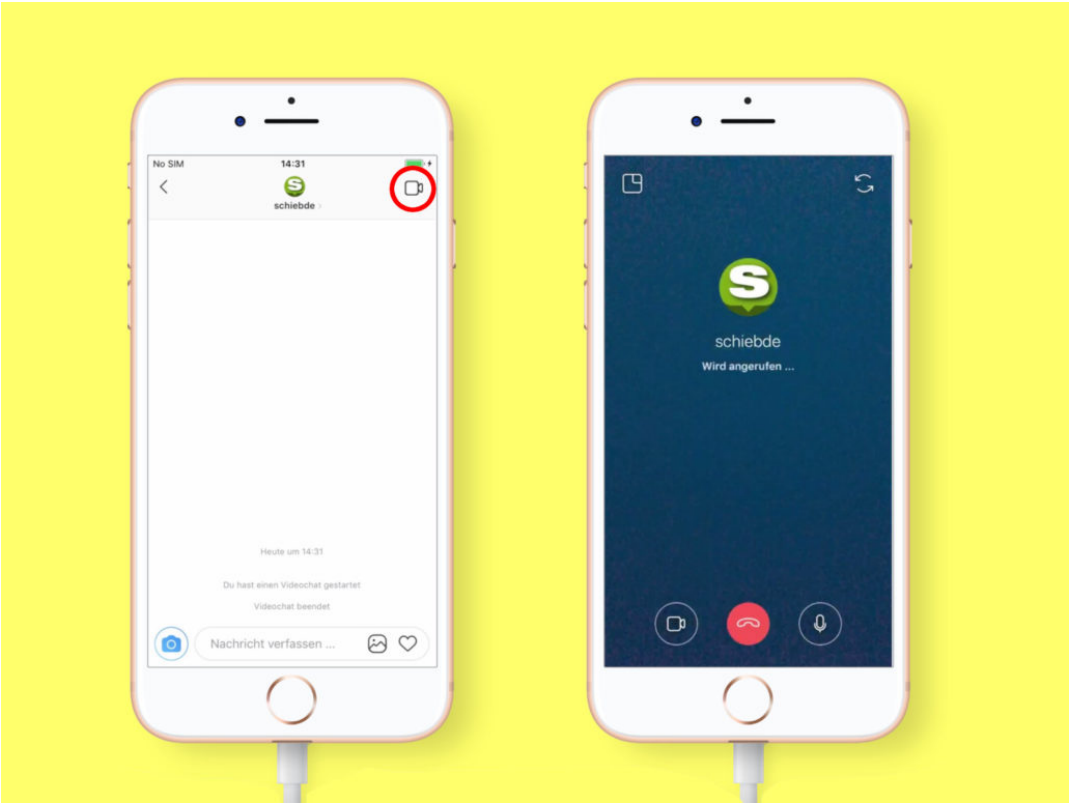
Abbildung 2: @ alexx-ego (CC0-Lizenz) / pixabay.com

Instagram: Video-Chat starten

Ab sofort können Nutzer von Instagram sich gegenseitig per Video-Chat anrufen und unterhalten. Dieses Feature hat Instagram direkt in den Posteingang integriert. Dort erreichen den Nutzer auch Antworten auf die geposteten Storys.

Mit Instagram lassen sich Video-Chats starten, indem zunächst den Posteingang gewechselt wird. Jetzt auf den Namen eines Kontakts tippen, der angerufen werden soll, oder oben rechts auf den Plus-Button klicken und dann einen Kontakt aus der Liste auswählen.

In der darauffolgenden Chat-Ansicht findet sich ab sofort ein Kamera-Symbol. Per Fingertipp auf dieses Icon wird der Anruf gestartet. Damit das klappt, muss der Empfänger die neueste Version der Instagram-App installiert haben. Nachträglich lassen sich Video-Anrufe übrigens auch zu einfachen Sprach-Anrufen umwandeln, indem die Kamera deaktiviert, das Mikrofon aber eingeschaltet bleibt. Zusätzlich lässt sich auch zwischen der Vorder- und der Rückseiten-Kamera wechseln.



