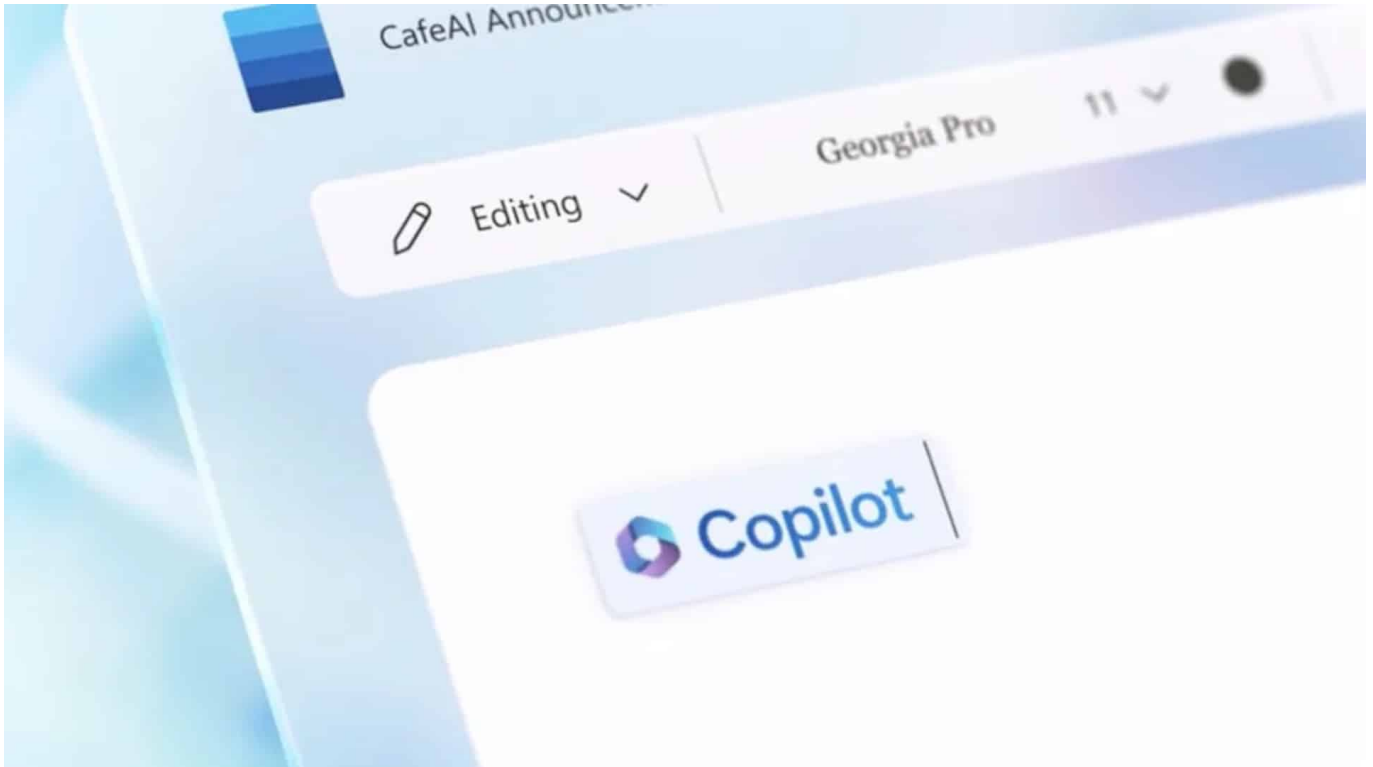


A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark and out of focus.

Schieb Report

Ausgabe 2024.15

Copilot Pro für iOS und Android



Copilot als Microsoft-KI für Office und alle Programme darum herum kommen auf immer mehr PCs. Aber auch auf dem Smartphone könnt ihr viele Funktionen nutzen, vor allem, wenn ihr die Pro-Version von Copilot verwendet!

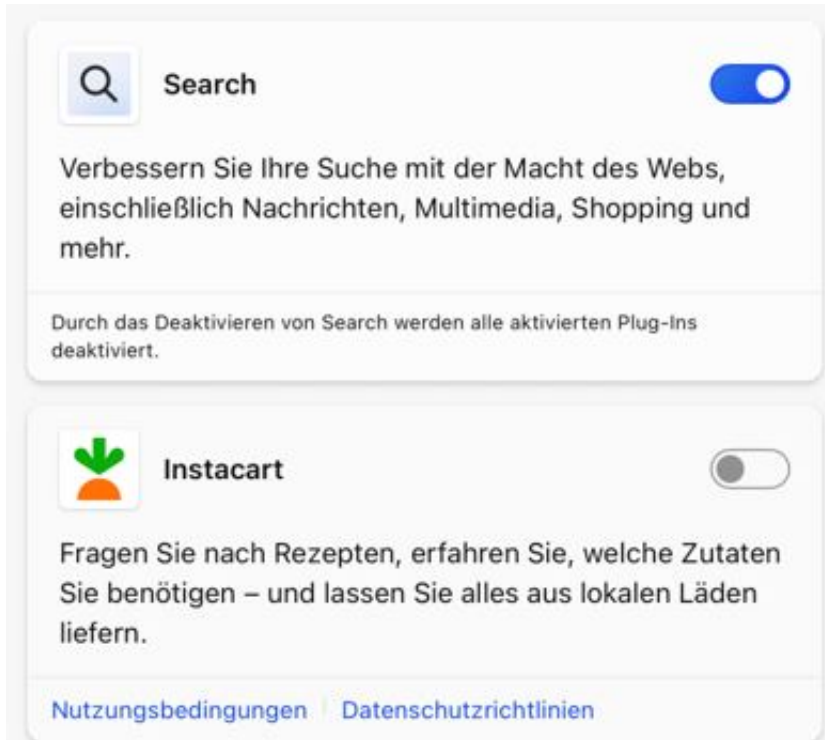
Wie bei den Office-Anwendungen und im Internet unterscheiden sich die Free- und die Pro-Version durch die Zahl und Komplexität der Funktionen, mehr dazu lest ihr [hier](#). Auch bei der Copilot-App gibt es einige besondere Funktionen, die der Pro-Version vorbehalten sind:

Plugins bei Copilot Pro

Wenn ihr die Pro-Version nutzt, dann könnt ihr den reinen Chatbot noch anreichern durch Plugins, die die Antworten mit weiteren Informationsquellen anreichern können.

- Tippt oben rechts in der App auf die drei Punkte, dann auf Plug-Ins.
- Copilot zeigt euch nun die verfügbaren Plug-Ins an. Im Standard können bis zu drei aktiviert werden, in dem ihr den Schalter neben dem jeweiligen [Plug-In](#) aktiviert.


- Einige Plug-Ins verlangen, dass sie exklusiv aktiviert werden, so zum Beispiel die Suche. In einem solchen Fall werden bei der Aktivierung des Plugins alle anderen deaktiviert.



Der Urlaubsplaner

Wolltet ihr schon immer mal eine tolle Reiseplanung machen oder neue Orte entdecken? Dann kann euch der [Copilot](#)-Reiseplaner helfen:

- Tippt in der App oben links auf euer Kontobild, dann im sich öffnenden Menü auf **Vacation Planner** (der Name ist immer noch englisch, die Bedienung und die Ergebnisse aber deutsch!).
- Gebt eine möglichst genaue Vorgabe für die Reise beispielsweise „Wo sieht man Nordlichter? Plane mir eine Reise mit dem Auto“.
- Der Vacation Planner sucht nun im ersten Schritt nach passenden Orten. Wenn ihr in der Anfrage schon eine Reiseart angegeben habt, dann müsst ihr im nächsten Schritt festlegen, welchen der möglichen Orte ihr besuchen wollt. Gebt den ins Eingabefeld ein.
- Der Vacation Planner stellt vielleicht noch die eine oder andere klarstellende Frage, um Eure Anfrage besser zu verstehen.
- Am Ende bekommt Ihr eure Reisebeschreibung. Gute Reise!

 **Sie**

wo sieht man Nordlichter? Plane mir eine Reise mit dem Auto

 **Vacation planner**

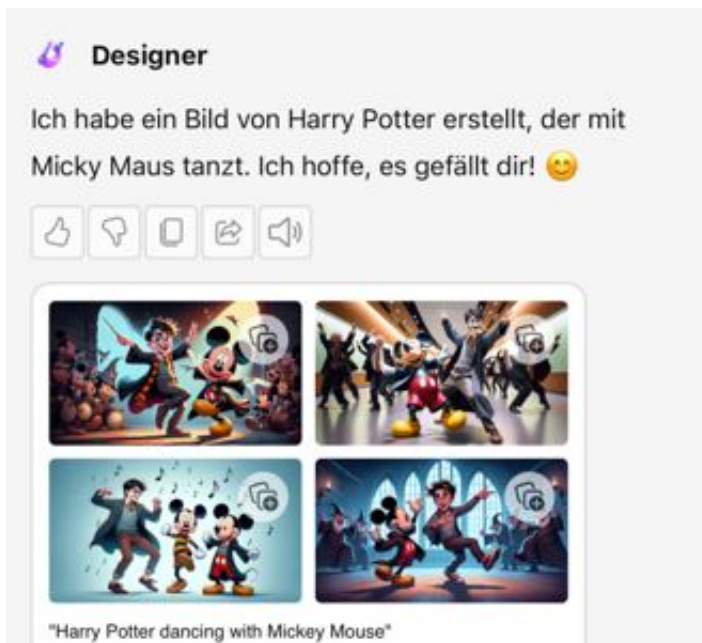
Die Nordlichter, auch bekannt als Aurora Borealis, sind ein faszinierendes Naturschauspiel, das man am besten in Regionen nahe des nördlichen Polarkreises beobachten kann. Zu den besten Orten, um die Nordlichter zu sehen, gehören:

Unterwegs Bilder erzeugen mit Dall-E/Designer

Fragen an eine KI zu stellen ist unterwegs kein Problem: Ob ihr eine Nachricht schreibt oder eine Anfrage an Copilot oder ChatGPT stellt, unterscheidet sich vom Aufwand her kaum. Ganz anders stellt sich die Situation dar, wenn ihr ein Bild benötigt, das ihr nicht so einfach schießen könnt und auch nicht in der Mediathek/im Fotoalbum habt. Dafür gibt es den Microsoft Designer, der [Dall-E](#) nutzt. Auf dem PC über die Webseite wunderbar bedienbar, auf dem Smartphone eher schwierig. Das macht aber nichts, denn die Pro-Version der Copilot-App hat eine Funktion, mit der ihr darüber Bilder in der App erzeugen könnt:

- Tippt in der App oben links auf euer Kontobild, dann im sich öffnenden Menü auf **Designer**.
- Gebt nun eine möglichst genaue Beschreibung des Bildes ein, das ihr erzeugen möchtet.
- Der Designer kann auf viele Bildquellen zugreifen. Wo er sich allerdings verweigert: Eine Mischung aus realen Personen und fiktiven Charakteren. „Ein Bild von Barack Obama und Harry Potter“ bekommt ihr nicht. „Ein Bild von Harry Potter, der mit Micky Maus tanzt“ schon.
- Über dem Bild findet ihr eine Symbolleiste, über die ihr die Bilder weiter verwerten könnt. Kopiert es in die Zwischenablage, um es in eine Mail oder ein Dokument einzufügen.
- Klickt auf das Teilen-Symbol, um es an andere Dienste weiterzugeben.

