Schieb Report

Ausgabe 2023.31

Handy weg: Maßnahmen davor und danach

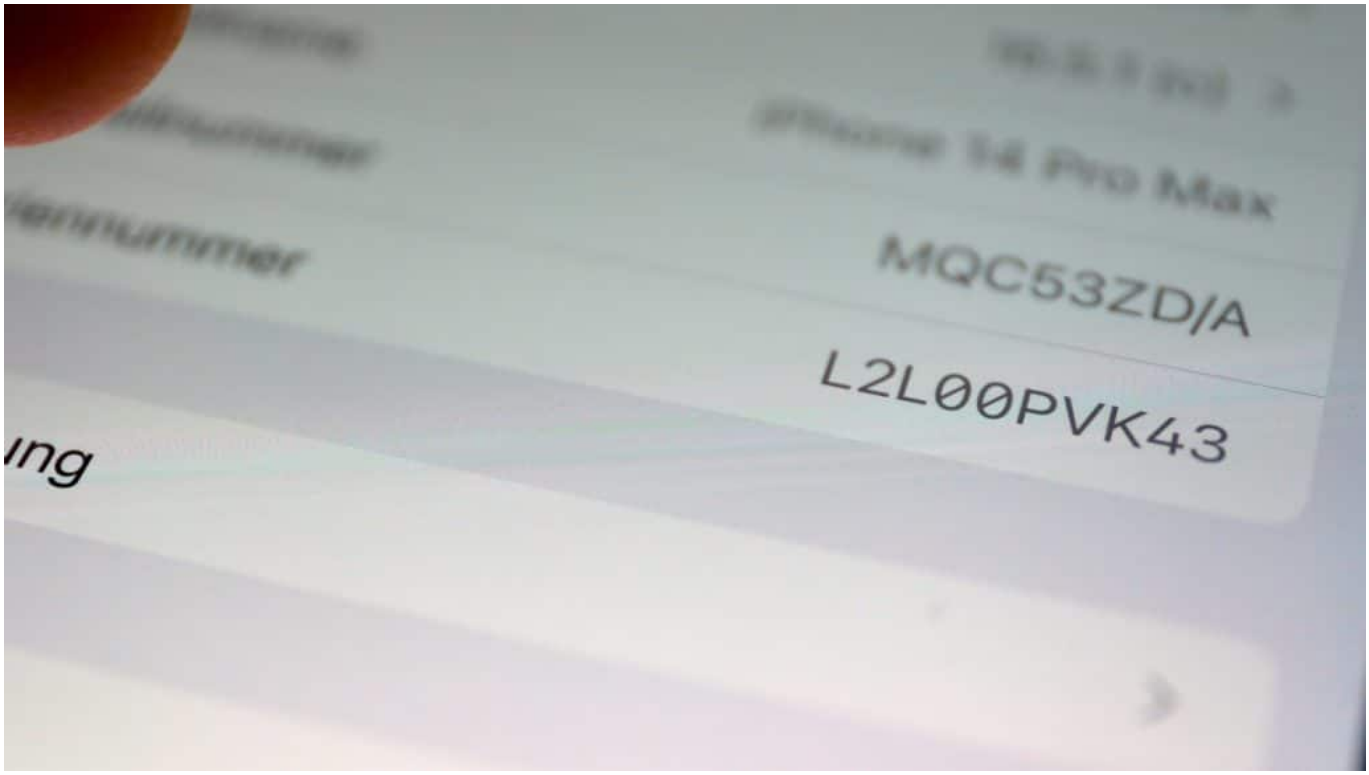
Smartphones sind heute mehr als nur ein teures Stück Hardware: Sie bergen häufig wichtige und sensible Daten. Wwas im Falle eines Diebstahls oder Verlust zu tun ist – und wie man sein Gerät gut vorbereitet.

Handys und Smartphones sind begehrtes Diebesgut: Laut Kriminalstatistik der Polizeilichen Kriminalprävention im Bundeskriminalamt (BKA) wurden im Jahr 2022 in Deutschland beinahe 185.000 Handys als gestohlen gemeldet. Besonders begehrt sind die Geräte der Luxusklasse. Die entwendeten Geräte lassen sich auf dem Schwarzmarkt weiterverkaufen – ältere Geräte zumindest zum Ausschlachten verwenden.