Wer übernimmt den Markt?

Video-Telefonate sind keine neue Funktion in Social Media-Apps sowie Messaging-Netzwerken. In vielen Programmen sind diese Live-Funktionen enthalten. Ursprünglich stammt die Idee aus dem Programm Skype – allerdings gibt es in letzter Zeit immer mehr und bessere Alternativen.

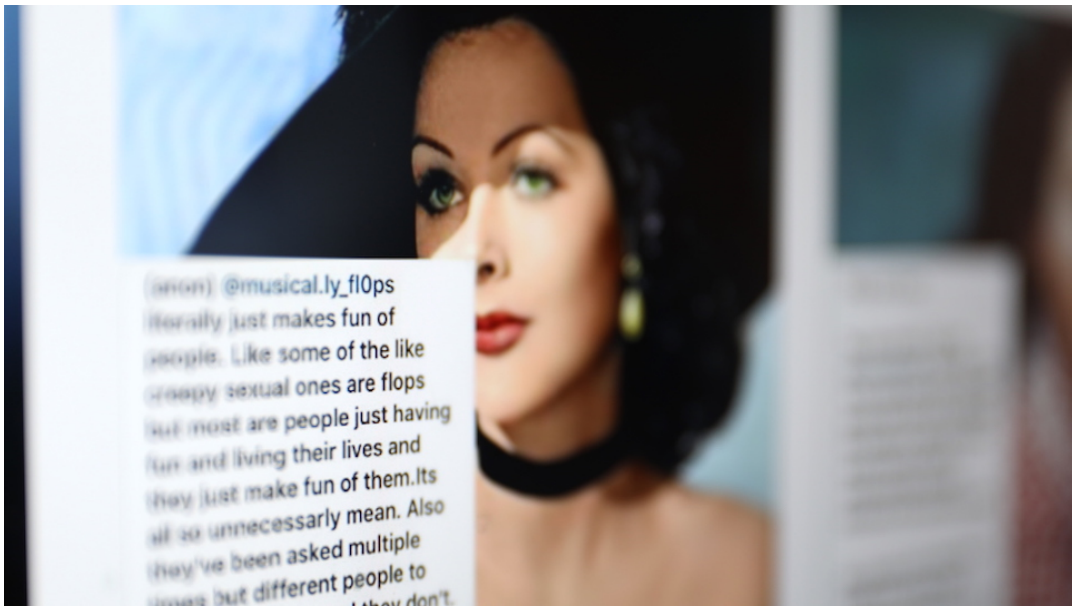
Gamer etwa bevorzugen Discord; Programmierer und andere Teams konzentrieren sich auf

Slack, und auch Facebook Messenger sowie WhatsApp verfügen über einen Audio- und Video-Chat. Ganz zu schweigen von Apple mit der iMessage- und FaceTime-Plattform. Instagram hat genauso hohe Chancen wie alle diese anderen Tools, um ein würdiger Nachfolger des inzwischen nicht mehr so beliebten Skype zu werden.

Jugendliche informieren sich verstärkt auf Instagram - in Flop-Accounts

Eigentlich ist Instagram eine Foto-Plattform. Doch immer mehr Jugendliche nutzen den Bilderdienst, um sich über aktuelle Themen auszutauschen. Eine ganz neue Kultur ist gestartet: Über sogenannte Flop-Accounts werden aktuelle Themen zur Diskussion gestellt. Meist gibt es mehrere Moderatoren.

Facebook? Nur was für alte Leute. Seitdem auch Lehrer, Eltern und Großeltern in Facebook sind, gilt Mark Zuckerbergs Netzwerk nicht mehr unbedingt als "the place to be". Andere Netzwerke sind populärer. Snapchat natürlich. Aber auch Instagram. Nun kennen wir alle Instagram als Foto-Plattform: Hier sehen wir, wie toll das Leben der anderen ist. Lecker Essen. Schöner Cocktail. Neues Kleid. Städtereise. Wellness. Sowas halt.



