

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark and out of focus.

Schieb Report

Ausgabe 2019.52

Mit dem richtigen Zubehör Geld sparen und die Computer-Arbeit erleichtern

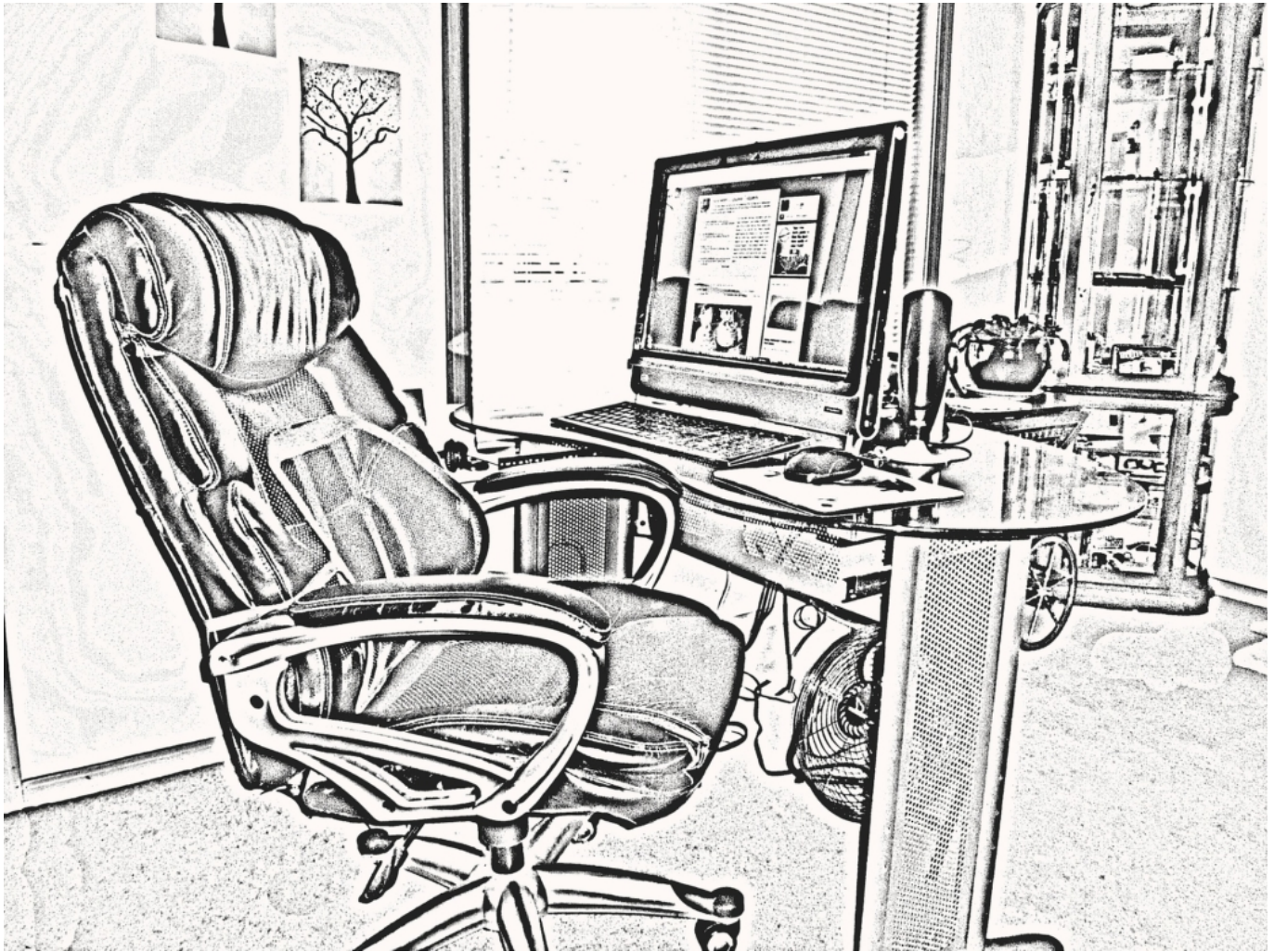
Mehr als sieben Millionen Menschen sitzen in Deutschland tagtäglich am Computer. Büroarbeit in modernen Unternehmen. Dabei wird im Zeitalter der Digitalisierung natürlich großen Wert auf eine sorgsame Arbeit am Computer gelegt. Die Arbeit am PC wird dabei um einiges leichter, wenn man auf das richtige Zubehör setzt.

Alle, die viel oder häufig am Computer oder Notebook sitzen, können mit den passenden Hilfsmitteln für eine große Entlastung sorgen. Ich weiß das aus eigener Erfahrung: Gerade erst habe ich Dokumenten-Scanner und Drucker durch neue Modelle ersetzt. Die Vorgängermodelle haben mich verrückt gemacht: Der Drucker hat manche Seite drei Mal gedruckt, der Scanner Blätter verschluckt. Seitdem ich die neuen Geräte habe, nutze ich die gut gelaunt.

Doch man kann sich die Arbeit am PC auch einfacher machen - etwa durch kleine ergonomische Hilfen oder cleveres Druckerzubehör. Auch mit Kleinigkeiten lässt sich oft eine positive Wirkung erzielen.

Oft benötigt es keinen großen Aufwand. Schon die richtige Position von Schreibtisch und Bürostuhl kann wahre Wunder bewirken - und wird von vielen unterschätzt. Immer mehr Menschen, die im Büro am PC sitzen, haben gleich mehrere Computermonitore auf dem Schreibtisch stehen. Das hat Folgen für die Sitzposition - und kann starke Verspannungen im Rücken zur Folge haben. Wer zu weit oder zu nah am Schreibtisch sitzt, klagt nicht selten über Rückenschmerzen und Gelenkschmerzen. Auch die Sitzhöhe spielt eine entscheidende Rolle.

Dabei begehen die meisten den Fehler, den Bürostuhl auf die maximale Sitzhöhe hochzuschrauben. So ergibt sich oft eine ungünstige, unnatürliche Sitzposition, die früher oder später in Gelenkschmerzen und Muskelspannung münden können. Deshalb den Arbeitsplatz für ein komfortables Sitzen einstellen.



Mit ergonomischen Büromöbeln die Körperhaltung verbessern

Aber nicht nur Stuhl, Monitor und Schreibtisch sind wichtig, sondern auch, was wir auf dem Schreibtisch haben - und ständig benutzen. Sogenannte "Vertikalmäuse" zum Beispiel entlasten die Handgelenke, da sie ein ergonomisches Arbeiten ermöglichen. Etwas gewöhnungsbedürftig, aber durchaus auch gut für entspanntes Arbeiten sind Beidhandmäuse.

Wie die Kollegen von "Impulse" herausgefunden haben, können [spezielle Bürostühle mit einem ergonomischen Rückenpolster](#) dafür sorgen, die Körperhaltung während der Arbeitszeit zu verbessern. Denn viele Bürostühle in Deutschland sind viel zu weich und polsternd eingestellt. Das mag bequem erscheinen, doch auf Dauer klagen nicht wenige Angestellte über Rückenschmerzen. Ergonomische Rückenlagen entlasten die Wirbelsäule.

Mit dem richtigen Zubehör Geld sparen

Aber auch die Kosten sollte man im Blick behalten. Im digitalisierten Büro gibt es heute eine Menge Fixkosten, die ordentlich ins Geld gehen können. Das gilt vor allem für Drucker-Zubehör wie Toner, Tinte oder Druckerpapier. Deshalb greifen viele Verbraucher auf Drucker-Zubehör von alternativen Herstellern zurück, etwa Toner oder Tinte. Die sind meist deutlich günstiger als

das Originalzubehör.

Einen ausführlichen Bericht zu alternativem [Drucker-Zubehör](#) und Büroartikeln gibt es auf der Plattform von prindo.de. Ein Versandhaus und Spezialist für Büroartikel, aber eben auch für Tinte und Toner. Einfach die Preise vergleichen: Hier kann sich jeder einen Überblick verschaffen und so herausfinden, wie es gelingt, [Kosten für Büroartikel einzusparen](#).