Wie viele Geräte darüber hinaus verloren gehen, weiß niemand.

Doch für die meisten Menschen ist nicht der materielle Wert eines Handys das größte Problem, sondern eher der immaterielle Schaden. In unseren Smartphones sind heute alle Kontakte gespeichert, viele Fotos und Videos – möglicherweise auch pikante oder brisante darunter –, sowie Notizen, Dokumente, Daten. Die sollten weder verloren gehen, noch in falsche Hände

geraten.



Das solltet Ihr vorher gemacht haben: Die IMEI ermitteln

Smartphone durch PIN und Biometrie absichern

Aus diesem Grund ist es äußerst wichtig, jedes Smartphone durch PIN (am besten 6-stellig) und/oder biometrische Daten sie Fingerabdruck oder Gesichts-Scan abzusichern. Die automatische Sperre sollte spätestens nach 30 Sekunden greifen: Damit Fremde und vor allem Kriminelle das Handy nicht einfach entsperren und die darin gespeicherten Daten abgreifen können.

In höherwertigen Modellen (etwa dem iPhone) lassen sich bei Bedarf auch höhere Sicherheitsstandard einstellen: Nach 10 vergeblichen Login-Versuchen werden die gespeicherten Daten auf Wunsch automatisch und unwiederbringlich gelöscht. Allerdings sollte man diese Option nur wählen, wenn man sicher sein kann, dass keine Kinder im Haus sind, die so etwas schon mal ungewollt auslösen.

Ohnehin sind die Daten in den meisten modernen Handys verschlüsselt

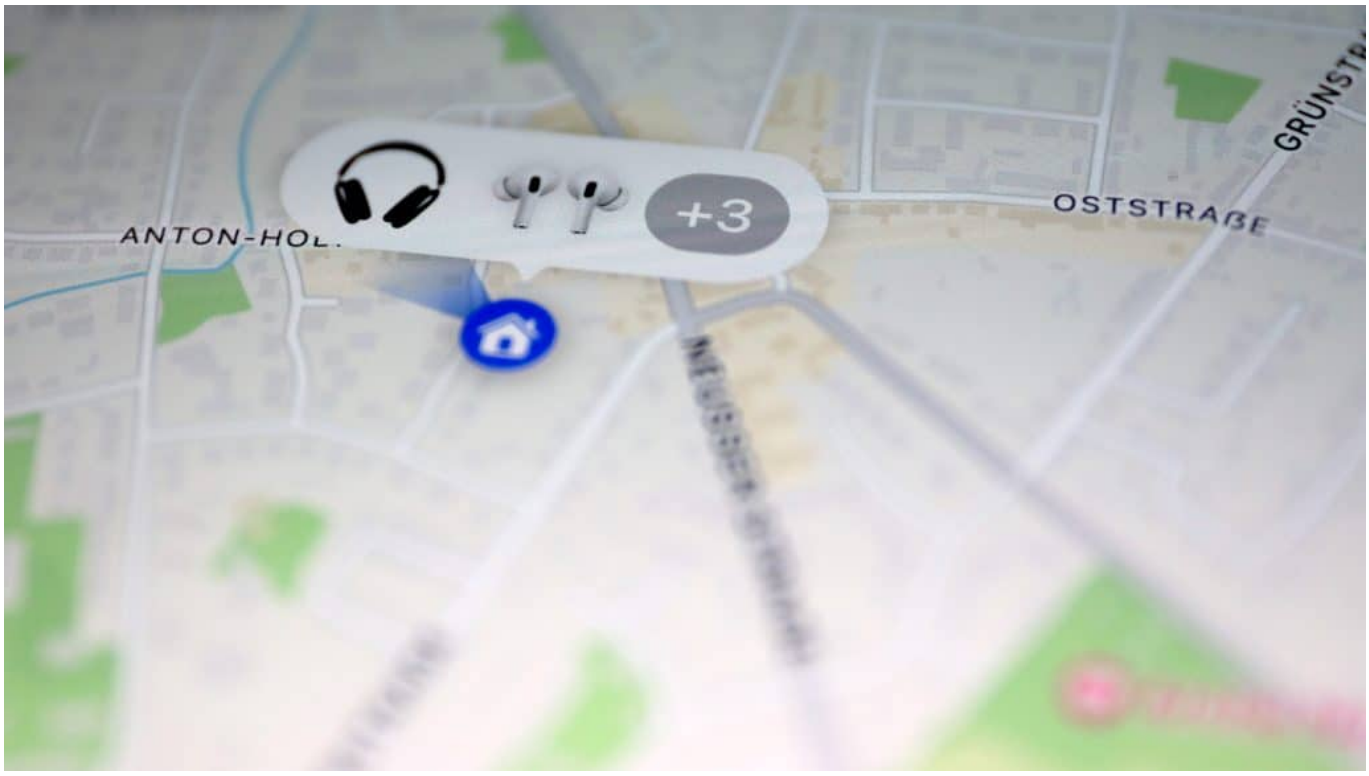
gespeichert und ohne korrekten Login nicht lesbar. Wer sein Smartphone nicht nur zu privaten Zwecken nutzt, sollte die Sicherheitsstandard so hoch wie möglich einstellen.