- Wenn das Bild nicht euren Wünschen entspricht, dann klickt unter dem Bild auf **Das ist großartig! Kannst Du noch ein Bild erstellen?**



Offline? So kann ein Leben ohne Internet Dein Wohlbefinden stärken

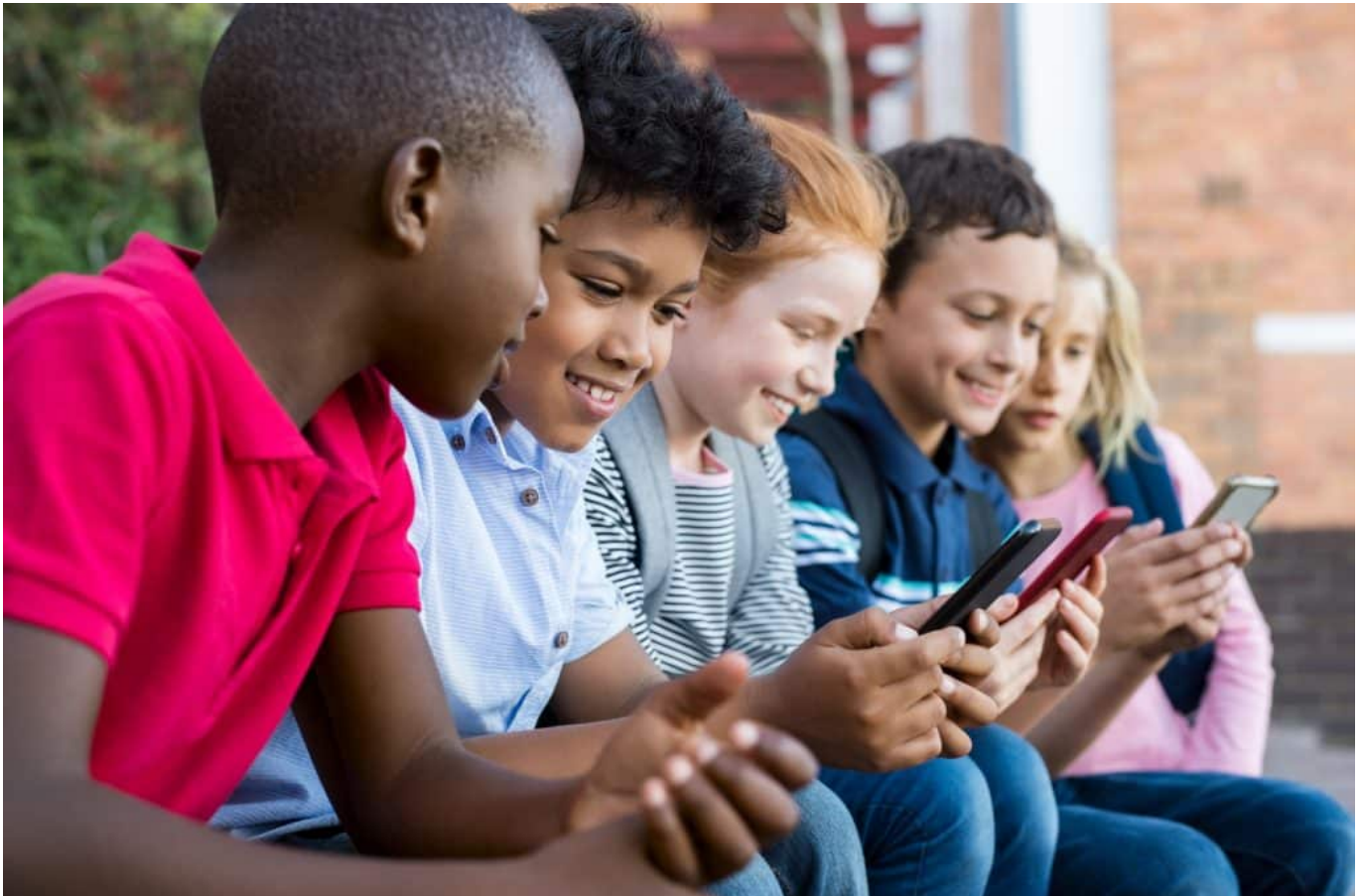


Nach einer aktuellen Statistik nutzen fünf Prozent der 16- bis 74-Jährigen Deutschen kein Internet. Deutschland liegt mit dem Schnitt leicht unter den anderen EU-Staaten.

Die Zahlen sind beeindruckend: Laut Statistischem Bundesamt (die Zahlen wurden gerade veröffentlicht) haben in Deutschland rund 3,1 Millionen Menschen im Alter von 16 bis 74 Jahren noch nie das Internet genutzt. Das sind gut 5 Prozent der Bevölkerung in dieser Altersgruppe.

Ein zweifellos bemerkenswerter Anteil in einer Zeit, in der viele von uns das Internet als unverzichtbaren Teil unseres Alltags wahrnehmen.

Doch gerade in einer zunehmend digitalisierten Welt kann ein Leben abseits des Netzes durchaus Vorteile haben. Lass uns einen genaueren Blick darauf werfen, was ein Leben offline für Dich bedeuten könnte.



Wenn Kids ein Smartphone nutzen, haben Eltern jede Kontrolle verloren

Entschleunigung und mehr Achtsamkeit

Eine der größten Herausforderungen unserer Zeit ist es, in der Flut an Informationen, Benachrichtigungen und ständiger Erreichbarkeit den Überblick zu behalten. Ohne Internet entfällt dieser permanente Reizstrom. Du kannst Deinen

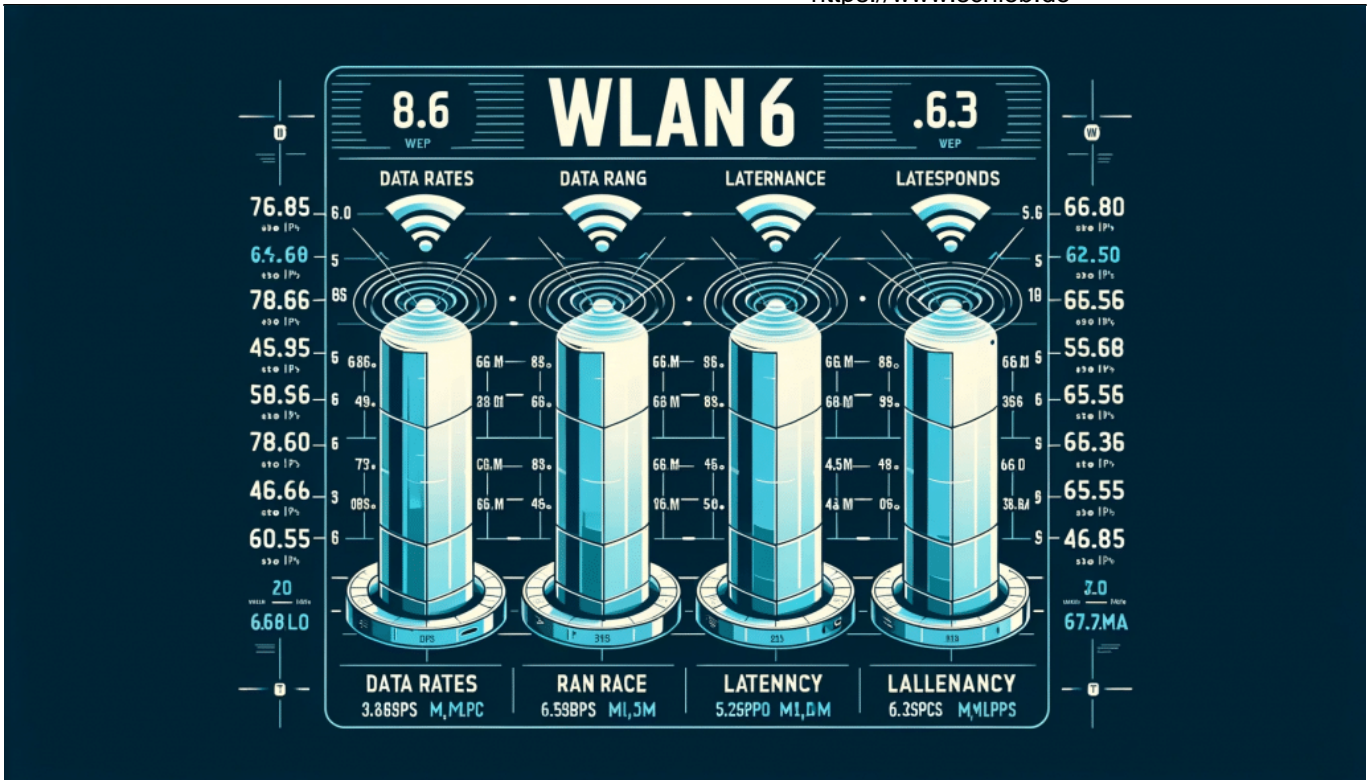
Alltag in Ruhe gestalten, ohne ständig abgelenkt zu werden.

Viele Menschen berichten, dass sie nach einer "digitalen Auszeit" plötzlich viel achtsamer und entspannter durchs Leben gehen. Sie nehmen ihre Umgebung, Mitmenschen und sich selbst bewusster wahr. Statt ständig auf Smartphone oder Laptop zu starren, widmest Du Dich ganz den Dingen, die gerade wichtig sind.

Mehr Zeit für Hobbys und soziale Kontakte

Ein Leben offline bedeutet auch, dass Du Dich von zeitfressenden Online-Aktivitäten wie endlosem Scrollen durch soziale Medien oder stundenlangem Netflix-Bingen verabschiedest. Stattdessen gewinnst Du wertvolle Zeit, die Du für Deine Hobbys, Freundschaften und Familie einsetzen kannst.

Vielleicht entdeckst Du Deine Leidenschaft für Basteln, Kochen oder Sport neu. Oder Du investierst mehr Zeit in persönliche Treffen mit Deinen Liebsten, ohne ständig von Benachrichtigungen abgelenkt zu werden. So stärkst Du Deine sozialen Bindungen auf eine ganz authentische Art und Weise.



Unabhängigkeit und Kontrolle über Deine Daten

In einer Welt, in der viele unserer Aktivitäten digital erfasst und ausgewertet werden, kann ein Leben offline auch ein Gefühl von Unabhängigkeit und Souveränität vermitteln. Du bestimmst selbst, welche Informationen über Dich preisgegeben werden und bist nicht ständig der Gefahr von Datendiebstahl oder Überwachung ausgesetzt.

Gerade in Zeiten, in denen Themen wie Datenschutz und digitale Sicherheit immer wichtiger werden, kann diese Unabhängigkeit ein echter Gewinn sein. Du musst Dir keine Sorgen um Tracking, Manipulation oder Cyberattacken machen und hast die volle Kontrolle über Deine persönlichen Daten.

Weniger Stress und mehr Gesundheit

Zahlreiche Studien belegen, dass ein übermäßiger Konsum digitaler Medien auch negative Auswirkungen auf unsere Gesundheit haben kann. Ständige Erreichbarkeit, Multitasking und die Reizüberflutung können zu Stress, Schlafstörungen und sogar Depressionen führen.

Ohne Internet entfallen diese Belastungsfaktoren. Du kannst Dich voll und ganz auf die Gegenwart konzentrieren, ohne ständig von Benachrichtigungen oder E-Mails abgelenkt zu werden. Dein Körper und Geist können so zur Ruhe kommen und regenerieren. Viele Offline-Fans berichten auch von einem Rückgang von Kopfschmerzen, Verspannungen und Müdigkeit.

Natürlich bringt ein Leben ohne Internet auch Herausforderungen mit sich. Gerade bei der Organisation des Alltags, der Informationsbeschaffung oder der Kommunikation über weite Distanzen kann es Einschränkungen geben. Doch die potenziellen Vorteile für Dein Wohlbefinden und Deine Lebensqualität sollten nicht unterschätzt werden.

Vielleicht ist es ja an der Zeit, Deine persönlichen Grenzen im Umgang mit digitalen Medien auszuloten und Dir bewusst "Offline-Zeiten" zu gönnen. Wer weiß, vielleicht entdeckst Du dadurch eine ganz neue Seite an Dir selbst.

Sicherheit beim Scannen von QR-Codes: Spezial-Apps können schützen



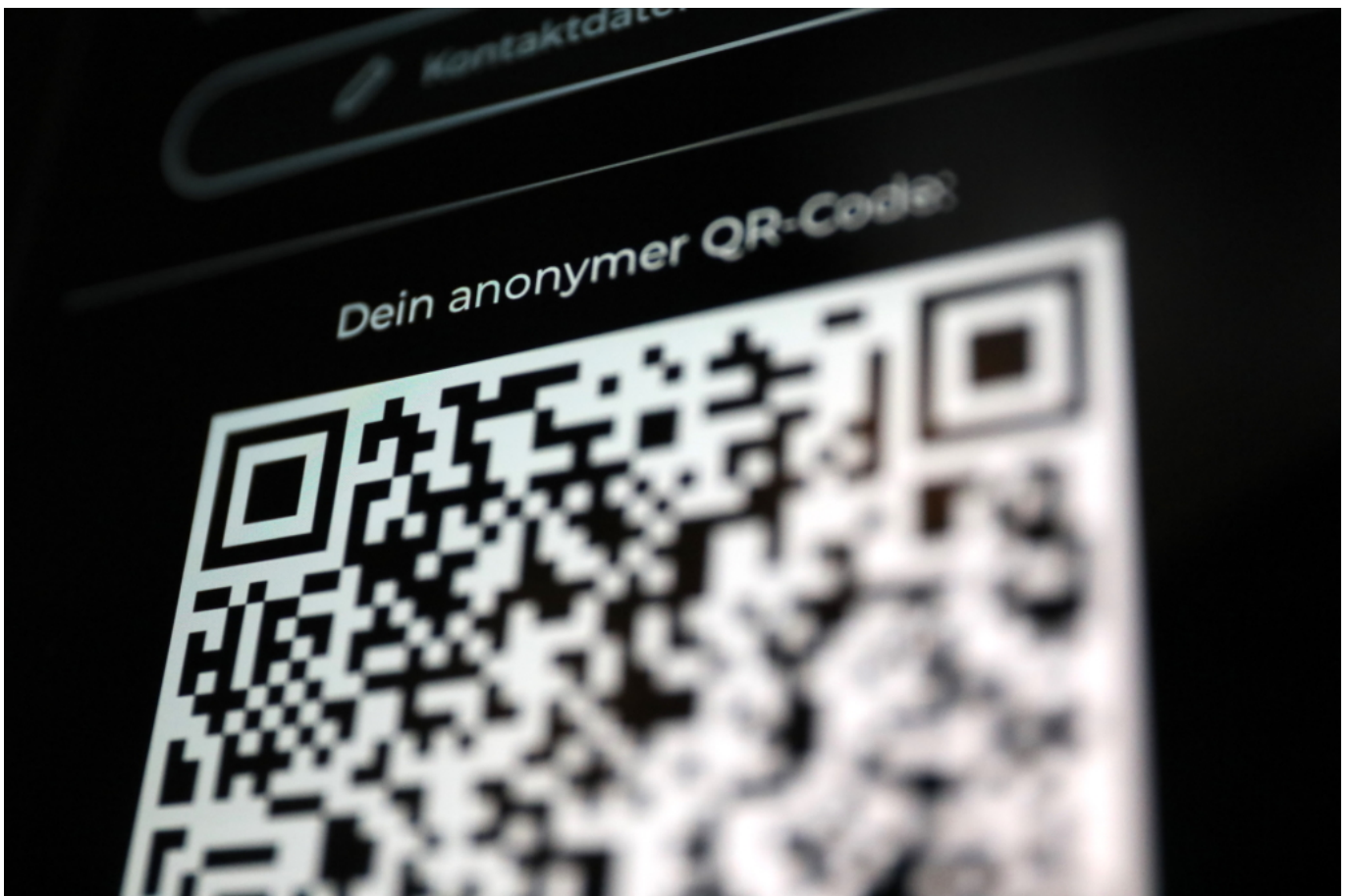
QR Codes sind praktisch. Aber sie können auch eine Falle sein. Leider gibt es hier immer mehr Betrugsversuche. Deshalb: Besser schützen!