Behörden sollen Passwörter bekommen: Welche Daten braucht die Polizei?

Das Bundesjustizministerium hat einen Gesetzentwurf entwickelt, der Hass und Hetze im Netz besser bekämpfen soll. Unter anderem, indem die Sozialen Netzwerke solche Posts melden müssen. Doch es gibt auch einen heiklen Part: Polizei und andere Behörden sollen künftig in bestimmten Fällen mehr User-Daten bekommen. Auch Passwörter. Ich habe mit der Polizei darüber gesprochen.

Die Diskussion um den aktuellen Gesetzentwurf des Bundesjustizministeriums sorgt für eine Menge Diskussionen: Mit neuen Regeln will die Ministerin die zunehmende Hasskriminalität im Netz bekämpfen.

Soziale Netzwerke sollen aktiv Postings mit Rechtsverstößen an das BKA melden. Außerdem sieht der Gesetzentwurf vor, dass in diesen und vielen anderen Fällen Polizei und andere Behörden schneller und mit mehr Daten versorgt werden sollen. Wir haben in Digitalistan [hier schon über die Pläne berichtet](#).

Die Netz-Community ist in heller Aufruhr. Verständlich, denn wenn den Behörden künftig selbst Passwörter ausgeliefert werden, scheint - gefühlt! - nichts mehr sicher. Denn Passwörter sind der Generalschlüssel zu Onlinediensten, Mail-Konten, Messengern.

Kein Wunder, dass viele fürchten, ihre Privatsphäre sei nichts mehr wert - oder zumindest erheblich bedroht. Renate Künast hat sogar verfassungsrechtliche Bedenken. Andere sprechen von einem "großen Lauschangriff". Das wiederum erscheint mir übertrieben.



Kein großer Lauschangriff - aber heikel

Denn ein Lauschangriff, zumal ein großer, würde bedeuten, dass massenweise spioniert wird. Das ist jedoch kaum möglich. Denn zum einen ist für die Herausgabe solch sensibler Daten eine richterliche Anordnung erforderlich - und die gibt es nicht massenweise. Zum anderen gibt es Passwörter in der Regel nur verschlüsselt, und die müssten dann erst mal aufwändig geknackt werden. Das ist schon im Einzelfall aufwändig - und taugt ganz gewiss nicht für massenhafte Überwachung.

Ich wollte mal wissen, wie die Polizei das sieht. Sebastian Fiedler vom Bund Deutscher Kriminalbeamter sagt: "Wir wollen nicht viele Daten. Die können wir gar nicht verarbeiten. Wir brauchen ganz gezielt Daten, um bei der Fahndung in Einzelfällen weiterzukommen." Fiedler erklärt mir anschaulich und glaubwürdig, dass die Polizei auf Daten angewiesen ist - aber zur Bekämpfung weniger Einzelfälle, nicht für die Masse. Das komplette Interview findet Ihr hier im Blog.

Polizei erklärt die Notwendigkeiten

Angesichts der Personalsituation bei der Polizei glaube ich das sofort. Das Misstrauen bei Netzaktivisten und vielen anderen richtet sich daher wohl eher gegen die Politik. Die hat ein Glaubwürdigkeitsproblem, nicht die Polizei.

Verständlich, denn wer derart sensible Eingriffe geplant, der muss genau erklären, was er will, wie das gehen soll und dass man - als Politik - verstanden hat, dass es heikel sein könnte. Und wie man vermeiden möchte, dass die IT-Sicherheit unbescholtener Bürger gefährdet ist.

Nicht umsonst haben hohe Gerichte immer wieder die Vorratsdatenspeicherung einkassiert. Weil es eben wichtig ist, eine gesunde Balance zu finden zwischen Rechten der Bürger und Notwendigkeiten der Behörden. Wer Polizei und andere Behörden mit den dringend nötigen Daten und Informationen versorgen will, kann das also nicht im Hauruck-Stil machen, sondern muss mit Augenmaß vorgehen - und erklären!

Das passiert leider viel zu selten.

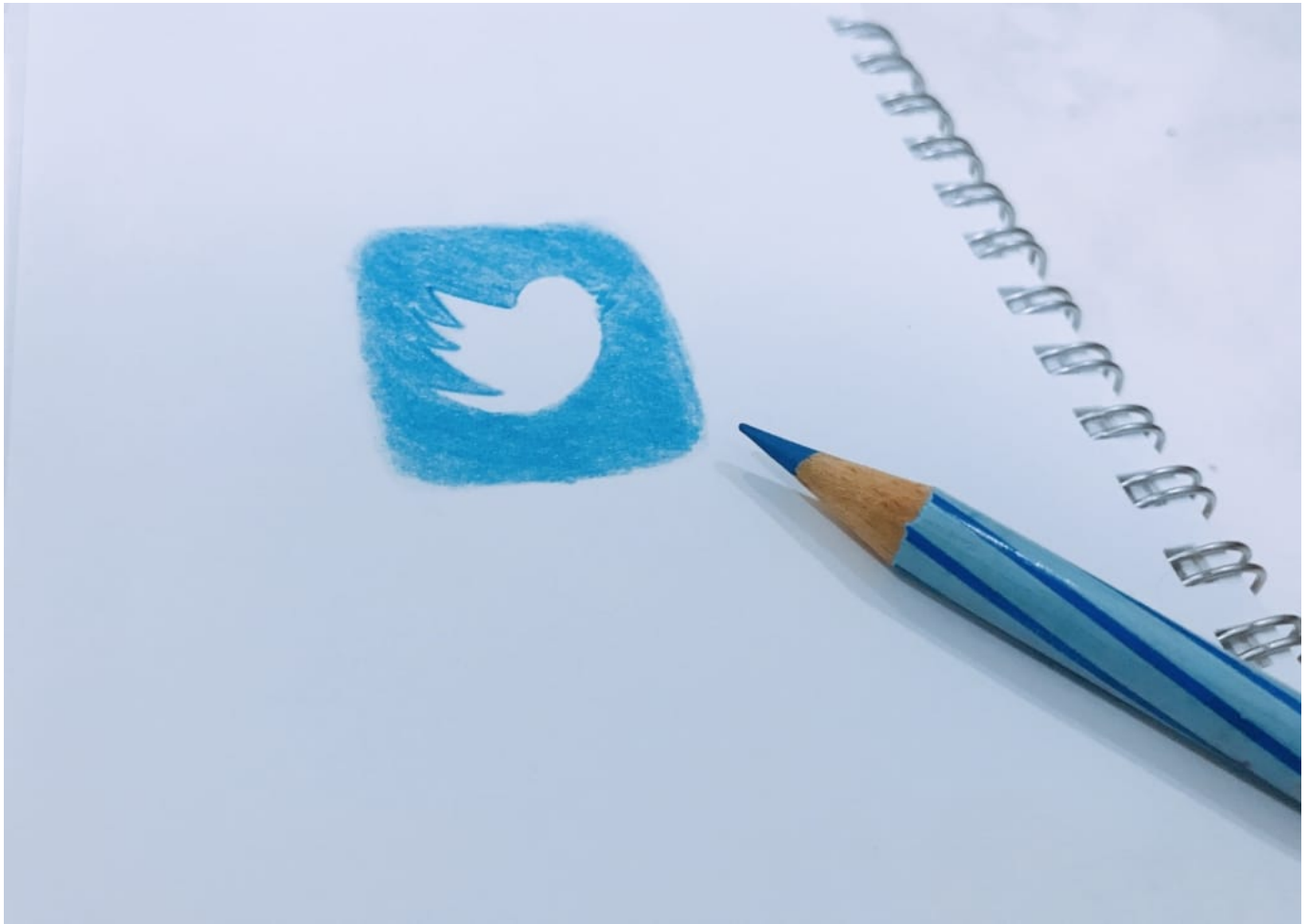
<https://vimeo.com/380757294>

Overblocking bei Twitter: Wir brauchen Lösungen

Donald Trump twittert täglich. Das wissen wir. Aber auch viele Behörden twittern. Die Polizei zum Beispiel. In Zeiten, in denen sich viele Menschen über ihr Smartphone informieren, kann das in Krisensituationen durchaus helfen. Es hat schon viele Fälle gegeben, da hat die Polizei über Twitter über Terrorlagen informiert. Doch vergangene Woche sind gleich 11 Polizei Twitter Accounts stillgelegt worden. Problematisch, wenn Konzerne wie Twitter die Accounts von Behörden sperren - wie gerade geschen.