Erste Pflichtübung: das Gerät orten

Aber ist das Gerät wirklich entwendet, oder hat man es selbst verloren oder irgendwo liegen lassen? Diese Frage muss als erstes geklärt werden. Dazu Funktionen wie „Wo ist?“ (iOS) oder „Gerät finden“ (Android) benutzen. Diese mittlerweile serienmäßig in den mobilen Betriebssystemen eingebauten Funktionen helfen dabei, das Handy in der Regel bis auf wenige Meter genau zu lokalisieren – oder sie zeigen zumindest den letzten gültigen Aufenthaltsort an.

Wer sein Handy nur irgendwo in einer Couch-Ritze hat liegen lassen, kann es so schnell finden und holen. Es ist auch möglich, einen lauten Ton abspielen zu lassen, damit andere auf das Handy aufmerksam werden. Das alles geht aber meist nur, solange das Handy eingebucht oder wenigstens im WLAN ist. Haben Kriminelle das Handy erst mal abgeschaltet oder in den Flugmodus versetzt, wird es schwierig mit der Ortung. Deshalb: Schnell reagieren.

Wichtig zu wissen: Es ist auch möglich, moderne Smartphones im Fall des Diebstahls aus der Ferne zu sperren – und alle gespeicherten Daten zu löschen. Unter iOS ist das eine Funktion in der iCloud, unter Android unter „Finde mein Gerät“. Eine Art Ultima Ratio, um sicherzustellen, dass Fremdem oder Kriminellen keine sensiblen Daten in die Hände geraten. Vor allem für Dienst-Handys oft eine wichtige Funktion.



Erst mal herausfinden: Wo befindet sich das Gerät gerade?

Wichtig: die Seriennummer

Die Polizei empfiehlt, jeden Diebstahl anzuzeigen. Dabei ist es hilfreich, die Seriennummer (IMEI, International Mobile Equipment Identity) des Geräts zu kennen. Jedes Smartphone hat eine eigene. Sie ist meist auf der Verpackung des Geräts aufgedruckt. Wer ein iPhone hat, kann die Seriennummer auch im Menü „Einstellungen“ und dort unter „Info“ in der Rubrik „Allgemein“ abfragen. Android-Nutzer finden sie Seriennummer in den Einstellungen unter dem Menüpunkt „Über das Telefon“.

Doch es gibt einen noch bequemeren Weg: Auf nahezu allen Handys und Smartphones kann die Kurzwahl ***#06#** verwendet werden (anstelle einer Rufnummer): Die Seriennummer erscheint sofort im Display – oft sogar mit noch einigen weiteren Informationen über das Gerät. Die Nummer unbedingt rechtzeitig erfragen, notieren und an einem sicheren Ort verwahren, da sie bei einer Anzeige unbedingt erforderlich ist.