Instagram als Infoquelle

Wer hätte gedacht, dass ausgerechnet Teens das Instagram-Netzwerk für andere Dinge nutzen - nämlich für Debatten und zum Diskurs? Ich war jedenfalls überrascht, dass immer mehr Jugendliche sich in Instagram über sogenannte Flop-Accounts informieren und schlau machen, etwa hier, hier oder hier. Sie diskutieren hier ernsthaft und intensiv relevante Themen. Und mit relevant meine ich nicht die Features der neuen X-Box, den Geschmack spezieller Colasorten oder die neusten Trick-Filter von Snapchat.

Nein, es sind vor allem ernsthafte Themen wie Waffenkontrolle, Einwanderung, Vergewaltigung, Sex in der Jugend oder Präsident Trump, mit denen sich die User/innen beschäftigen. Aber auch die Ausbrüche von YouTubern, Breaking News oder was im Netz gerade viral geht, wird aufgegriffen. Solche Themen werden in den Flop-Accounts auf Instagram tatsächlich diskutiert. Betreut werden die jeweiligen Flop-Accounts von mehreren Jugendlichen, die ein Auge darauf haben, dass nichts aus dem Ruder läuft.

https://vimeo.com/282643840

Flop-Accounts auf Instagram: Moderatoren wählen Themen aus

Treffpunkt: Unter sich bleiben

Es gibt eine Menge guter Gründe, wieso sich die Jugendlichen in Instagram treffen. Dort gibt es - noch - nicht so viele "Trolls", also Verrückte, die mit ihren verdrehten Kommentaren alles aufmischen, so wie bei Twitter, Facebook oder Reddit längst üblich. Außerdem werden Jugendliche in vielen Foren nicht ernst genommen. Last not least sind viele reguläre Foren überflutet von Nachrichten, die Spam-Bots einspeisen.

Also schaffen sich die Jugendlichen eine eigene Diskussionskultur. Aber wieso "Flop"-Account? Weil es vor allem darum geht, über "Flops" zu sprechen. Wenn zum Beispiel der Präsident etwas twittert oder sagt, das - sagen wir mal - anfechtbar ist. Oder wenn ein YouTuber sich rassistisch äußert. Oder überhaupt alles, was Jugendliche als unangemessen oder falsch empfinden (könnten) - und in den traditionellen Medien nicht auftaucht. So was landet in Flop-Accounts - als Text, mit Fotos, Videos, Screenshots oder Links.