Betroffen waren nicht große Städte wie Köln oder Düsseldorf, sondern Orte wie Borken, Höxter, Heinsberg oder Steinfurt, die in der Regel zwischen 400 und 1200 Follower haben. Also eher Mini-Accounts. Nicht nur Journalisten greifen auf diese Kanäle zu, um sich zu informieren, sondern auch Bürger. Doch für etliche Stunden stand in den Profilen: Weil eine ungewöhnliche Aktivität von den Profilen ausgegangen sei, seien die Profile eingeschränkt oder blockiert worden.

Eine typische Meldung: Hier hat sich die Aufpasser-Software von [Twitter](#) an irgendwas gestört und die Profile kurzerhand eingeschränkt oder lahmgelegt. Die Nutzer müssen in einer solchen Situation explizit zustimmen, um weiterlesen zu können. Über die Suchfunktion von Twitter sind solche Profile dann nicht zu erreichen. Einige Behörden mussten gegenüber Twitter Belege vorbringen, damit Twitter die Accounts wieder freischaltet.



Algorithmen entscheiden über Sperrung

Dass Konten von Promis oder jetzt von Behörden gesperrt werden, kommt immer wieder vor. Es gibt Nutzungsbedingungen, was in einem Konto erlaubt ist und was nicht. Das gibt es in allen Sozialen Netzwerken. Und alle Dienste nutzen Algorithmen, um das zu überwachen. Fällt ihnen etwas Verdächtiges auf – etwa das Verteilen von Pornografie, Hass oder Hetze oder bestimmter Sprachgebrauch, sperren die Aufpasser-Algorithmen die Konten entweder selbst, oder sie markieren sie und „Supervisor“ aus Fleisch und Blut sperren sie und entscheiden dann.

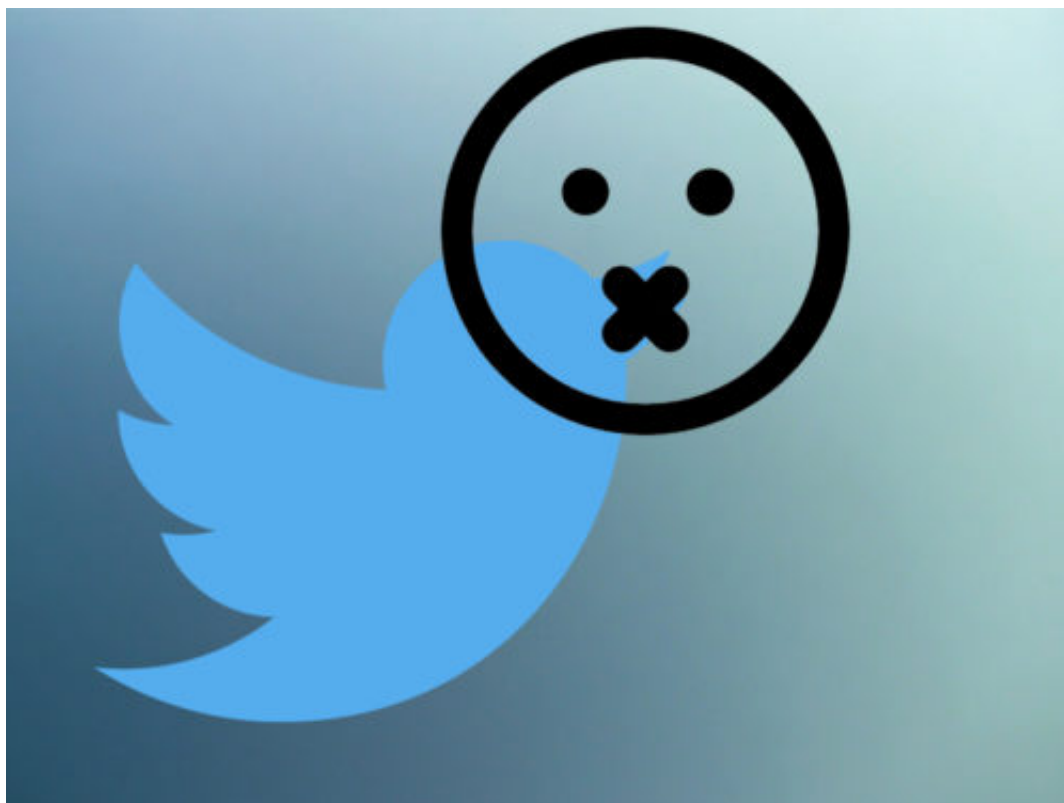
Deshalb kommt es vor, dass Konten gesperrt werden, für die es eigentlich gar keine guten Gründe gibt. Das wird dann „[Overblocking](#)“ genannt: Also die Sperrung kompletter Konten aus übertriebener Vorsicht. Es gibt beides: Einigen Konten werden nicht gesperrt, obwohl es dringend erforderlich wäre, andere werden gesperrt, obwohl es Unsinn ist. Bei Accounts von Behörden ist das natürlich besonders heikel.

Overblocking kommt immer wieder vor

Kein Einzelfall, dass Konten unnötigerweise gesperrt werden. Der Fall ist nur ein weiteres Beispiel aus einer ganzen Reihe von Sperren, die zuletzt für viel Unmut in der Nutzerschaft

gesorgt hatten. Der Schriftsteller Tom Hillenbrand hat wegen eines satirischen Tweets zur Europawahl seit Monaten keinen Zugriff auf seinen Account – [und zuletzt im Mai getwittert. Auch viele andere Nutzer wurden deshalb gesperrt.](#)

Im Mai hat Twitter [das Konto der Jüdischen Allgemeinen blockiert](#). Autoren, Satiriker, sogar Redaktionen sind betroffen. Die Filter-Algorithmen sind zu „dumm“, um zu unterscheiden, wer da twittert. Es macht halt einen Unterschied, ob eine Redaktion zB etwas zitiert oder ein Satiriker etwas aufschreibt, oder ob jemand offen und ungeniert hetzt.



Es braucht unterschiedliche Kontoarten

Ich denke, es wäre klug und wohl auch nötig, verschiedene Kontoklassen anzubieten. Zum Beispiel spezielle Konten/Accounts für Öffentliche Stellen, für Behörden wie die Polizei, aber auch für journalistische Angebote, Künstler oder Satiriker. Denn wenn der Account einer Behörde wie der Polizei geblockt wird – in der Regel wohl unzutreffenderweise –, dann hat das Konsequenzen für alle.

Darum sollten Dienste wie Witter bei bestimmten Inhabern lieber zwei Mal drauf schauen, bevor so ein Account geblockt oder eingeschränkt wird. Auch sollten zum Beispiel Künstler oder Satiriker mehr sagen dürfen. Hier könnte eine Äußerung durch die Kunstfreiheit gedeckt sein, es könnte auch ein Zitat sein – was bei jemand anders juristisch bedenklich ist. Am Ende müssen sich diese juristischen Unterschiede doch auch in den Onlinediensten widerspiegeln.

Gekaufter Beifall: Wie sich Promis Likes kaufen

Ein Herzchen in Instagram, ein blauer Daumen in Facebook - jeder freut sich über ein bisschen Zustimmung. Aber manche wollen sich gar nicht selbst freuen, sondern andere beeindrucken. Sie kaufen deshalb "Likes" ein: Sie bezahlen dafür, dass andere sie mögen. WDR, NDR und Süddeutsche Zeitung haben jetzt herausgefunden, wer dafür so alles Geld ausgibt.

Es ist ein Phänomen, das schon lange bekannt ist: [Likes](#) - also der leise, dafür aber für jeden sichtbare Applaus - auf Facebook, Instagram, YouTube und Co. ist käuflich. Wenn neben dem Foto auf Instagram 100 Herzchen stehen, muss das nichts bedeuten. Vielleicht sind 80 gekauft. Oder 99. Oder 100.