QR-Codes sind heute überall: QR-Code scannen, um ins WLAN zu kommen. Oder die Speisekarte im Restaurant oder Biergarten: QR-Code scannen, schon sieht man das Menü. Auch Plakate oder Werbung ist immer häufiger mit QR-Codes versehen. Und im Museum können wir darüber Erläuterungen abrufen.

Doch die kleinen quadratischen Codes bergen auch Gefahren. Cyberkriminelle nutzen sie gerne, um unwissende Nutzer auf betrügerische Websites umzuleiten oder sogar Malware auf deren Geräte zu schleusen.

Wer mag, kann sich vor allzu großen Risiken schützen. Dann scannt man die QR-Codes nicht wie sonst direkt in der Kamera oder im Browser, sondern schaltet eine Sicherheits-App dazwischen.

Zum Glück gibt es spezielle Sicherheits-Apps, die dabei helfen, potenzielle Betrügereien und Stolperfallen zu umgehen.



Wie Sicherheits-Apps QR-Code-Risiken erkennen

Die Hauptaufgabe dieser Apps ist es, die Sicherheit von QR-Codes zu überprüfen, bevor man sie scannt. Dafür greifen sie auf verschiedene Methoden zurück:

- **URL-Analyse:** Die Apps überprüfen, ob die hinter dem QR-Code stehende URL als sicher eingestuft wird. Dafür verwenden sie Datenbanken mit bekannten Malware-Domains oder Phishing-Seiten.
- **Reputation-Checks:** Manche Apps gleichen die URL auch mit Reputationsservices ab, um einzuschätzen, ob es sich um eine vertrauenswürdige Seite handelt.
- **Verhaltensanalyse:** Fortschrittlichere Apps beobachten auch das Verhalten der Website, sobald man sie aufruft. So lassen sich verdächtige Aktivitäten wie Weiterleitung oder Datenabgriff erkennen.

Wenn die App Risiken erkennt, warnt sie den Nutzer umgehend und verhindert so, dass er auf eine gefährliche Seite weitergeleitet wird.

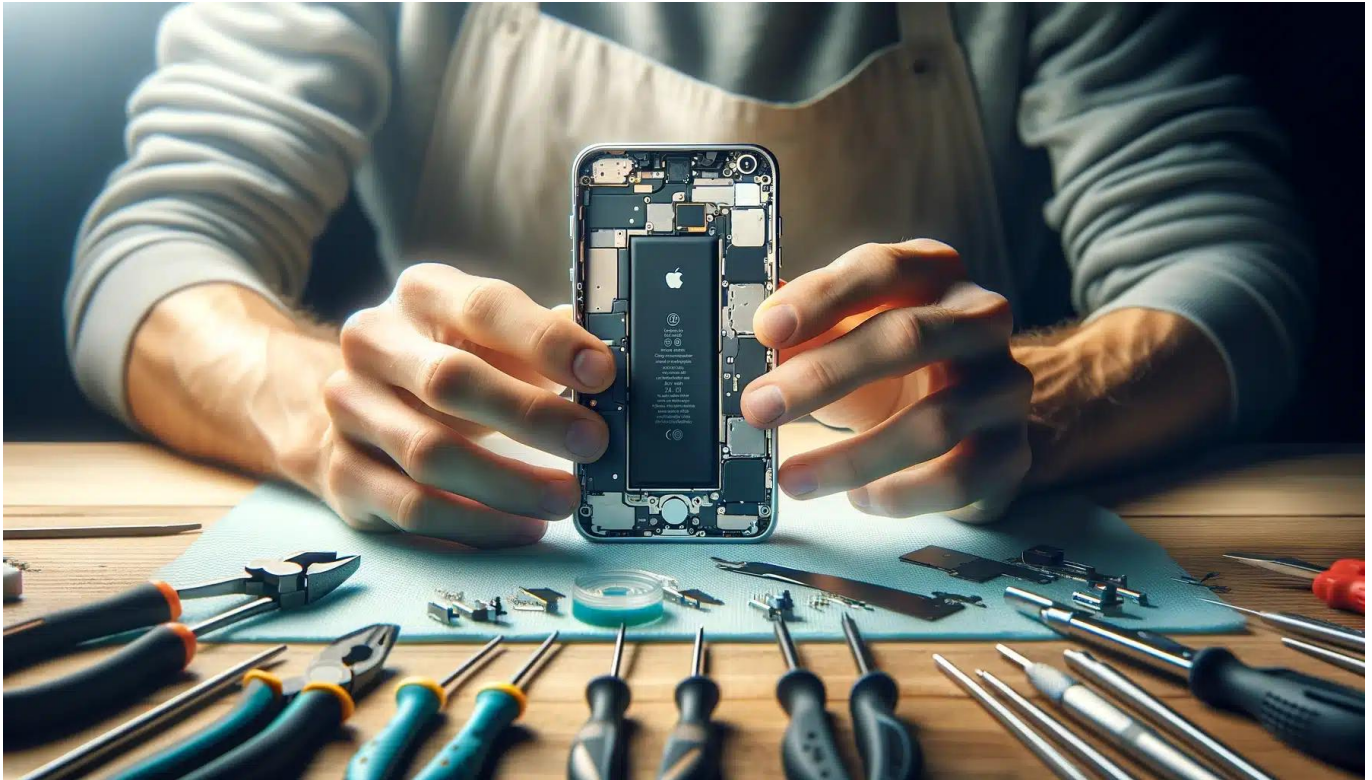
Übersicht der wichtigsten Sicherheits-Apps für QR-Codes.

App	Funktionen
Kaspersky QR Scanner	- URL-Analyse - Reputation-Check - Verhaltensanalyse

App	Funktionen
Norton Mobile Security	<ul style="list-style-type: none">- Echtzeit-Warnung vor Bedrohungen- URL-Analyse- Reputation-Check- Erkennung von Malware-Aktivitäten
McAfee Safe Connect	<ul style="list-style-type: none">- URL-Analyse- Warnung vor bekannten Bedrohungen- Anonymes Surfen nach Scan
Trend Micro Mobile Security	<ul style="list-style-type: none">- URL-Analyse- Verhaltensanalyse- Identifizierung von Phishing-Versuchen
Avast Mobile Security	<ul style="list-style-type: none">- URL-Analyse- Reputation-Check- Erkennung von Schadsoftware

Mit diesen Sicherheits-Apps können Nutzer also deutlich besser einschätzen, ob ein QR-Code vertrauenswürdig ist oder nicht. So lassen sich die Risiken des QR-Code-Scannens deutlich minimieren.

Apple erweitert Reparaturmöglichkeiten um Unterstützung für gebrauchte Originalteile

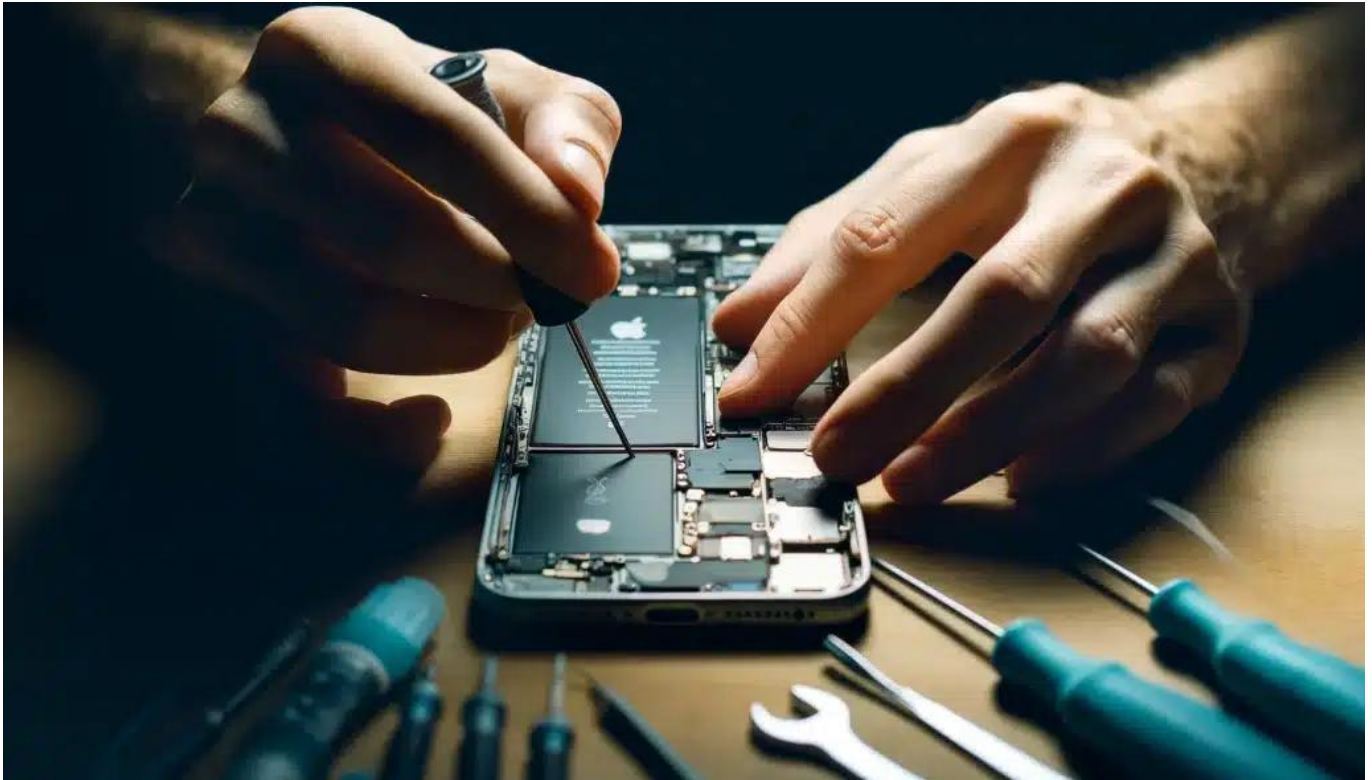


Smartphone kaputt? Oh, das kann kostspielig werden. Apple erweitert die Möglichkeiten zur Reparatur. Künftig können auch gebrauchte Einzelteile für die Reparatur verwendet werden – was die Kosten senkt und die Umwelt schont.

Gute Nachrichten: Apple ermöglicht künftig die Wiederverwendung gebrauchter Teile für iPhone-Reparaturen.

In einem wichtigen Schritt zur Förderung der Nachhaltigkeit hat Apple angekündigt, dass Kunden und unabhängige Reparaturanbieter bald gebrauchte Apple-Originalteile für die Reparatur ihrer iPhones verwenden können. Bislang

war dies nicht möglich.



Auch gebrauchte Ersatzteile lassen sich künftig weiter nutzen

Ab Herbst mehr Möglichkeiten bei der Reparatur

Ab Herbst startet Apple den neuen Reparaturprozess zunächst für ausgewählte iPhone-Modelle. Dabei bleibt der Schutz der Nutzerdaten, der Sicherheit und des Schutzes der iPhones gewährleistet. Gleichzeitig erhalten Verbraucher mehr Möglichkeiten, die Lebensdauer ihrer Geräte zu verlängern und die Umweltauswirkungen von Reparaturen zu minimieren.