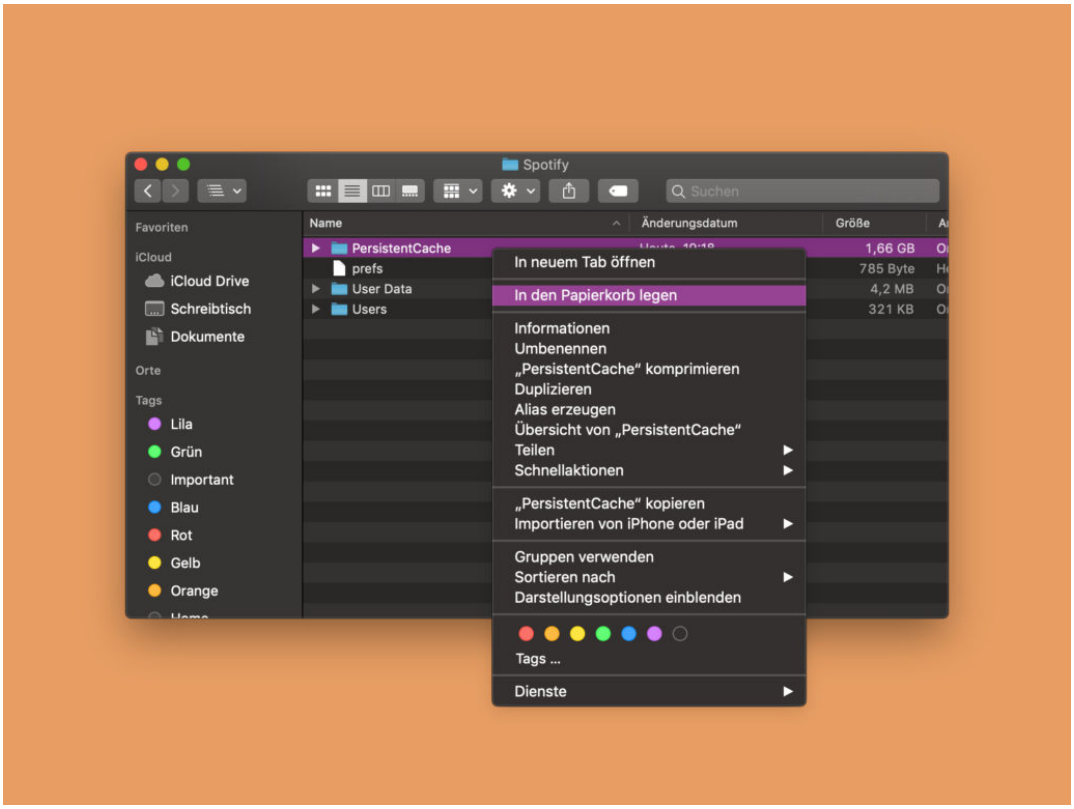
Mac: Spotify-Cache leeren

Songs, die man auch offline hören will, lassen sich mit Spotify als Download auf der Festplatte sichern. Sie sind dann auch abrufbar, wenn gerade keine Verbindung zum Internet besteht. Kommt Spotify durcheinander, kann dieser Cache auch manuell zurückgesetzt werden.

Aber Achtung: Löscht man den Download-Cache des Musik-Programms, müssen anschließend alle Playlists, die auch offline verfügbar sein sollen, erneut vom Server des Anbieters synchronisiert werden. Das kann einige Zeit dauern – je nachdem, wie viele Songs in den Wiedergabe-Listen enthalten sind.

Mit den folgenden Schritten lässt sich der Spotify-Cache unter macOS leeren:

1. Zunächst die Spotify-App beenden, falls sie offen sein sollte.
2. Jetzt ein neues Finder-Fenster öffnen.
3. Hier zum eigenen Profil-Ordner wechseln. Am einfachsten geht das durch Aufrufen des Menü-Eintrags **Gehe zu, Benutzerordner**.
4. Nun den Ordner **Library, Application Support, Spotify** öffnen.
5. Hier das Verzeichnis **PersistentCache** löschen – fertig.



Schutz gegen Hackangriffe

Der WDR und das ZDF wurden gehackt. Das kann grundsätzlich jedem drohen. Auch Politikern, Institutionen, Unternehmen – und natürlich auch Privatleuten. Denn Hacker kennen keinen Schlaf: Sie sind rund um die Uhr im Einsatz, in allen Zeitzonen. Aber wie groß ist das Risiko, kann man Hackangriffe erkennen und wie sich dagegen schützen?

Wie groß ist eigentlich das Risiko, als Privatmensch von Hackern angegriffen zu werden?

Da muss man differenzieren. Wenn ich zum Beispiel in einem Unternehmen arbeite, das für Industriespionage in Frage kommt, etwa weil ganz besonders interessante Produkte entwickelt und hergestellt werden, dann bin ich auch als Privatmann gefährdet – also wenn ich nicht am Arbeitsplatz bin. Dasselbe gilt für Geheimnisträger ganz allgemein: Erfinder, Journalisten, Politiker, Juristen, Beamte...

[caption id="attachment_759293" align="alignnone" width="500"]


pixelcreatures / Pixabay[/caption]

Wenn Hacker gezielt angreifen, dann werden sie es nicht nur im Büro probieren, sondern auch – und vielleicht sogar ganz gezielt – im Privatbereich. Solche gezielten Angriffe, die auf ganz bestimmte Personen abzielen und zugeschnitten sind, sind allerdings eher selten.