Es ist Realität: Wer nicht darauf warten will, dass Heerscharen von Besuchern herbeiströmen und den "Gefällt mir"-Button anklicken oder antippen, kauft sich diesen Crowd-Jubel einfach kurzerhand ein. Es gibt diverse Agenturen, die gegen Bezahlung für einen Like-Teppich sorgen. Damit die anderen denken: Wow - er oder sie hat aber eine Menge Zustimmung. Da mach ich doch mit... Je mehr jemand investiert, desto mehr Likes gibt es.



Wer Likes will, kann sie haben - gegen Bezahlung

Kollegen von NDR, WDR und Süddeutscher Zeitung haben in Zusammenarbeit mit der Ruhr-Universität Bochum untersucht, wer von solchen Likes profitiert. Ausgewertet wurde ein umfangreicher Datensatz des nach eigenen Angaben größten Anbieters dieser Art, der Firma Paidlikes aus Magdeburg. Die Firma beauftragt in großem Stil Clickworker - und die setzen ihre Likes je nach Wunsch des Auftraggebers. Es geht um rund 90.000 Social-Media-Seiten.

Darunter die Seiten von Politikern und Parteien, von Unternehmen und Influencern, Friseuren und Fitnesstrainern - allerdings kaum bekannte Namen.

Wer es nötig hat, sich Likes einzukaufen, ist zu bedauern. Aber überraschen kann es nicht: In der Welt der Sozialen Netzwerke gilt eben nur der etwas, der viele Follower hat - und möglichst viele Likes bekommt. Reichweite ist eine Ressource. Je größer sie ist, desto höher die Preise, wenn ein Influencer etwas in die Kamera hält. Kapitalismus pur. Gefakte "Gefällt mir"-Zahlen können deshalb mittelbar zum Erfolg führen - und die Investition kann sich lohnen. Das Unternehmen „Paid Likes“ sagt übrigens, die Sehnsucht nach Ruhm im Netz sei ein legales und legitimes Geschäftsmodell.

Ab zu TikTok: Hier werden jetzt Likes gesammelt

Die Recherche zeigt: Dem Daumen nach oben bei Facebook oder dem Herzchen bei Instagram ist einfach nicht immer zu trauen. Neu ist diese Erkenntnis nicht - aber wichtig, sie bis in den letzten dunklen Winkel zu verteilen. Denn je mehr Menschen darum wissen, desto geringer ist das Risiko, dass Unternehmen, die Heerscharen von Anklick-Sklaven beschäftigen, weiterhin beauftragt werden, die "Gefällt mir"-Statistiken zu schönen.

Was die Menschen nicht alles anstellen, nur um Klick-Applaus zu bekommen, kann man derzeit besonders gut auf TikTok beobachten. Das neueste Netz-Phänomen: Die Nutzerzahlen explodieren hier aktuell. Vielleicht, weil auf Instagram teilweise schon keine Like-Zahlen mehr angezeigt werden. Instagram [testet, wie es ankommt, wenn die Herzchen für die Allgemeinheit unsichtbar sind](#).

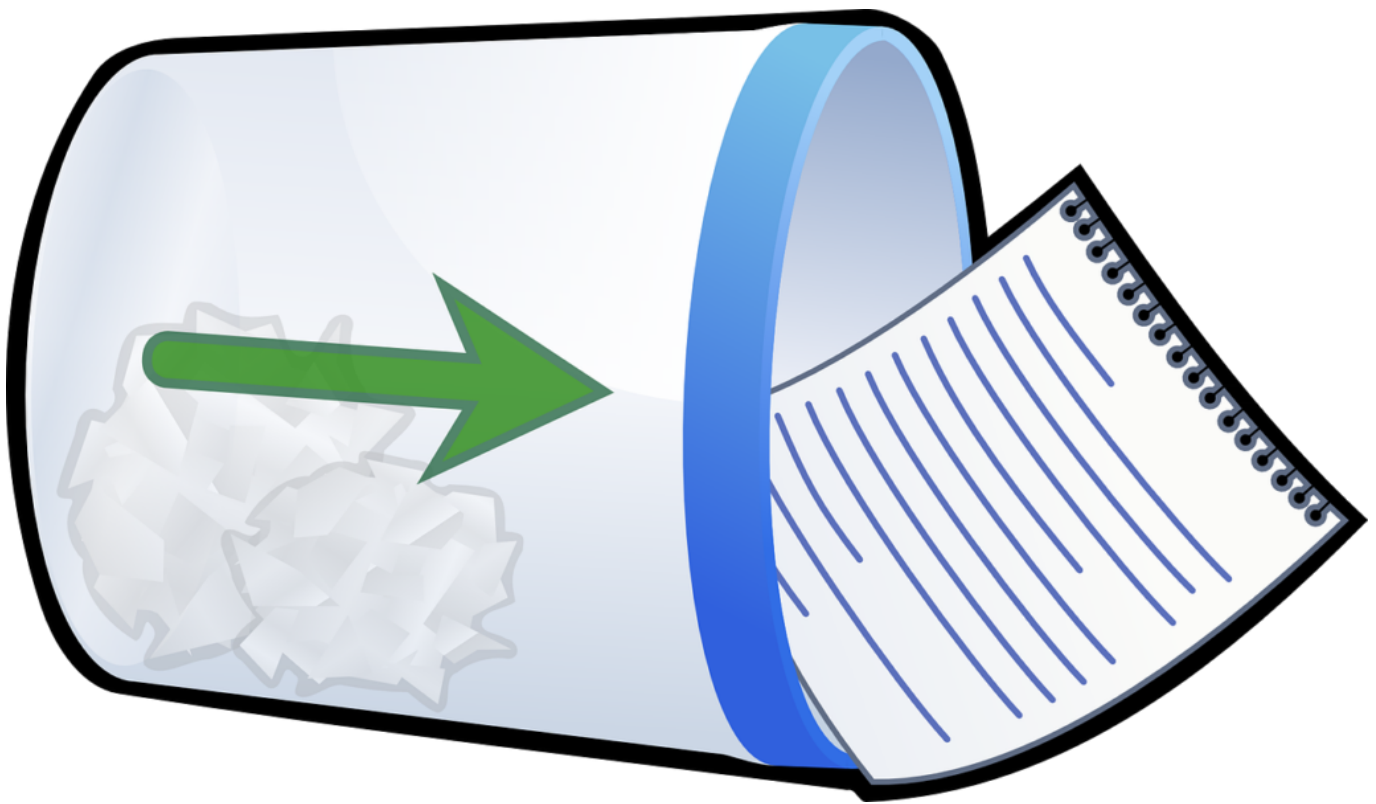
Gefällt keineswegs allen. Viele Menschen sind eben süchtig nach dieser fragwürdigen Art der Anerkennung.



Datenrettung mit FonePaw

Wir vertrauen unseren Geräten jede Menge wichtiger Daten und Dateien an. Nicht nur Termine und Kontakte, sondern auch Texte, Fotos oder Videos. Immer wieder passiert es, dass wichtige Daten oder Dateien verschwinden - aus technischen Gründen, weil wir einen Bedienfehler gemacht haben oder schlicht auf unerklärliche Weise. In solchen Fällen lohnt es sich, einen Rettungsversuch zu unternehmen.

Wir stellen hier auf [schieb.de](https://www.schieb.de) immer wieder spezielle Programme vor, um verloren gegangene Daten zu retten. Das Angebot an entsprechender Software ist erstaunlich groß. Vermutlich, weil es so häufig passiert, dass uns Usern Daten verloren gehen - und wir dann händeringend nach Hilfe suchen, die uns die Daten zurückholt.