Gebrauchte Apple-Originalteile profitieren künftig von derselben Funktionalität und Sicherheit wie neue Teile. Der Prozess, um die Echtheit eines Reparaturteils zu

überprüfen und Informationen darüber zu sammeln, ist entscheidend für den Datenschutz und die Sicherheit.

Apple hat hart daran gearbeitet, die Wiederverwendung sensibler Komponenten wie biometrischer Sensoren für Face ID oder Touch ID zu ermöglichen.

Gestohlene Geräte lassen sich nicht mehr einfach so ausschlachten

Ab Herbst erfolgt die Kalibrierung neuer oder gebrauchter Originalteile direkt auf dem Gerät nach der Installation. Zukünftige iPhone-Versionen werden auch gebrauchte biometrische Sensoren unterstützen. Um den Reparaturprozess zu erleichtern, müssen Kunden und Serviceanbieter bei Reparaturen ohne Austausch des Logikboards künftig nicht mehr die Seriennummer des Geräts angeben.

Darüber hinaus weitet Apple die beliebte Aktivierungssperre auch auf iPhone-Teile aus, um zu verhindern, dass gestohlene Geräte zerlegt und Einzelteile weiterverwendet werden. Wenn ein Reparaturteil von einem anderen Gerät mit aktivierter Sperre stammt, werden die Kalibrierungsmöglichkeiten dafür eingeschränkt.

Mit wachsender Geräteleblichkeit ist es Apple wichtig, dass Besitzer transparenten Zugriff auf die vollständige Reparatur- und Teilhistorie ihres Geräts erhalten. Der Teile- und Serviceverlauf in iOS wird daher um den Hinweis erweitert, ob ein Teil neu oder gebraucht ist.



EU-Kommission fordert: Mindestens fünf Jahre Recht auf Reparatur

Reparaturen werden einfacher

Apples Erweiterung der Reparaturoptionen ist ein weiterer Schritt, um den Zugang zu sicheren und kostengünstigen Reparaturen zu erleichtern.

In den letzten fünf Jahren hat Apple die Zahl der Servicestellen mit Zugang zu Originalteilen, Werkzeugen und Schulungen nahezu verdoppelt. Auch das Self-Service-Reparaturprogramm, das 2022 gestartet wurde, bietet Zugang zu denselben Ressourcen wie in autorisierte Werkstätten.

Wo ist meine Geldbörse? Slimtags statt Airtags



Es gibt wenige Momente, die eine solche Panik hervorrufen wie der vermeintliche Verlust der Geldbörse. Da diese immer kleiner werden, ist es schwer, die mit Ortungschips zu versehen. Da helfen die SlimTags!

Ortung per AirTags

Das Problem bei Ortungs-Chips: Die zu ortenden Gegenstände können sich potenziell überall befinden, wo ihr mit ihnen wart. Dieser Ort kann sich aber ändern, denkt nur an eine im Taxi vergessene Geldbörse. Die Ortung steht und fällt also damit, dass die Position regelmäßig aktualisiert wird, und das möglichst automatisiert.

Apple hat mit den AirTags eine Lösung geschaffen, die eine anonyme Ortung mit jedem geeigneten iPhone erlaubt: Die Geräte erkennen alle [Airtags](#) (ohne den Besitzer zu kennen) und melden diese anonym ans Netzwerk. Ihr könnt dann die Position über die FindMy-App abfragen.

So schön das ist, einen Nachteil haben die AirTags: Sie sind relativ dick und lassen sich in einer schmalen Geldbörse kaum unterbringen. Besser wäre die dünne Form einer Kreditkarte. Die gibt es mit den [SmartTags](#), die verschiedene Hersteller anbieten.

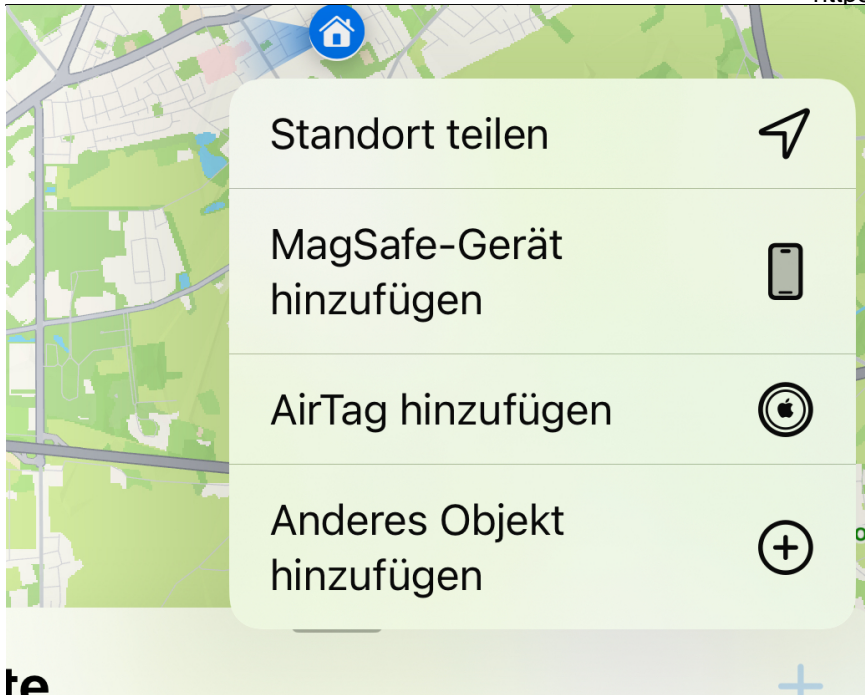
- SmartTags sind über das [FindMy-Netzwerk](#) ortbar und in der App mit ihrer zuletzt gemeldeten Position zu sehen.
- Sie können über die App als verloren gemeldet werden, ebenso kann ein Ton zur Ortung wiedergegeben werden.
- Eine feine Navigation, wie die AirTags sie bieten, ist damit aber nicht möglich.
- Ein SmartTag sollte nicht in einem Kartenfach aufbewahrt werden, das RFID-Schutz hat, dies behindert die Ortung.



Konfigurieren des SmartTags

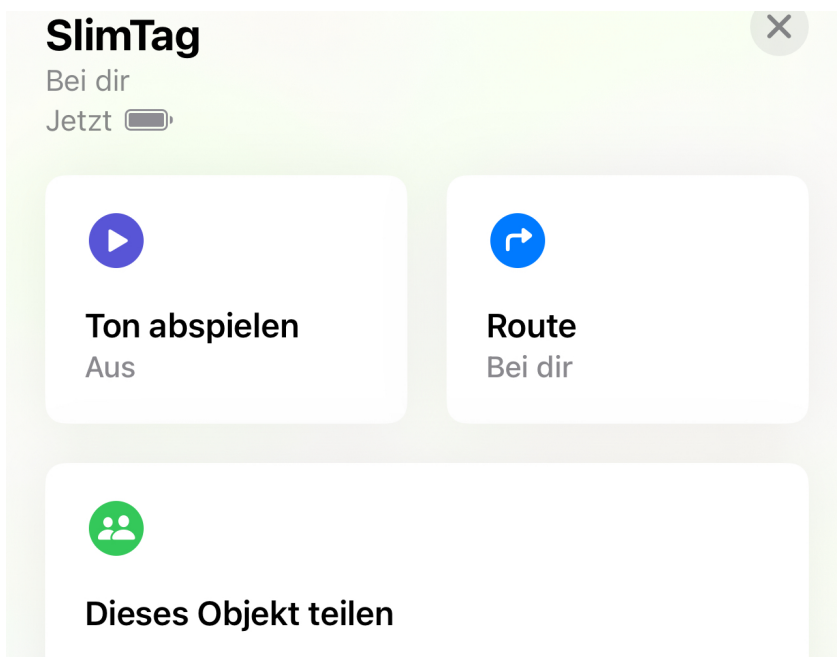
Im Gegensatz zum AirTag ist das SmartTag zwar mit dem Apple FindMy-Netzwerk kompatibel, wird aber nicht automatisch erkannt. Ihr müsst die Kopplung also manuell durchführen:

- Schaltet das SmartTag ein, wie in dessen Anleitung beschrieben.
- Startet auf dem iPhone die FindMy-App, darin tippt unten auf **Objekte**.
- Tippt oben rechts auf das Plus-Zeichen, dann auf **Anderes Objekt hinzufügen**.
- Folgt nun den Anweisungen auf dem Bildschirm eures iPhones und gebt dem SlimTag einen Namen und ein Symbol, mit dem ihr es identifizieren könnt.

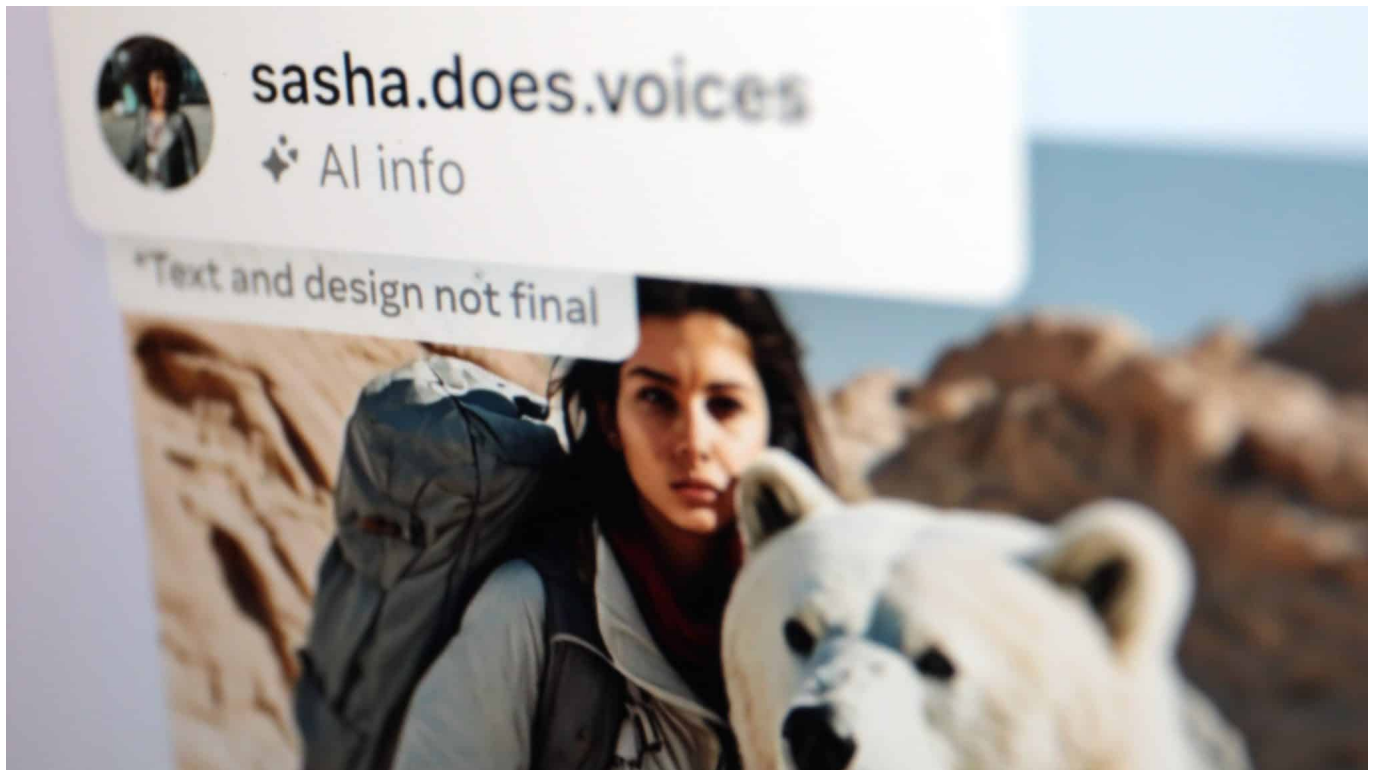


Um das SlimTag jetzt zu orten, startet die FindMy-App und ruft die Objekte auf.

- In der Liste tippt auf den Eintrag den SlimTags, alternativ könnt ihr auch in der Karte auf das Symbol klicken.
- Im Detailfenster könnt ihr nun eine **Route** erstellen lassen oder einen **Ton abspielen**, wenn ihr in der Nähe seid.



"Made with AI": Facebook und Instagram wollen KI-Inhalte künftig kennzeichnen



Wir sehen im Netz immer häufiger Inhalte, die mit KI erstellt wurden – das kann verwirren und irritieren. Deshalb müssen die Plattformen schon bald KI-generierte Inhalte markieren. Der Meta-Konzern hat Maßnahmen angekündigt,

Die Frage müssen wir uns künftig immer häufiger stellen: Echt – oder mit KI gemacht?