Üblicher sind Hackangriffe, die im großen Stil durchgeführt werden: Da werden die Opfer nicht gezielt ausgewählt, weil man weiß, dass sie etwas zu bieten haben, sondern zufällig. Nach dem Motto: Mal sehen, was es da zu holen gibt.

Wie laufen gezielte Angriffe grob ab?

Wenn ich zum Beispiel Zugriff auf die Mails eines Vorstands kommen möchte, kann ich als Hacker versuchen, mir Zugang zu den Rechnern oder Mobilgeräten des Vorstands zu besorgen – oder gehe über die Assistenz, die in der Regel auch Zugang hat. Dann wird teilweise genau recherchiert: Wer ist das? Welche Interessen hat er oder sie?

So etwas nennt man "Social Engineering". Liebt die Assistentin des Vorstands zum Beispiel Radtouren in Frankreich, dann bekommt sie eine Mail, die auf genau dieses Themengebiet abzielt – mit einem Link auf eine Webseite, die speziell dafür gemacht ist. Und in der Mail ist eine Phishing-Attacke versteckt oder auf der Webseite ein Trojaner.

[caption id="attachment_759294" align="alignnone" width="500"]

 xusenru / Pixabay[/caption]

Durch Ausnutzen von Sicherheitslücken werden dann Zugangsdaten abgefischt – oder Trojaner eingespielt. Software, die spioniert und womöglich die Tastatur abhört. So kommt man an Zugangsdaten. Der Aufwand ist allerdings sehr groß. Der wird nur betrieben, wenn es sich richtig lohnt – oder wenn es den Auftrag gibt, etwa von Geheimdiensten. Die große Masse wird also nicht à la Hollywood angegriffen.

Sind wir dann also sicher – oder gibt es trotzdem Hackangriffe?

Der Begriff "Hackangriff" ist ja weit gefasst. Wenn ein Hacker versucht, in den Server eines Onlinedienstes einzudringen, wo ich ein Onlinekonto habe, dann kann ich betroffen sein, ohne dass meine Rechner oder Mobilgeräte angegriffen, untersucht oder manipuliert werden. Denn ist der Server schlecht abgesichert, das Passwort vielleicht unzureichend gesichert gespeichert, muss ich erleben, dass meine Zugangsdaten abgegriffen werden.

Das kommt leider vergleichsweise häufig vor. Dann gehen die Zugangsdaten im Netz herum – und können missbraucht werden. Dritte können meine Identität einnehmen, in meinem Namen

Mails schreiben, einkaufen, andere traktieren. Oder aber, meine Geräte werden angegriffen, wie die von Millionen anderen auch, um zu sehen, welches Betriebssystem ich nutze, ob es Sicherheitslecks gibt – und ob man mir Software unterjubeln kann, die Schaden anrichtet.

Manche Programme spionieren Daten aus, etwa Zugangsdaten oder Kontodaten, andere Programme versuchen mich zu erpressen oder sie nutzen meinen Rechner, um Bitcoins zu schürfen.

[caption id="attachment_756101" align="alignnone" width="500"]

TheDigitalArtist / Pixabay[/caption]

Phishing-Methode

Wie es aussieht, wurden mal wieder Phishing-Methoden eingesetzt, um vertrauliche Informationen auszuspähen. Von Phishing hat man eigentlich schon lange nichts mehr gehört.

Phishing ist eine beliebte Methode: Man bekommt eine Mail, die täuschend echt aussieht, so als wäre sie von Amazon, Paypal, meiner Bank – oder meiner Firma. Ich werde aufgefordert,

mich einzuloggen, etwa, weil das Passwort sonst ausläuft. Ich lande auf einer Webseite, die ebenfalls täuschend echt aussieht.

Ich gebe dort die Zugangsdaten ein – aber die Webseite war getürkt, die Daten landen bei den Betrügern. Dagegen kann man sich wehren, indem man moderne Browser nutzt. Die kennen die populärsten Phishing-Seiten und warnen einen, wenn man dort landet. Außerdem sollte man nie aus Mails heraus wichtige Seiten aufrufen, sondern immer Lesezeichen verwenden. Und die Adressen im Browser genau im Auge behalten. So kann man Phishing schon ganz gut vermeiden.