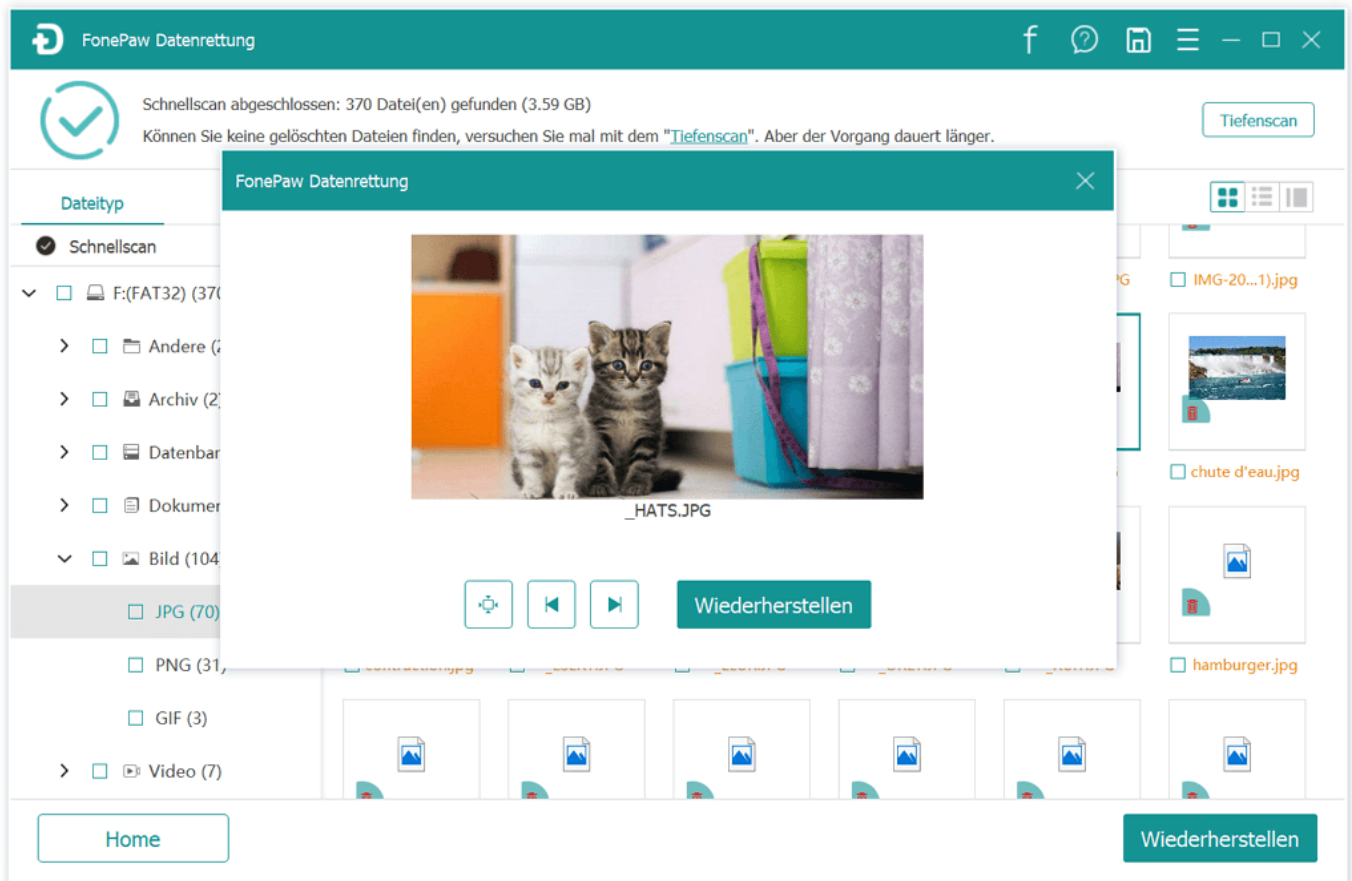
Gute Chancen auf Wiederherstellung

Die gute Nachricht: Bloß, weil eine Datei oder ein Dokument nicht mehr zu sehen ist, bedeutet das nicht, dass die Daten unwiederbringlich verloren sind. Denn sind die Dokumente aus Versehen im [Papierkorb gelandet](#), besteht Grund zur Hoffnung. Selbst wenn man [Dateien oder Dokumente](#) versehentlich überschrieben oder gelöscht haben sollte, kann ein Rettungsversuch erfolgreich sein - sogar sehr wahrscheinlich. Auch bei Hardwaredefekten ist die Chance auf Wiederherstellung durchaus hoch.

Was man als Laie wissen muss: Wenn ein Betriebssystem oder Mobilgerät Daten auf der Festplatte, im internen [Speicher](#), auf der Speicherkarte oder der externen Festplatte [löscht](#) oder

überschreibt, dann werden die Daten nicht wirklich gelöscht. Es ist vielmehr so, dass diese Daten durchaus noch auf dem Datenträger sind - allerdings nicht mehr von der jeweiligen Datei sichtbar gemacht werden.

So lange die betreffenden Sektoren oder Bereiche des Datenträgers nicht erneut zum Speichern von Daten genutzt werden - was in der Regel eine ganze Weile dauert -, lassen sich die Informationen mit Spezial-Software finden und rekonstruieren.



FonePaw rekonstruiert die Daten automatisch

Mit Datenretungs-Tools wie [FonePaw Datenrettung](#) lassen sich gelöschte Dateien wiederherstellen. Das funktioniert sowohl unter MacOS als auch unter Windows. Als Benutzer muss man gar nicht viel tun: Einfach die Software laden und starten. Danach das Laufwerk angeben, das die gelöschten Dateien und Dokument enthält. Danach begibt sich die Software auf die Suche. Alle entdeckten gelöschten Ordner, Dokumente und Dateien werden angezeigt - und können auf Wunsch auch rekonstruiert werden. Das gelingt keineswegs immer, aber doch erstaunlich häufig.

Mir zum Beispiel passiert es immer wieder, dass Videos versehentlich gelöscht werden. Beim Umgang mit umfangreichen Bild- und Videomaterial ist das kein Wunder. FonePaw hat spezielle Funktionen, mit denen sich [gelöschte Videos wiederherstellen](#) lassen.

Ganz wichtig ist in solchen Situationen: Hat man bemerkt, dass wichtige Dateien oder Dokumente verloren sind, sollten auf dem betreffenden Speichermedium nichts mehr gespeichert werden. Am besten sofort alle anderen Arbeiten beenden, damit keine Daten mehr gespeichert werden - das bedeutet nämlich ein Risiko, dass die verloren gegangenen Daten überschrieben werden. Anschließend sofort das Rettungs-Tools aufrufen und starten und die Rettungsaktion starten!

Wo ist der Weihnachtsmann?

Nun ist es wieder soweit: Der Weihnachtsmann - international als Santa Claus oder liebevoll einfach nur Santa bekannt - ist auf dem Weg, die kleinen und großen Kinder auf der Welt mit seinen Geschenken zu bedenken. In den vergangenen Jahren hat es sich eingebürgert, den Weg über die Erde zu verfolgen. Wir zeigen Ihnen zwei Varianten davon.

Der [Google Santa Tracker](#) ist eine mobil optimierte Webseite, auf der der Weg des Weihnachtsmanns angezeigt wird. Die Seite funktioniert am besten auf einem Smartphone. Google optimiert die Darstellung automatisch auf den kleinen Bildschirm. Damit haben Sie die aktuelle Position des Weihnachtsmannes wie auch die Orte, die er schon besucht hat, immer dabei.



Noch schöner hat NORAD, das North American Aerospace Defense Command, das Ganze aufgemacht. Der [Offizielle NORAD Santa Tracker](#) ist ab dem 23.12. spätabends online. Durch Sponsoring von US-amerikanischen und kanadischen Firmen finden Sie auf der Seite nicht nur eine Karte. Viele Geschichten, Musikstücke und Bilder runden die Weihnachtserfahrung auf der Seite ab.



Viel Spaß!

Schutz vor Schädlingen im WLAN: Bitdefender Home Scanner

Ein WLAN zu schützen, ist auf den ersten Blick eine einfache Aufgabe. Den Router schotten Sie so weit es geht ab, das WLAN mit einem langem, kaum merkbaren Kennwort verschlüsselt und die SSID am besten noch verborgen. So kann niemand, der dort nichts zu suchen hat, in Ihr WLAN gelangen und Daten stehlen. Wie so oft ist das eigentliche Problem oft ein Innentäter. Nicht ein Mitglied Ihres Haushalts, sondern ein Gerät, das infiziert ist und irgendetwas Böses versucht. Wir zeigen Ihnen eine kostenlose Lösung!