Mit dem Fortschritt künstlicher Intelligenz (KI) werden generierte Fotos in Zukunft immer realistischer aussehen, sodass eine Unterscheidung zwischen echten und gefälschten Bildern möglicherweise kaum noch möglich sein wird. Diese Entwicklung könnte erhebliche Auswirkungen auf Social Media haben.

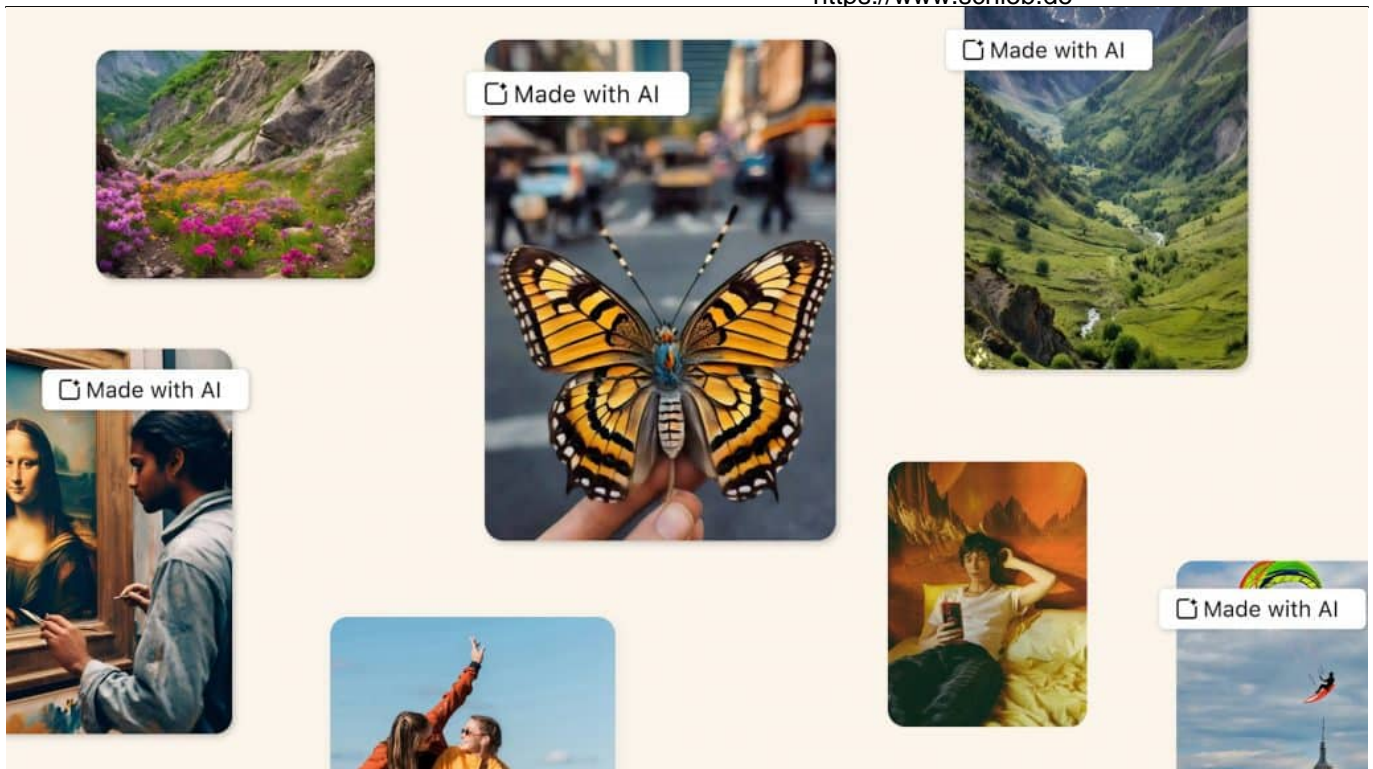
Das Problem

Da visuelle Inhalte einen großen Einfluss auf die Meinungsbildung und Informationsverbreitung haben, könnten gefälschte Fotos, die von KI-Systemen erstellt wurden, die Glaubwürdigkeit und Vertrauenswürdigkeit von Informationen untergraben. Manipulierte Bilder könnten dazu verwendet werden, falsche Ereignisse oder Situationen zu inszenieren, Persönlichkeiten zu diffamieren oder politische Propaganda zu verbreiten.

Dies könnte zu einer verstärkten Verbreitung von Fehlinformationen und einem Anstieg von Desinformation führen, da die Grenzen zwischen Realität und Fiktion verschwimmen. Es wird eine dringende Notwendigkeit geben, Tools und Mechanismen zu entwickeln, um gefälschte Bilder zu erkennen und die Authentizität visueller Inhalte zu gewährleisten, um die Integrität und Zuverlässigkeit von Informationen in der digitalen Ära zu schützen.

Ob auf Facebook, Instagram, Twitter, Youtube oder TikTok: User posten immer mehr Inhalte, die mit KI erstellt wurden. Und es ist keineswegs immer klar, wer die Inhalte hergestellt hat. Der Einsatz von KI wird immer häufiger.

Kein Wunder, denn es gibt immer mehr KI-Systeme, die in der Lage sind, mehr oder weniger auf Knopfdruck Texte, Bilder, Fotos und Audio zu erzeugen (und schon sehr bald auch Videos) zu erzeugen, die täuschend echt aussehen.



Der Meta-Konzern hat schon vorgelegt, wie diese Markierung künftig aussehen wird

KI-Fotos werden zunehmend realistisch

Wenn wir uns Fotos und Bilder anschauen, die KI-Systeme wie Midjourney, Stable Diffusion, Dall-E3 oder Ideogram erzeugen, kann man sagen: Die Ergebnisse werden immer realistischer. Häufig lässt sich kaum noch sagen, ob ein Foto echt ist oder mit KI erzeugt wurde.

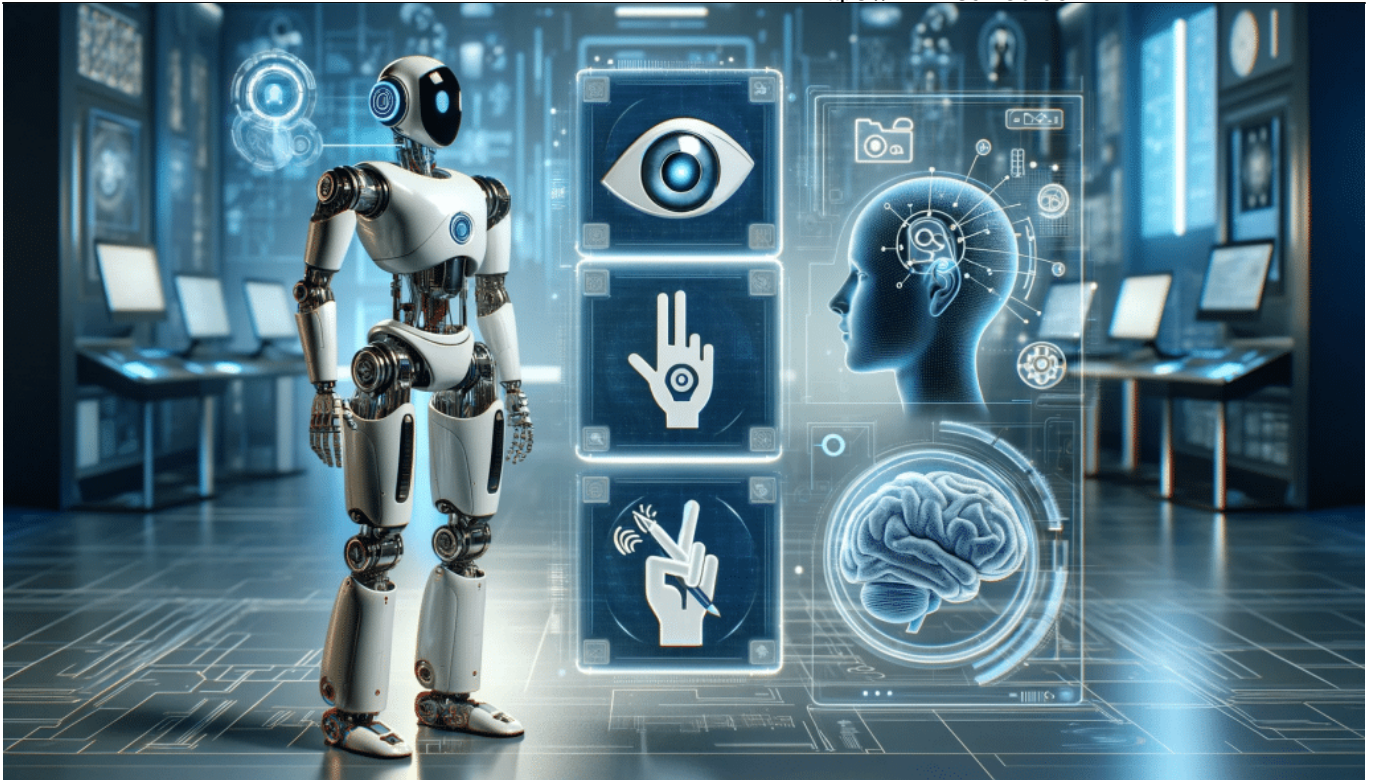
Um Täuschungsversuche und Verwirrungen zu vermeiden, hat der Meta-Konzern deshalb angekündigt, ab Mai auf seinen Plattformen Facebook und Instagram alle Inhalte, die durch KI erzeugt oder manipuliert wurden entsprechend zu kennzeichnen – völlig automatisch.

"Unsere User haben uns gesagt, dass sie Transparenz rund um diese neue Technik schätzen", schreibt Meta-Manager Nick Clegg in dem Blogpost, in dem die geplanten Maßnahmen näher erläutert werden. Sein Motto: KI-Inhalte nicht blocken oder löschen, sondern markieren und so für Transparenz sorgen.

Meta will ab Mai KI-Fotos kennzeichnen

Metas Ingenieure arbeiten daran, fotorealistische Aufnahmen – und nur hier besteht ein Risiko der Verwirrung oder Täuschung – mit geeigneten technischen Maßnahmen (unter anderem mit KI) automatisch zu erkennen und zu kennzeichnen. Viele KI-Systeme, die Fotos erzeugen, markieren die Bilder (unsichtbar) schon jetzt automatisch.

Die meisten KI-Systeme wie Midjourney, Dall-E3, Artbreeder, Dream und viele andere kennzeichnen die erzeugten Bilder sowohl durch entsprechende Angaben in den Metadaten (Exif) der Bilder als auch durch unsichtbare Wasserzeichen. OpenAI hat diese Maßnahme gerade erst Mitte Februar eingeführt.



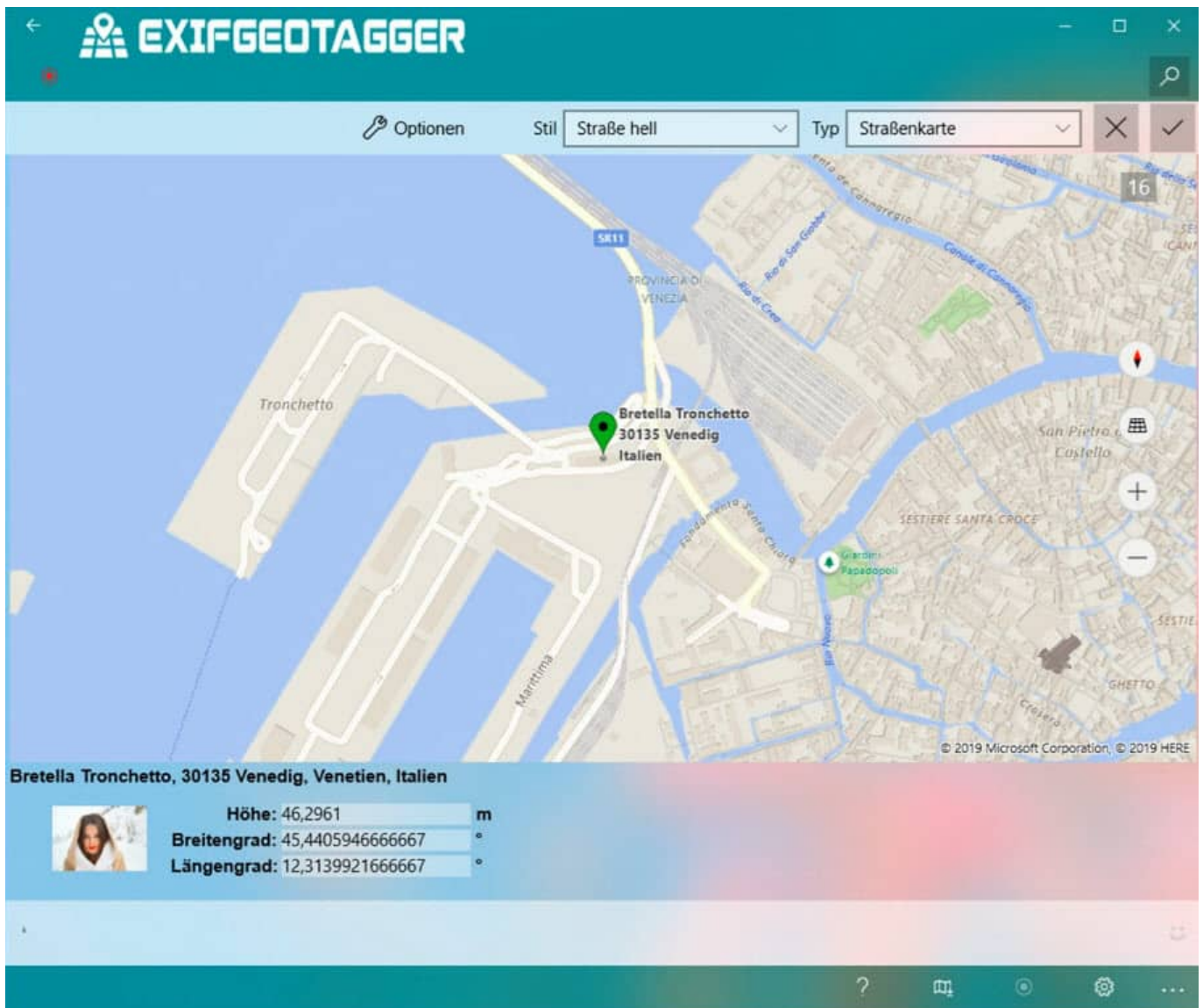
ChatGPT kann hören, sprechen, verstehen, texten und Bilder generieren