Zwei Faktor Authentifizierung

Wir schützen unsere Onlinekonten ja in der Regel durch Passwörter – es sollen sichere sein, das wissen wir mittlerweile. Aber reicht das, ein sicheres Passwort zu wählen?

Nein, das reicht nicht. Denn Passwörter könnten sich knacken lassen – oder sie werden ausspioniert, zum Beispiel durch einen Phishing-Angriff. Es gibt eine Methode, mit der man seine Onlinekonten deutlich besser absichern kann: die Zwei-Faktor-Authentifizierung. Da muss man beim Einloggen neben Benutzername und Passwort auch noch einen Code eingeben, der

im Handy erzeugt wird.

Das bedeutet: Ich kann Dir mein Passwort für Facebook, Twitter oder meine E-Mail verraten. Kein Problem. Du hast keine Chance, weil Du den zusätzlichen Sicherheitscode nicht kennen kannst. Der wird beim Einloggen in meinem Handy erzeugt. Man braucht also zwingend Zugriff auf das Smartphone. Die Zwei-Faktor-Authentifizierung macht Onlinekonten deutlich sicherer, ohne großen Aufwand. Man muss diese Zwei-Faktor-Authentifizierung allerdings ausdrücklich aktivieren. Das geht bei Facebook, Twitter, Google, Amazon, Apple und viele, viele weitere Dienste.

Wer mehr dazu wissen will: In meinem eBook Das sichere Login beschreibe ich alles ausführlich.

Firewalls und andere Schutzmechanismen

Eine "Firewall" ist eine komplizierte Sache: Damit sie ordentlich funktioniert, muss man eine

Menge davon verstehen – und auch wissen, was man zulassen will und was nicht. Um so etwas perfekt einzustellen, muss man Profi sein. Sonst ist man entweder unzureichend geschützt, fühlt sich aber sicher, oder manche Dinge funktionieren nicht.

Besser sind Schutz-Pakete, die darauf achten, dass man nicht auf Phishingseiten landet, die verdächtige Aktivitäten wie Datenübertragung im Hintergrund erkennen und auf Viren und Trojaner achten. So etwas kann sinnvoll sein, vor allem auf Windows-Rechnern und Android-Mobilgeräten. Ansonsten gilt: Immer Updates für Betriebssystem, Browser und Standard-Softeare einspielen. Das ist die beste Absicherung, denn in der Regel werden vorhandene Sicherheitslecks genutzt beim Hacken. Gibt es die nicht, laufen die meisten Tricks auch ins Leere.

[caption id="attachment_759295" align="alignnone" width="500"]

TheDigitalArtist / Pixabay[/caption]

Alte geplante Aufgaben bereinigen

Wird auf einem Windows-PC Software installiert, etwa Google Chrome, können dabei auch gleichzeitig Aufgaben geplant werden, die das Programm später im Hintergrund ausführen will. Das Problem: Beim Entfernen der Software bleiben diese geplanten Tasks oft ungewollt erhalten.

Dabei lassen sich alte geplante Aufgaben bei Bedarf auch manuell aus der zugehörigen Liste löschen. Dazu ist ein Eingriff in den Aufgabenplaner erforderlich:

1. Zunächst auf **Start** klicken.
2. Dann ins Suchfeld den Begriff **Aufgabenplanung** eintippen.
3. Nun auf das erste Ergebnis klicken.
4. Hier auf der linken Seite zur Aufgabenplanungs-Bibliothek navigieren.
5. Dort lassen sich Einträge finden, die problemlos bereits entfernten Programmen zugeordnet werden können. Im Beispiel geht es um **GoogleUpdate TaskMachineCore** – den automatischen Update-Mechanismus von Chrome und Co.
6. Nachdem der jeweilige Eintrag markiert ist, kann in der Spalte rechts auf **Löschen** geklickt werden.