Auf Ihren normalen Geräten haben Sie meist Virens Scanner. Regelmäßig aktualisiert schützen die vor bekannter Malware. In letzter Zeit erfolgen aber immer mehr gezielte Angriffe auf Geräte im Netzwerk. Kameras, Rauchmelder, Sprachassistenten: Auch vor Netzwerkfestplatten machen die Angreifer nicht Halt, wie die [QSnatch-Malware](#) eindrucksvoll zeigt. Für IoT-Geräte und andere "Nicht-PCs" gibt es leider keine Virens Scanner, und so bleibt nur die Analyse des Netzwerkverkehrs auf Auffälligkeiten.

The screenshot shows the Bitdefender Home Scanner interface. At the top, it displays the network name 'WLAN-Netzwerk 'WOPPC_Speed_2'' with 31 devices found. A toggle for 'AUTOMATISCHE GERÄTEERKENNUNG' is turned on. Below this is a search bar and a table of devices.

GERÄT	LETZTER SCAN	STATUS
Nest Protect smoke detector 192.168.0.42	Letzter Scan Nie	PRÜFUNG >
Onkyo speakers 192.168.0.102	Letzter Scan Heute	KEINE RISIKEN GEFUNDEN >
Onkyo speakers 192.168.0.106	Letzter Scan Heute	KEINE RISIKEN GEFUNDEN >
Andreas' Philips Hue smart bulbs 192.168.0.20	Letzter Scan Heute	KEINE RISIKEN GEFUNDEN >
NETGEAR device 192.168.0.111	Letzter Scan Heute	KEINE RISIKEN GEFUNDEN >
NETGEAR device 192.168.0.67	Letzter Scan Heute	KEINE RISIKEN GEFUNDEN >

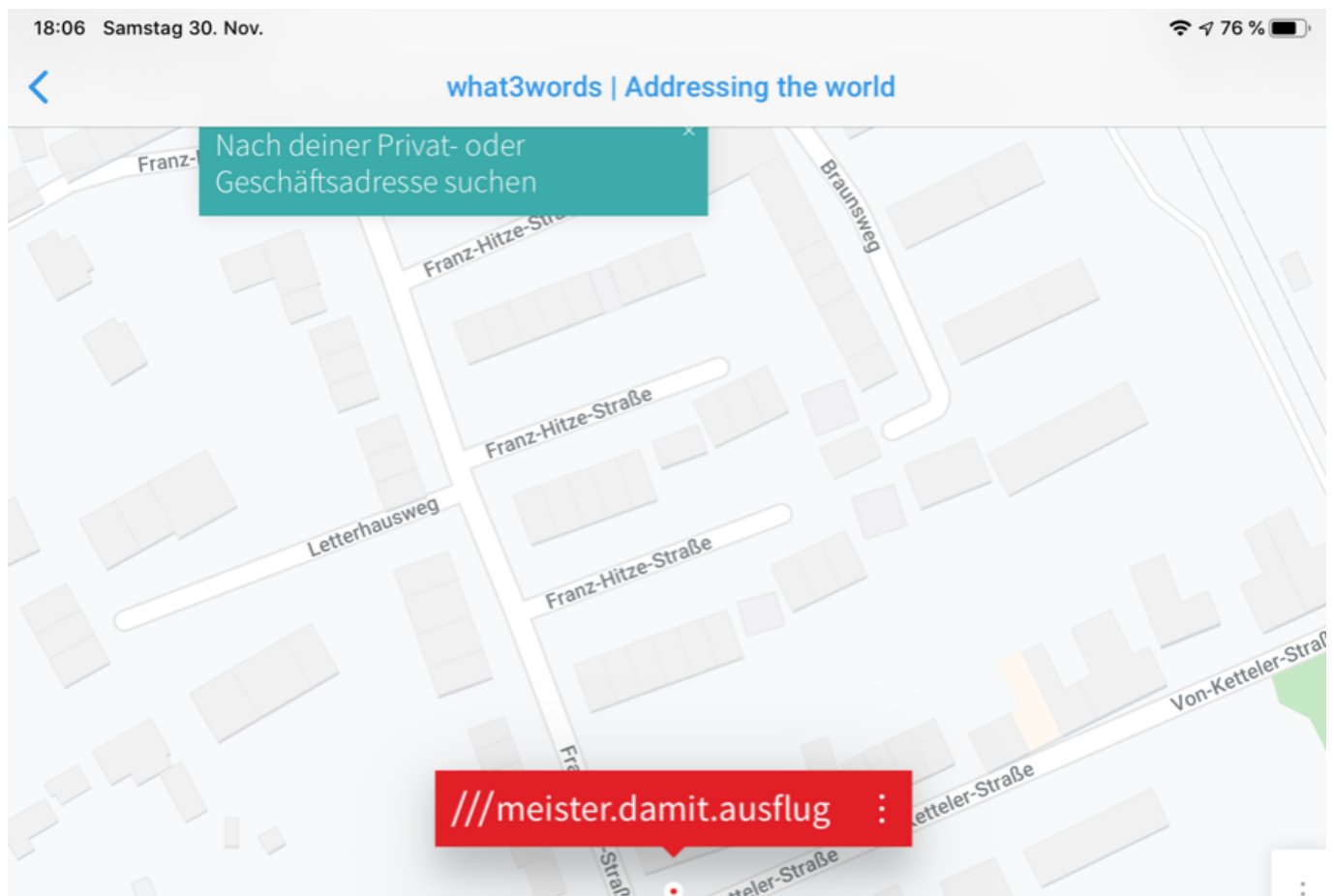
Der Antiviren-Software-Hersteller Bitdefender bietet mit dem kostenlosen [Home Scanner](#) ein Programm an, das Ihr Netzwerk überwacht. Der zusätzliche Vorteil des ersten Scans: Jeder IP wird ein Produkt zugewiesen. In der Übersicht können Sie also erkennen, welches Gerät sich hinter einer IP-Adresse verbirgt. Danach bekommen Sie das Ergebnis für jedes Gerät angezeigt, idealerweise **Keine Risiken gefunden**. Sollte noch ein unnatürliches Verhalten erkannt worden sein, dann liefert Ihnen der Home Scanner dafür mögliche Lösungsansätze.

Das Programm bietet zwar keine absolute Sicherheit, aber zumindest einen guten Überblick über Gefahren in Ihrem WLAN.

Geositionen einfacher merken: What3Words

Wenn Sie sich unter Freunden verabreden wollen, dann bekommen Sie im Idealfall eine Adresse, die Straße, Hausnummer und Ort besteht. Viele Informationen, die auf Grund der Eigennamen schwierig zu merken sein können. Im weniger idealen Fall ist der Treffpunkt mitten in der Pampa und Sie bekommen nur eine Adresse aus Längen- und Breitengrad besteht. Zahlenkolonnen, die komplett nicht zu merken sind. Aber es gibt eine Alternative.

[What3Words](#) ist ein kostenloser Dienst, der einen einfachen Ansatz verfolgt: Jede Adresse der Welt lässt sich aus einer Kombination aus drei Worten darstellen. Und das auch noch in den Sprachen, die Sie brauchen: Rufen Sie die Webseite aus Deutschland aus, dann wird die Adresse mit deutschen Wörtern gebildet, rufen Sie sie aus England aus, dann eben in Englisch. Der Vorteil: Das menschliche Gehirn schafft es, aus diesen Worten einen Satz zu bilden, den Sie sich einfach merken können! Einfacher, als eine Adresse oder eine Zahlenkombination.



Klicken Sie auf **Finde Deine Dreiwortadresse**, dann bewegen Sie die Karte zu der Adresse, die Sie weitergeben möchten. Oder geben Sie im Suchfeld die gesuchte Adresse ein. Jedes Quadrat in der Karte hat eine eigene Adresse. Somit können Sie sogar noch ein wenig variieren, um die für Sie am besten merkbare Dreiwortadresse herauszusuchen.

Der Empfänger der Adresse kann die Dreiwortadresse eingeben und bekommt die damit verbundene Position angezeigt.