Wasserzeichen und Exif-Metadaten

Allerdings können die meisten Wasserzeichen und auch Metadaten von Menschen mit Expertise entfernt werden. Auf Dauer dürfen sich die Algorithmen bei Meta also nicht allein auf solche Merkmale verlassen, sondern müssen im Zweifel auch weitere Untersuchungen vornehmen. Es ist – zumindest bislang – durchaus möglich, die Wahrscheinlichkeit zu berechnen, nach der ein Foto echt ist oder durch KI erzeugt wurde.

Meta setzt auf zwei Standards: Zum einen auf die “Coalition for Content Provenance and Authenticity” (C2PA) sowie den des „International Press Telecommunications Council“ (IPTC). Diese Standards beschreiben Verfahren, um Bilder digital zu markieren. Beim C2PA-Standard sind Microsoft und Adobe beteiligt, die ebenfalls KI-generierte Inhalte markieren.

Ab Mai soll es losgehen. Es ist zu erwarten, dass nicht alle KI-generierten Fotos automatisch erkannt und korrekt markiert werden. Aber es ist ein erster Schritt, um die dringend erforderliche Transparenz einzuführen.



„AI Act“ der EU sieht ohnehin Kennzeichnung vor

Völlig freiwillig kommt die Maßnahme indes nicht. Denn zwischen Mai und Juli dieses Jahres soll der vom EU-Parlament beschlossene „AI Act“ in Kraft treten, der ohnehin schon bald eine Kennzeichnungspflicht für KI-Inhalte vorsieht.

Künftig wird die Maßnahme auf Audios und Videos ausgedehnt. Bei Videos und Tonspuren sollen die Uploader bei Facebook und Instagram selbst offenlegen müssen, ob es sich um KI-erzeugte Inhalte handelt.

<https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads>

Warum sind Online-Spiele weltweit so beliebt?



Es gibt viele Arten, sich unterhalten zu lassen oder abzulenken. Games und Spiele am Handy oder zu Hause an der Konsole sind definitiv eine Möglichkeit. Auch im Netz wartet jede Menge Ablenkung.

Allein in Deutschland zocken über 34 Millionen Menschen regelmäßig Videospiele. Das entspricht fast der Hälfte der erwachsenen Gesamtbevölkerung.

Und die Mehrheit davon spielt nicht mehr vor allem auf klassischen Konsolen, sondern über das Internet – und ganz besonders auf dem Smartphone. Online-Spiele sind aus unserem digitalen Alltag nicht mehr wegzudenken.

Vom einfachen Browser-Game bis hin zu aufwendigen Multiplayer-Blockbustern: die virtuellen Welten üben eine magische Anziehungskraft aus.

Wie tief ist die Faszination für Online-Gaming verwurzelt und was treibt Millionen Menschen an, Tag für Tag in diese parallel existierenden Universen einzutauchen?



Online-Spiele entführen mitunter in Fantasiewelten

Drei Milliarden Gamer weltweit

Nach einigen Untersuchungen gibt es mehr als drei Milliarden Menschen auf der Welt, die zumindest eine Art von Online Spiel spielen. Sie sind sogar so beliebt, dass sie zu einem internationalen Zeitvertreib geworden sind.

Einige sind sogar noch einen Schritt weiter gegangen und haben es zu ihrem Beruf gemacht. Es gibt viele Arten von Spielen, die sich ausprobieren lassen. Hier sind fünf Gründe, warum Menschen Online-Spiele spielen.

1: Die reine Unterhaltung

Der offensichtlichste Grund, warum Menschen Online-Spiele spielen, ist sich zu unterhalten. Die Ablenkung, könnte man auch sagen. Es ist eine sichere und unterhaltsame Möglichkeit, eine virtuelle Welt zu erkunden und Dinge zu tun, die im wirklichen Leben unmöglich sind.

In der Umgebung des Spiels kann ein Spieler ein Krieger sein und Magie einsetzen. Sie können sich auf Abenteuer begeben und Spaß mit ihren Online Freunden haben. Online-Spiele [bieten den Spielern eine Menge Spaß und Unterhaltung](#).

Man kann den Stress in der Schule oder im Beruf für ein paar Stunden am Tag vergessen, indem man sich in sein Lieblingsspiel vertieft. Man muss nicht einmal ein ernsthafter Gamer sein – man kann auch ein Gelegenheitsspiel auf dem Handy spielen, um den Stress des Alltags zu bewältigen.

Kurz gesagt, der Hauptgrund, warum Menschen Online-Spiele spielen, ist Spaß zu haben, sich zu unterhalten und Zeit mit Freunden zu verbringen.



Auch Kinder spielen gerne, müssen aber besonders geschützt werden

2: Einnahmequelle

Für Nicht-Insider kaum zu glauben, aber Online-Spiele sind für einige zu einer lukrativen Einnahmequelle geworden. Es gibt Gamer und YouTuber, die sich dem Gaming verschrieben haben und allein mit dem Spielen von Spielen Millionen von Dollar verdienen. ESports und Game-Streaming sind zu einer der besten Karrieren des 21. Jahrhunderts geworden. Die Konkurrenz ist groß, aber wer eine Nische gefunden hat, kann viel Geld verdienen.

Einige besuchen aber auch gerne Online-Casinos wie [krypto casino](#), und machen ds zur Haupteinnahmequelle. Wobei es sich hier nun wirklich nicht um eine verlässliche Einnahmequelle handelt. Doch bei einigen Spielen wie "Poker" steht nicht allein das Glück im Vordergrund, sondern auch Erfahrung und Können. Da kann das funktionieren. Es besteht aber auch immer ein erhebliches Risiko, Geld

zu verlieren.

Eine weitere ungewöhnliche Art, solche Angebote zu nutzen, ist: Es handelt sich um eine Form des digitalen Zahlungsverkehrs. Krypto-Zahlungen in Online [Casinos in Österreich](#) ermöglichen es Menschen, Geld schnell und kostengünstig zu senden, ohne auf traditionelle Finanzinstitute angewiesen zu sein.

3: Bewegungsfreiheit

Online-Spiele bieten die Möglichkeit, auf gesunde Art und Weise zu flüchten ("Eskapismus"). Einer der größten Vorteile (oder nennen wir es "Reize") vieler Online-Spiele ist die Erkundung und Bewegungsfreiheit, die sie bieten.

Wer zum Beispiel **Assassin's Creed Origins** spielt, hat die Möglichkeit, das Land des alten Ägyptens zu erkunden. Super Mario oder Pokemon lassen einen in eine virtuelle Welt mit vielen lustigen Elementen eintauchen. Inzwischen gibt es auch Open-World-Spiele, bei denen die Welt des Spiels vollständig erkundet werden kann.



Fortnite ist eine der populärsten Online-Games

4. Freunde finden und mit ihnen in Kontakt bleiben

Online-Spiele ermöglichen es den Spielern auch, Freunde zu finden und mit ihnen in Kontakt zu bleiben. Es gibt viele Menschen, die unter sozialen Ängsten oder anderen Behinderungen leiden, die sie daran hindern, in die Welt hinauszugehen und mit anderen Menschen zu interagieren.

Ein Online-Spiel ist für sie ein sicherer und geschützter Ort, an dem sie Zeit verbringen können. Sie können online Freunde finden und viele, viele Tage lang mit ihnen in Kontakt bleiben.

Viele mögen es, online mit anderen Menschen zu daddeln, mit Menschen, die sie

kennen, aber auch mit Menschen, die sie (noch) nicht kennen.

Die Freiheit der Wahl, die Online-Spiele bieten, ist etwas ganz anderes. Wer mag, kann sich auch von Zeit zu Zeit mit Online-Freunden treffen, mit ihnen chatten und amüsieren. Online-Spiele lassen sich auch nutzen – [sagt die Wissenschaft](#) –, um Beziehungen zu Freunden aufzubauen und zu pflegen.



Gamescom: Es kann immer weniger vor Ort gedaddelt werden

5: Gefühl der Autonomie

Online-Spiele ermöglichen Action und Kämpfe, die in der realen Welt unmöglich und illegal sind.

In der Tat können Action-Videospiele eine großartiges Training zur Teambildung sein. Beim Spielen von Online-Spielen kann man die ganze Aufregung und den Nervenkitzel einer Online-Umgebung erleben, während man zu Hause in Sicherheit ist.

Spieler können gegen Dämonen kämpfen, auf Feinde schießen und schnelle Autos fahren, ohne ihr eigenes Leben zu riskieren.

Online-Spiele bieten den Menschen auch ein hohes Maß an Autonomie. Dies ist eine hilfreiche Umgebung für Menschen, die in der Vergangenheit mit kontrollierenden und missbrauchenden Familien oder Partnern zu tun hatten. Sie können die Kontrolle im Rahmen ihrer Dominanz zurückgewinnen.

Außerdem helfen Spiele den Menschen, ein Gefühl der Verbundenheit zu finden, was sie durch die Interaktion mit anderen Spielern online tun können.

Fazit

Das sind nach wissenschaftlichen Erkenntnissen die fünf wichtigsten Gründe, warum Menschen Zeit mit Online-Spiele verbringen. Es handelt sich im Grunde um einige Bedürfnisse, die Online-Games bis zu einem gewissen Grad erfüllen können.

Für einige bieten Online-Spiele eine großartige Möglichkeit, Kontakte zu knüpfen und sich mit Freunden und Familienmitgliedern auszutauschen, die vielleicht weit weg wohnen.