Automatische Synchronisationsjobs auf Netzwerkfestplatten

Ein Netzwerkspeicher (Network Attached Storage, NAS) ist eine Sicherung für die Daten. Diese liegen im Netzwerk, meist über RAID-Formate geschützt und damit auch bei Ausfall einer oder zweier Festplatten immer noch verfügbar. Das nützt aber nicht, wenn das NAS gestohlen wird oder bei einem Brand oder Wasserschaden komplett ausfällt. Sinnvoll also, die wichtigsten Daten vom NAS auf USB-Festplatten zu sichern. Wir zeigen Ihnen, wie.

Jeder NAS-Hersteller hat für seine Systeme einen eigenen App-Store, in dem Apps für das NAS angeboten werden. Dort findet sich auch diverse Sicherungssoftware. Eine davon ist [Hybrid Backup Sync](#). Um einen neuen Synchronisationsjob anzulegen, starten Sie die App auf dem NAS. Die USB-Festplatte sollten Sie bereits angeschlossen haben.




Klicken Sie auf **Synchronisierung > Erstellen**, dann entscheiden Sie sich, ob Sie eine Zwei-Wege-Synchronisierung (Abgleich der Daten zwischen Quelle und Ziel) oder eine Ein-Wege-Synchronisierung (reine Datensicherung von Quelle zu Ziel) wollen.

Aufträge

Meine Aufträge
Eingehende Aufträge
Lokal: 3 Rem

Zeigen Sie Details zu vorhandenen Aufträgen an.

▶ Start
✕ Stoppen
🗑️ Löschen

<input type="checkbox"/>	Typ	Auftragsname	Quelle/Ziel	Zeitplan	Status
<input type="checkbox"/>	 Synchronisi...	Serien	Quelle: qnap2ofppc.myqnapcloud.co... Ziel: qnap2ofppc.myqnapcloud.com -...	Wöchentlich: Monta...	✔ Erfolgreich 2019/11/25 22:22
<input type="checkbox"/>	 Synchronisi...	FLACsBilder	Quelle: qnap2ofppc.myqnapcloud.co... Ziel: qnap2ofppc.myqnapcloud.com -...	Wöchentlich: Dienst...	🔄 Aktiv...85% <div style="width: 85%; background-color: #007bff; height: 10px;"></div>
<input type="checkbox"/>	 Synchronisi...	Backup Datalogger	Quelle: qnap2ofppc.myqnapcloud.co... Ziel: qnap2ofppc.myqnapcloud.com -...	Wöchentlich: Mittwo...	🔄 Aktiv...45% <div style="width: 45%; background-color: #007bff; height: 10px;"></div>

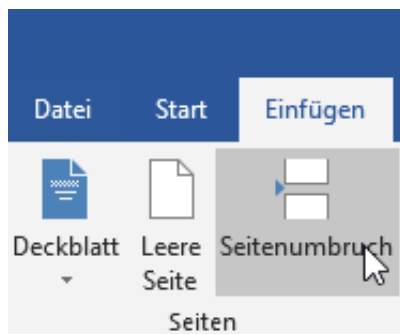
Als nächstes müssen Sie das Ziellaufwerk festlegen. Lassen Sie sich nicht verwirren: Die externe Festplatte erscheint hier nicht als Eintrag. Sie findet sich nur unter dem Eintrag **Lokales NAS**, dort können Sie dann das Laufwerk und das gewünschte Verzeichnis auswählen. Legen Sie nun den Quell- und den Zielordner fest. Sie können bei der Vergabe des Zielordners auch direkt einen neuen Ordner anlegen, indem Sie auf das Ordnersymbol mit dem Plus klicken.

Als Letztes legen Sie unter **Zeitplan** fest, ob der Job einmalig, nach einem anderen Job oder regelmäßig ausgeführt werden soll. Den Rest übernimmt Ihr NAS automatisch, ohne Ihren Benutzereingriff.

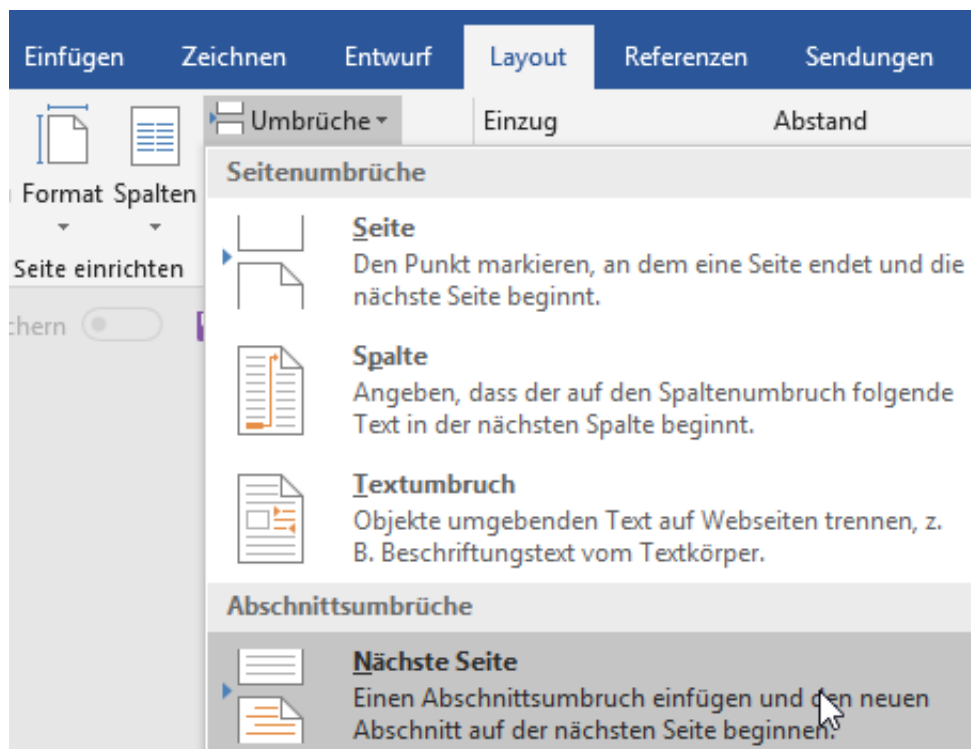
Seiten in Word wechselnd ins Hoch- und Querformat bringen

Word ist das Programm zur Erzeugung, Bearbeitung und Verwaltung von Dokumenten. Eigentlich so intuitiv, als würden Sie mit Papierblättern arbeiten und Ihre Texte dort hinein schreiben. Wo aber das Blatt Papier mal eben so ins Hoch- oder Querformat drehbar ist, ist das bei Word ein wenig schwieriger: Im Standard dreht Word das ganze Dokument ins das neue Format, statt nur einzelne Seiten. Mit einem kleinen Trick bekommen Sie das in den Griff.

Das Zauberwort dafür ist Umbrüche. In Word können Sie ein Dokument entweder manuell oder automatisch auf eine neue Seite oder einen neuen Abschnitt wechseln lassen. Der manuelle Umbruch ist dann wichtig, wenn Sie an einer bestimmten Stelle auf eine neue Seite oder einen neuen Abschnitt wechseln wollen. Das Risiko: Wenn Sie den Text davor verändern und dabei verlängern oder verkürzen, dann bleibt der Umbruch trotzdem an der von Ihnen festgelegten Stelle. Auch wenn er da nicht mehr passt!



Fügen Sie einen manuellen Seitenumbruch ein, indem Sie auf **Einfügen > Seitenumbruch** klicken. Wenn Sie allerdings auf der folgenden Seite das Seitenformat (von Hoch- in Querformat oder umgekehrt) ändern wollen, dann ist der Seitenumbruch die falsche Wahl. Verwenden Sie dafür den Abschnitt-Umbruch. Dazu klicken Sie auf **Layout > Nächste Seite**.



Zwischen Abschnittsumbrüchen kann das Seitenformat problemlos angepasst werden, ohne das restliche Dokument zu beeinflussen.