QuickFreeze: Die datenschutzfreundliche Alternative zur Vorratsdatenspeicherung



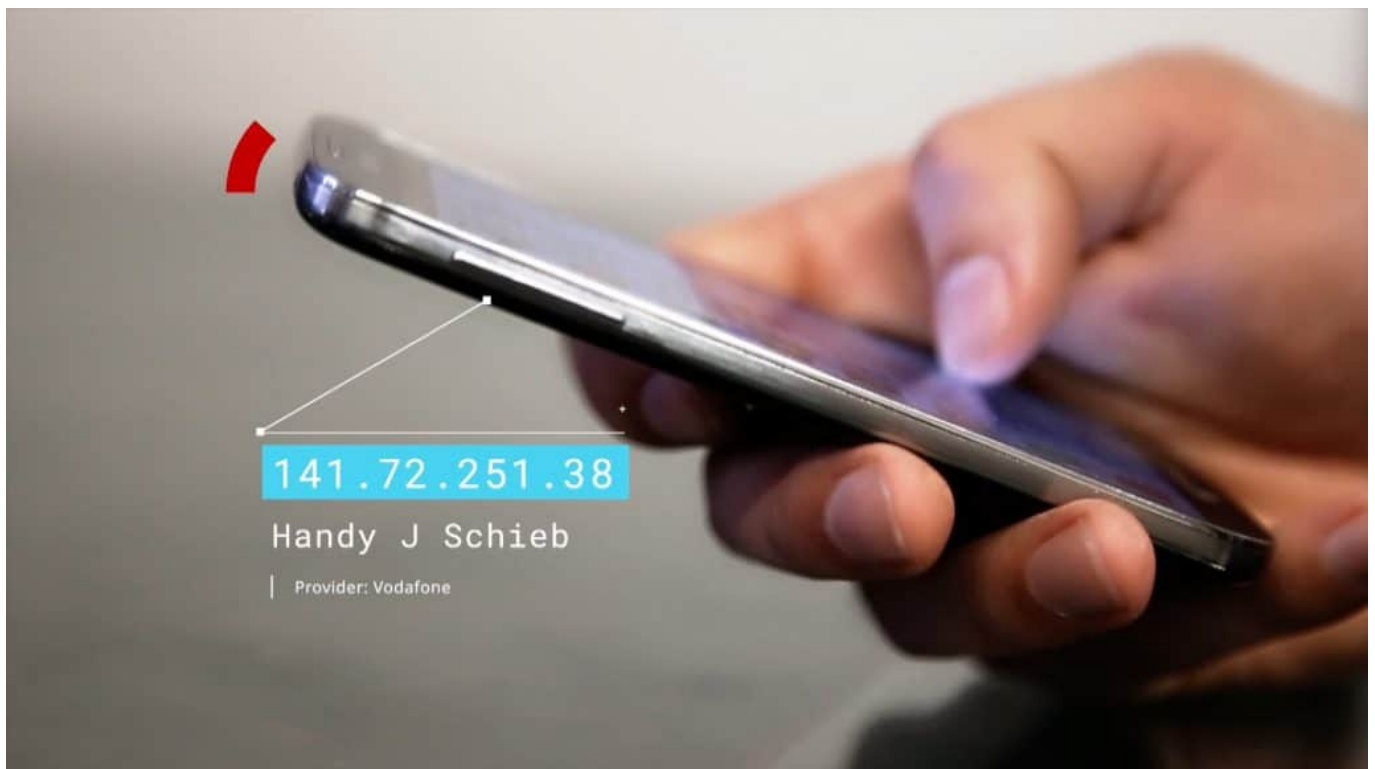
Die Regierungsparteien SPD und FPD haben sich auf Kabinettschere geeinigt. Zur Bekämpfung schwerer Straftaten soll das Quick-Freeze-Verfahren kommen. Damit wäre die umstrittene Vorratsdatenspeicherung vom Tisch.

Die Vorratsdatenspeicherung steht seit Jahren in der Kritik (und wurde von diversen Gerichten auch immer wieder als unzulässig erklärt).

Doch Polizei und Ermittlungsbehörden sind bei schweren Straftaten auf Spuren und Daten angewiesen. Mit dem **QuickFreeze**-Verfahren gibt es nun eine vielversprechende Alternative, die den Datenschutz wahrt und trotzdem effektiv gegen Kriminalität vorgeht.

Stellt euch vor, all eure Daten werden ohne konkreten Anlass für Monate oder sogar Jahre gespeichert – für die meisten eine beunruhigende Vorstellung, die mit der Vorratsdatenspeicherung Realität geworden ist.

Doch was, wenn es eine Möglichkeit gäbe, Daten nur dann zu sichern, wenn ein begründeter Verdacht vorliegt? Genau hier setzt das QuickFreeze-Verfahren an.



Die Vorratsdatenspeicherung wurde schon mehrfach von Gerichten gekippt

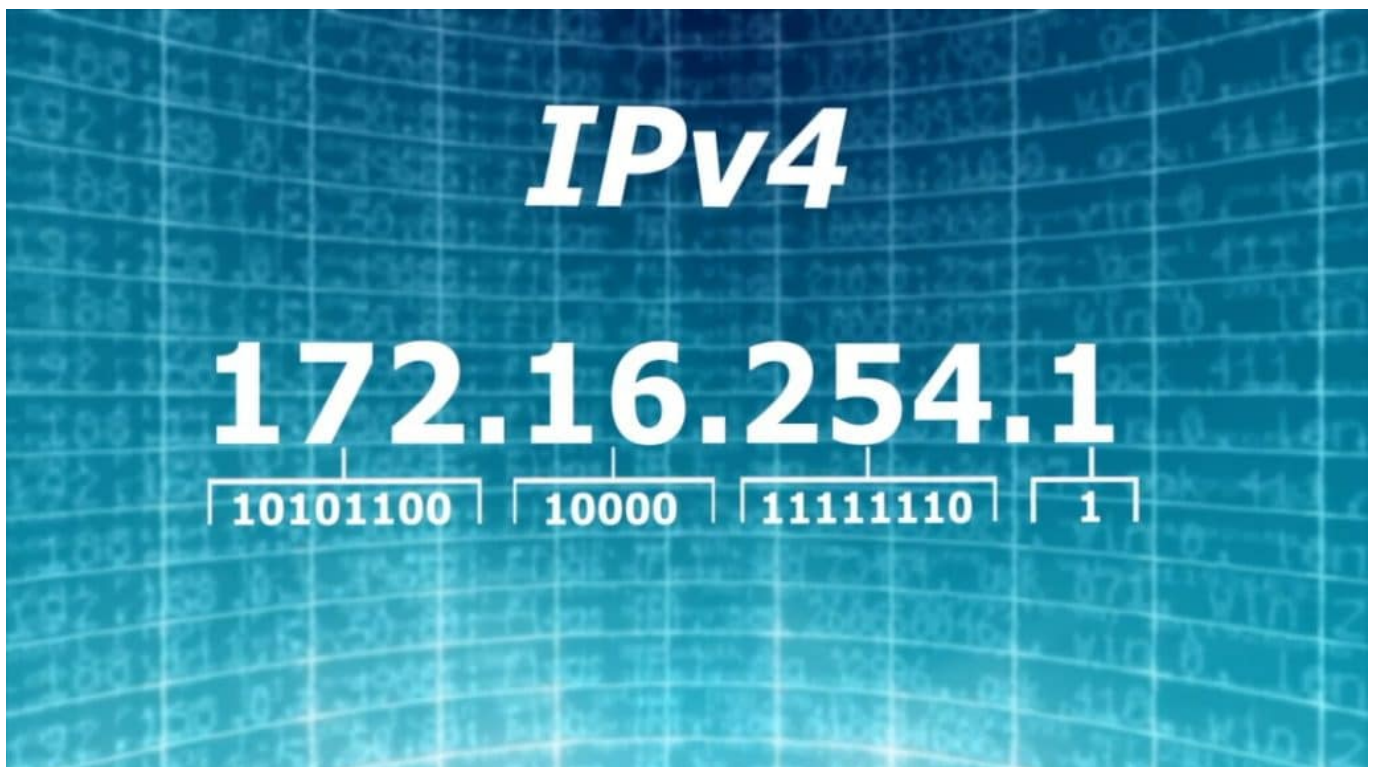
Das QuickFreeze-Verfahren - Eine Einführung

Das QuickFreeze-Verfahren ist eine respektierte Alternative zur umstrittenen Vorratsdatenspeicherung. Bei der Vorratsdatenspeicherung werden die

Verbindungsdaten aller Bürger für einen bestimmten Zeitraum anlasslos gespeichert. Etwa Bewegungsdaten des Handys, Nutzung von E-Mail, Aufruf von Webseiten und vieles mehr.

Dies geschieht unabhängig davon, ob ein Verdacht auf eine Straftat besteht oder nicht. Im Gegensatz dazu erfolgt beim QuickFreeze-Verfahren die Datenspeicherung nur dann, wenn ein konkreter Anlass dafür vorliegt.

Das Prinzip des QuickFreeze-Verfahrens ist einfach: Anstatt die Daten aller Bürger auf Vorrat zu speichern, werden die Daten nur dann "eingefroren", wenn ein begründeter Verdacht auf eine schwere Straftat besteht. Die Entscheidung darüber trifft grundsätzlich ein unabhängiger Richter und erfolgt damit auch nur nach Bedarf. Liegt eine richterliche Anordnung vor, müssen die Telekommunikationsanbieter die Daten der betroffenen Person für einen festgelegten Zeitraum speichern und den Ermittlungsbehörden zur Verfügung stellen.



Die IP-Adresse lässt Rückschlüsse zu

Vorteile des QuickFreeze-Verfahrens

Schutz der Privatsphäre

Ein wesentlicher Vorteil des QuickFreeze-Verfahrens liegt im Schutz der Privatsphäre unbescholtener Bürger. Da die Daten nur bei einem konkreten Verdacht gespeichert werden, entfällt die anlasslose Massenüberwachung, wie sie bei der Vorratsdatenspeicherung praktiziert wird. Dies stärkt das Grundrecht auf informationelle Selbstbestimmung und schützt die Bürger vor ungerechtfertigten Eingriffen in ihre Privatsphäre.

Gezielte Strafverfolgung

Durch das QuickFreeze-Verfahren können Ermittlungsbehörden gezielt gegen Verdächtige vorgehen. Die richterliche Anordnung stellt sicher, dass nur in begründeten Fällen auf die Daten zugegriffen wird. Somit können Straftaten effektiv aufgeklärt werden, ohne dass unbescholtene Bürger unter Generalverdacht gestellt werden. Die Ressourcen der Ermittlungsbehörden können so zielgerichtet eingesetzt werden.

Einhaltung rechtsstaatlicher Prinzipien

Das QuickFreeze-Verfahren wahrt wichtige rechtsstaatliche Prinzipien. Durch die richterliche Anordnung wird sichergestellt, dass die Speicherung und Nutzung der Daten verhältnismäßig und rechtmäßig erfolgt. Die unabhängige richterliche Kontrolle schützt vor willkürlichen Eingriffen und stärkt das Vertrauen der Bürger in den Rechtsstaat.

Dauer der Datenspeicherung

Ein weiterer Vorteil des QuickFreeze-Verfahrens liegt in der begrenzten Dauer der

Datenspeicherung. Anders als bei der Vorratsdatenspeicherung, bei der die Daten für einen festen Zeitraum gespeichert werden, richtet sich die Speicherdauer beim QuickFreeze-Verfahren nach dem konkreten Ermittlungsverfahren. Sobald die Daten für die Ermittlungen nicht mehr benötigt werden, müssen sie gelöscht werden. Dies verhindert eine unnötige Anhäufung von Daten und minimiert das Risiko von Datenmissbrauch.

Herausforderungen und Diskussion

Trotz der genannten Vorteile gibt es auch Herausforderungen und Diskussionspunkte beim QuickFreeze-Verfahren. Kritiker argumentieren, dass das Verfahren nicht effektiv genug sei, da die Daten erst nach einer richterlichen Anordnung gespeichert werden. Dies könnte die Aufklärung von Straftaten erschweren, insbesondere wenn die Daten in der Zwischenzeit gelöscht wurden.

Befürworter des QuickFreeze-Verfahrens halten dem entgegen, dass eine anlasslose Massenüberwachung unverhältnismäßig und mit rechtsstaatlichen Prinzipien unvereinbar sei. Sie betonen, dass die gezielte Speicherung von Daten bei konkretem Verdacht ausreichend sei, um Straftaten effektiv zu bekämpfen. Zudem sei es wichtig, die Grundrechte der Bürger zu schützen und das Vertrauen in den Rechtsstaat zu stärken.



Normalerweise löschen Provider die Verkehrsdaten relativ schnell wieder

Ausblick und Fazit

Das QuickFreeze-Verfahren bietet eine vielversprechende Alternative zur umstrittenen Vorratsdatenspeicherung. Es schützt die Privatsphäre der Bürger, ermöglicht eine gezielte Strafverfolgung und wahrt rechtsstaatliche Prinzipien. Dennoch bleiben Herausforderungen und Diskussionspunkte bestehen, die es zu berücksichtigen gilt.

Es ist wichtig, dass bei der Umsetzung des QuickFreeze-Verfahrens klare rechtliche Rahmenbedingungen geschaffen werden. Dazu gehören präzise Vorgaben für die richterliche Anordnung, Transparenz bei der Datennutzung und wirksame Kontrollmechanismen. Nur so kann sichergestellt werden, dass das Verfahren rechtskonform und verhältnismäßig angewendet wird.

Letztlich muss ein Ausgleich zwischen den berechtigten Sicherheitsinteressen und dem Schutz der Grundrechte gefunden werden. Das QuickFreeze-Verfahren bietet hierfür einen vielversprechenden Ansatz. Es ermöglicht eine effektive Strafverfolgung, ohne die Privatsphäre unbescholtener Bürger unverhältnismäßig zu beeinträchtigen. Eine sachliche und differenzierte Debatte über die Vorteile und Herausforderungen des Verfahrens ist notwendig, um einen gesellschaftlichen Konsens zu finden.