Animierter Weihnachtstanz mit Ihren Gesichtern: XMAS Dance für iOS

Witzige Memes und Bilder haben in der Weihnachtszeit Hochkonjunktur. Nichts ist schöner, als den Lieben einen personalisierten Weihnachtsgruß zukommen zu lassen. Nur hat man eigentlich alles schon gesehen: Das Gruppenbild, die geschmückten Haustiere, der Weihnachtsbaum in der Totalen oder Detailansicht: Zeit für etwas Neues! Die kostenlose App [XMAS Dance](#) für iOS ist eine nette Alternative!

Nach Installation der App auf Ihrem iPhone müssen Sie ein wenig Geduld mitbringen: In der kostenlosen Version bekommen Sie so einige Werbung zu sehen. Die bekommen Sie weg, indem Sie auf das Kreuz oben rechts in der Anzeige klicken.



Tippen Sie auf **Start**, dann können Sie als erstes das Design der Mütze der Figuren auswählen: klassisch rot oder fesch gestreift stehen zur Auswahl. Wählen Sie dann das Geschlecht der Figur.



Nun können Sie entweder ein in Ihren Fotos gespeichertes Bild auswählen oder mit der Kamera des Smartphones ein neues machen. Das Bild muss nun so in die Schablone eingepasst werden, dass die Ohren richtig sitzen. Bewegen, drehen und zoomen Sie so lange, dass das passt.

Fügen Sie so lange Figuren hinzu, bis alle Teilnehmer Ihres virtuellen Weihnachtstanzes auf dem Bildschirm sind. Dann wählen Sie den Hintergrund und die mittanzenden Figuren (wie Schneemänner oder Rentiere) aus. Schon tanzen alle mit Ihren Gesichtern gemeinsam. Leiten Sie die Animation an die gewünschten Empfänger weiter. Schon haben Sie einen persönlichen Weihnachtsgruß!

Vorsicht bei unbekanntem Gruß-E-Mails

Weihnachten, Ostern, Feiertage: Glück- und Segenswünsche per E-Mail haben Hochkonjunktur. Leider senden Ihnen nicht nur wohlmeinende Bekannte Grüße, sondern auch Menschen, die Ihnen Böses wollen. Im Anhang der Mails finden sich dann vermeintliche Grußkarten, die aber in Wirklichkeit Schadsoftware enthalten. Schnell weicht die Feiertagsfreude dann dem Stress, Ihren PC wieder ans Laufen zu bekommen und den Schaden zu begrenzen. Das muss nicht sein!

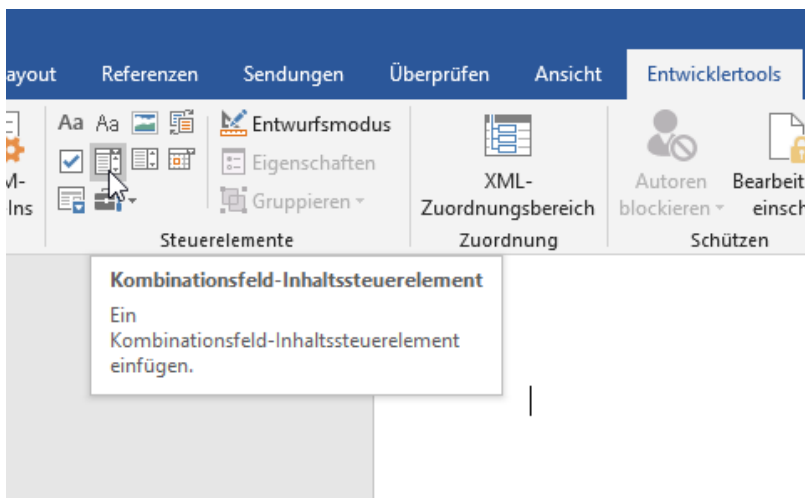
Gerade in den Zeiten, in denen die Zahl der E-Mails hoch ist, klicken Sie schneller auf Anhänge und Links. Nehmen Sie sich gerade jetzt ein wenig mehr Zeit! Mit wenigen Schritten können Sie die meisten Fallen vermeiden:

- Kontrollieren Sie den Absender der E-Mail. Auch wenn dort ein bekannter Name steht, platzieren Sie den Mauszeiger darüber. Einen kleinen Moment dauert es, dann zeigt Ihnen Outlook weitere Informationen zum Absender an. Wenn dort beispielsweise eine komische E-Mail-Adresse steht, löschen Sie die E-Mail.
- Öffnen Sie keine Dokumente von unbekanntem Absendern. Auch in Word- oder PDF-Dateien kann sich Schadsoftware befinden.
- Klicken Sie auf keine Links in einer E-Mail, über deren Ursprung Sie sich nicht absolut sicher sind. Hinter Links in gefälschten E-Mails stehen oft Webseiten mit Schadsoftware, teilweise auch täuschend echt aussehende Webseiten, die Ihre persönlichen Daten abgreifen wollen.
- Aktualisieren Sie unbedingt regelmäßig Ihre Antiviren-Software! Wenn trotz aller Vorsicht doch einmal ein Virus durchkommt, dann ist ein aktueller Virenschutz das letzte Bollwerk vor einer Infektion!

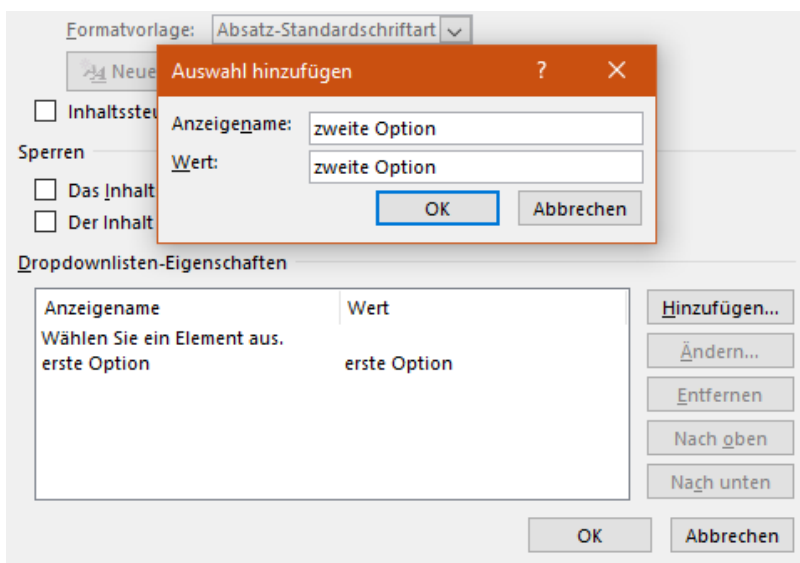
Erstellen von Auswahllisten in Word

Wenn Sie ein Formular in Word entwerfen, dann ist es oft so, dass Sie darin bestimmte Formularfelder wollen. Statt frei Text einzutragen soll der Ausfüllende einfach nur aus einer Liste vorgefertigter Optionen eine Auswahl treffen. Dazu erlaubt Word das Einrichten von Drop Down-Boxen, die genau diese Auswahlmöglichkeiten anzeigen. Wir zeigen Ihnen, wo!

Diese Funktion hat Word gut versteckt: Bewegen Sie den Cursor an die Position im Text, an der das Auswahlfeld erscheinen soll. Dann klicken Sie auf die Registerkarte **Entwicklertools**. Suchen Sie mit dem Mauszeiger und dem daran erscheinenden Hilfetext das Symbol für **Kombinationsfeld-Inhaltssteuerelement** und klicken Sie darauf.



Lassen Sie den Cursor in dem neuen Feld stehen und klicken Sie dann auf **Entwicklertools > Eigenschaften**. Klicken Sie dann auf **Hinzufügen** und geben Sie die erste Listenposition der Auswahlliste ein. Machen Sie das für alle Einträge in der Liste erneut.



Wenn Sie zwischenzeitlich feststellen, dass die Reihenfolge der Einträge nicht stimmt, dann

können Sie das korrigieren. Klicken Sie einen umzuordnenden Eintrag an, dann klicken Sie auf **Nach oben** oder **Nach unten**. Schließen Sie die Anlage der Liste durch einen Klick auf **OK** ab. Die Werte sind nun in der Auswahlliste gespeichert. Im Dokument klicken Sie nun auf den Pfeil nach unten in der Liste und wählen dann einen Wert aus. Nur die angegebenen Werte sind zulässig.