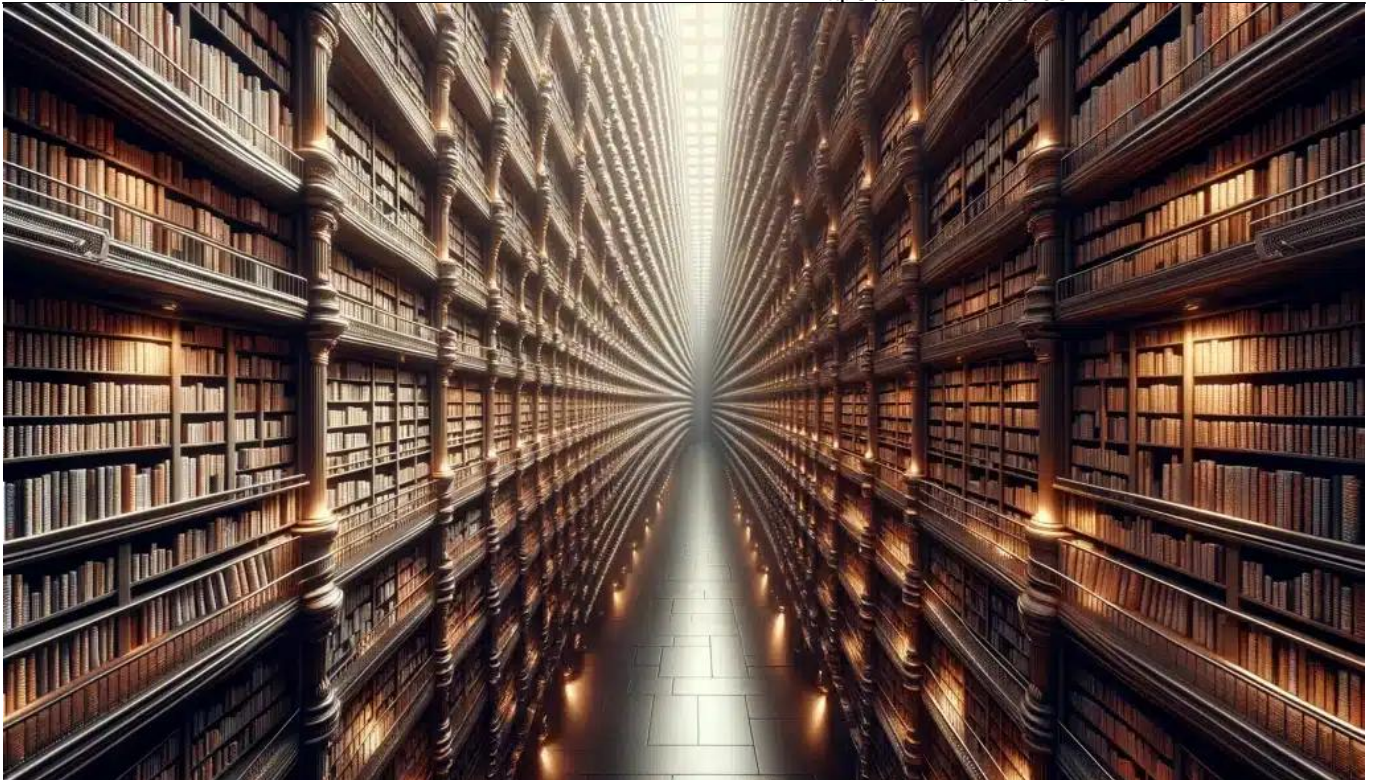
In einer Zeit, in der der Schutz persönlicher Daten immer wichtiger wird, stellt das QuickFreeze-Verfahren eine datenschutzfreundliche Alternative zur Vorratsdatenspeicherung dar. Es zeigt, dass es möglich ist, die Sicherheit zu gewährleisten und gleichzeitig die Grundrechte der Bürger zu achten. Die Einführung des QuickFreeze-Verfahrens wäre ein wichtiger Schritt hin zu einer ausgewogenen und rechtsstaatlichen Sicherheitspolitik.

Ein Zetabyte - eine unvorstellbar große Datenmenge



Wir speichern immer mehr Daten. Das prognostizierte Volumen aller gespeicherten Daten explodiert. Wir werden uns an eine neue Einheit gewöhnen müssen: Zetabyte.

Wenn es um die Beschreibung riesiger Datenmengen geht, kommen wir heutzutage an Begriffen wie "Zetabyte" nicht mehr vorbei. Aber was genau ist eigentlich ein Zetabyte und wie lässt sich diese unfassbar große Zahl greifbar machen?



Die Speichermengen verfünffachen sich alle paar Jahre

Byte, KByte, MByte, ..., Zetabyte

Beginnen wir bei den Grundlagen der Datenmengenverwaltung: Unsere geläufigen Einheiten sind Byte, Kilobyte, Megabyte, Gigabyte und Terabyte. Jede Einheit ist jeweils 1000 Mal größer als die vorherige.

Doch irgendwann stoßen wir an die Grenzen dieser Skala. Denn nach dem Terabyte (1 Billion Byte) kommt das Petabyte (1 Billiarde Byte), das Exabyte (1 Trilliarde Byte) und schließlich das **Zetabyte**.

Ein Zetabyte entspricht der unglaublichen Menge von 1 Sextillion Bytes! Das sind 1.000.000.000.000.000.000.000 Byte oder eine 1 mit 21 Nullen.

Um das etwas greifbarer zu machen:

- Würde man alle Zetabyte, die es weltweit gibt, auf Blu-ray Discs speichern, würde man genug Discs füllen, um den Mond etwa 23 Mal zu bedecken.
- Wenn man alle Zetabytes in 1 TB Festplatten umwandeln würde, könnte man damit etwa 1 Milliarde PCs ausstatten.
- Alle Zetabytes an Daten entsprechen etwa der Menge an Wasser, die in 40 Millionen Olympischen Schwimmbecken passt.

Das zeigt, welche unvorstellbaren Dimensionen wir hier erreichen. Ein Zetabyte ist schlichtweg eine gigantische, kaum mehr fassbare Datenmenge. Zum Vergleich: Das gesamte Internet umfasste 2018 "nur" ca. 33 Zetabytes.



Bedarf an Speicherkapazität explodiert

Doch der Bedarf an solch riesigen Speicherkapazitäten wächst stetig. Durch Big Data, KI, autonomes Fahren und das Internet der Dinge entstehen immer mehr Daten, deren Verwaltung und Speicherung eine enorme technische Herausforderung darstellt.

Zetabyte-Dimensionen werden daher in Zukunft immer selbstverständlicher werden.

Für Prognosen zu den weltweit gespeicherten Datenmengen und dem Bedarf an Speichermedien gibt es verschiedene Studien und Analysen:

1. IDC Worldwide Global DataSphere Forecast:

- Laut der jährlichen IDC-Prognose wird das weltweite Datenvolumen von 59 Zettabyte im Jahr 2020 auf 175 Zettabyte im Jahr 2025 anwachsen.
- Der Großteil dieses Wachstums wird durch Daten aus dem Internet der Dinge, Videoüberwachung, autonome Fahrzeuge und andere Quellen angetrieben.

2. Seagate Rethink Data Report:

- Seagate schätzt, dass das weltweite Datenvolumen von 59 Zettabyte im Jahr 2020 auf 175 Zettabyte im Jahr 2025 und 869 Zettabyte im Jahr 2030 ansteigen wird.
- Der Bedarf an Speicherkapazität wird demnach massiv zunehmen, was den Einsatz verschiedener Speichertechnologien wie Festplatten, SSDs und Bandlaufwerke erfordert.

3. Cisco Annual Internet Report:

- Cisco prognostiziert, dass das globale IP-Datenvolumen von 59 Exabyte pro Monat im Jahr 2018 auf 330 Exabyte pro Monat bis 2023 anwachsen wird.
- Dies entspricht einem jährlichen Wachstum von 26% und erfordert

massive Investitionen in Netzwerk- und Speicherinfrastrukturen.

4. Statista Prognose zum Datenspeichervolumen:

- Statista schätzt, dass das weltweite Datenspeichervolumen von 6,7 Zettabyte im Jahr 2018 auf 49 Zettabyte im Jahr 2024 ansteigen wird.

- Der zunehmende Bedarf wird durch den Einsatz von Cloud-Speicher, Festplatten und anderen Speicherlösungen gedeckt.

Zusammengefasst gehen diese Studien von einem enormen Wachstum des weltweiten Datenvolumens in den nächsten Jahren aus, was einen entsprechenden Ausbau der Speicherkapazitäten erfordert. Unternehmen und Anbieter müssen sich auf steigende Investitionen in Speichertechnologien und Infrastrukturen einstellen.

Versteckte und Systemdateien ein- und ausblenden



Ein Windows-System hat eine kaum überschaubare Anzahl von Dateien in verschiedenen Ordnern. Nur wenige davon sind für den Anwender aktiv nutzbar. Andere sind ausgeblendet, aber vielleicht trotzdem von Interesse. Ihr habt die Kontrolle!

Normale, versteckte, Systemdateien: Warum?

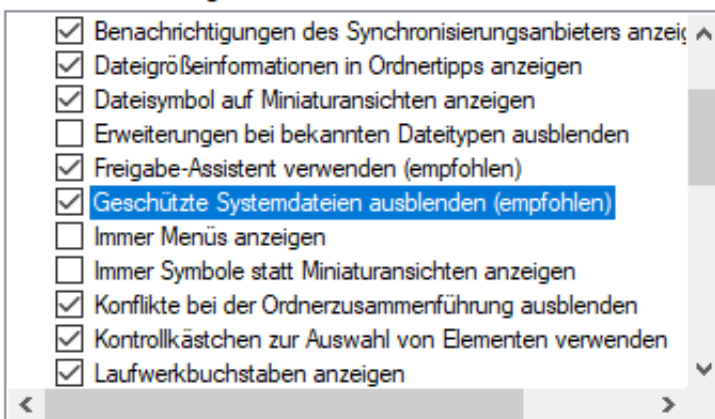
Für den Anwender sind Dateien die Container, die seine Daten enthalten: Das Word-Dokument, die Excel-Tabelle, die PowerPoint-Präsentation, aber auch der Speicherstand des Lieblingsspiels oder die Bilder der Digitalkamera. all diese Dateien liegen in [Verzeichnissen](#) auf den Datenträgern. Dazu kommen allerdings noch viele weitere Dateien:

- Windows-Programmteile
- Systemdateien
- Treiber und Zubehörinformationen

- Apps und Programme
- Gespeicherte Einstellungen der Programme
- Temporäre Dateien, die nur zum ordnungsgemäßen Betrieb von Windows und/oder Programmen benötigt werden.

Diese [Dateien](#) soll der Benutzer im Idealfall gar nicht selbst verwenden: Löscht oder verändert er sie, dann kann das schnell dazu führen, dass ein Programm oder gar der ganze PC nicht mehr störungsfrei laufen. Aus diesem Grund sind viele dieser Dateien i Standard ausgeblendet. Frei nach dem Motto: Was der Benutzer nicht sieht, kann er auch nicht kaputt machen.

Erweiterte Einstellungen:



Ändern der Ansichtsoptionen

Im Standard wählt Windows bei der Installation die Ansichtsvariante, die am sichersten erscheint: Versteckte und Systemdateien werden im Explorer gar nicht erst angezeigt. Wenn ihr Gründe habt, diese Dateien anzeigen zu lassen (oder ihr komisch aussehende, halbtransparente Dateien auf dem Desktop oder in Verzeichnissen angezeigt bekommt), dann geht so vor:

- Startet den Explorer und navigiert in das Verzeichnis, in dem diese Dateien angezeigt werden.
- Klickt auf **Ansicht > Optionen > Ordner- und Suchoptionen ändern** in der Menüleiste des Explorers.
- Klickt dort in die Registerkarte **Ansicht**.
- In der Liste der [Ansichtsoptionen](#) gibt es jetzt zwei Bereiche, auf die ihr euer Augenmerk richten solltet.
- **Geschützte Systemdateien ausblenden** sollte in jedem Fall aktiviert sein, denn diese Dateien sind die kritischsten und können bei

versehentlichem Löschen den meisten Schaden anrichten.

- Weiter unten unter **Versteckte Dateien und Ordner** könnt ihr auswählen, ob diese angezeigt werden sollen oder nicht. Oft werden interessante Dateien, die der Benutzer nicht sehen soll, durch das Attribut "versteckt" seinem Blick entzogen. Wenn ihr eine Datei nicht findet, dann kann das daran liegen. Mit diesen Dateien solltet ihr trotzdem vorsichtig sein!

Die Änderungen werden sofort aktiv, wenn ihr auf **OK** oder **Übernehmen** klickt.

Erweiterte Einstellungen:

Ordnerfenster in einem eigenen Prozess starten

Popupinformationen für Elemente in Ordnern und auf dem Desktop anzeigen

Statusleiste anzeigen

Verschlüsselte oder komprimierte NTFS-Dateien in anderen Ordnern anzeigen

■ Versteckte Dateien und Ordner

● Ausgeblendete Dateien, Ordner oder Laufwerke nicht anzeigen

○ Ausgeblendete Dateien, Ordner und Laufwerke anzeigen

Vollständigen Pfad in der Titelleiste anzeigen

Vorherige Ordnerfenster bei der Anmeldung wiederherstellen

Vorschauhandler im Vorschaufenster anzeigen

■ Navigationsbereich