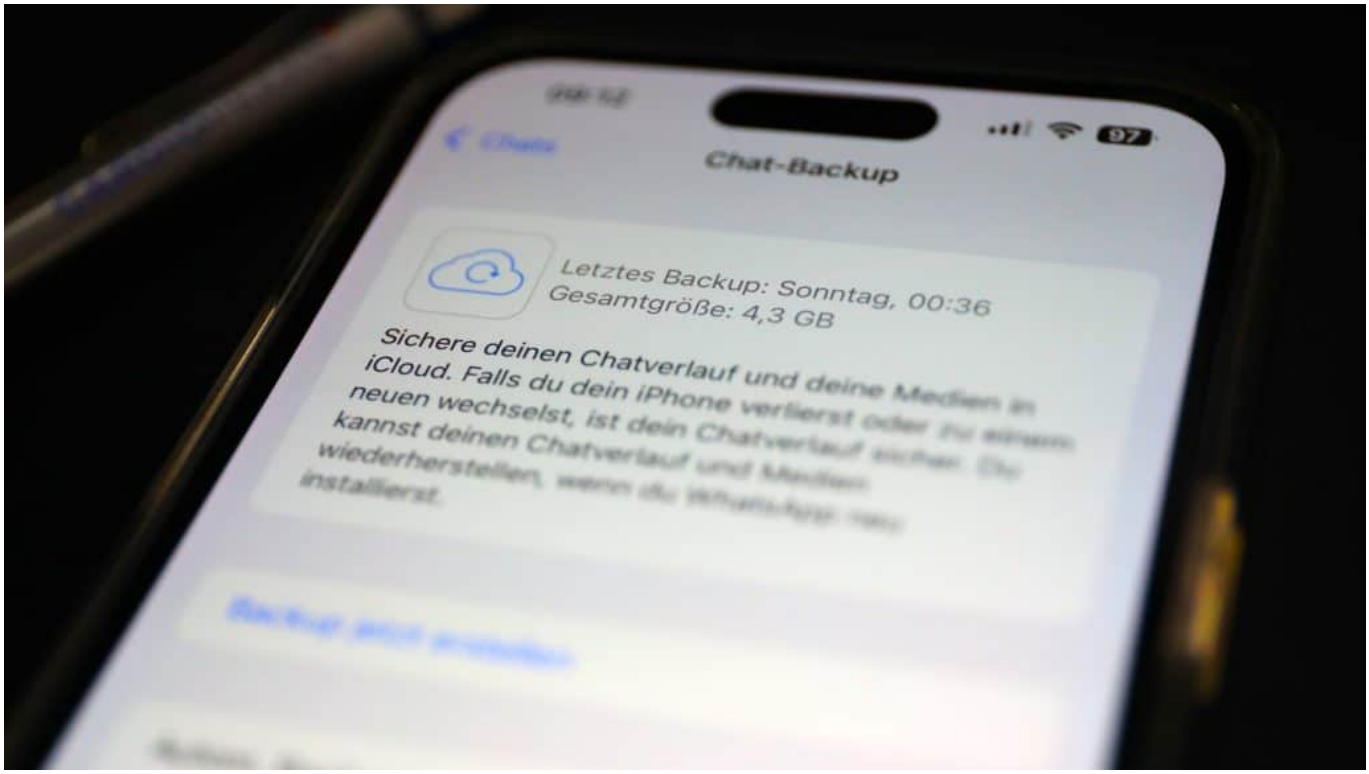
Daten sicher verschlüsselt speichern

Wichtige Daten wie Dokumente oder Dokumente speichern heute ohnehin die

meisten Menschen in der Cloud. Apple und Google bieten ihren Nutzern in ihren Cloud-Diensten entsprechend Speicherplatz zur Verfügung, der komfortabel genutzt werden kann. Die Daten werden verschlüsselt übertragen und gespeichert. Apple bietet ab iOS 16.2 sogar die Möglichkeit an, dass die Daten Ende-zu-Ende-verschlüsselt werden. Was bedeutet, dass wirklich niemand an die Daten kommt – nur der Besitzer.

Ein anderer möglicher Weg ist, die Daten in einem Cloud-Dienst wie iCloud, Google Drive, OneDrive oder Dropbox zu speichern – und ein Plugin wie Boxcryptor oder Cryptomator zu verwenden. Mit den (je nach Umfang) kostenlosen Anwendungen lassen sich die Daten in den handelsüblichen Cloud-Diensten sicher verschlüsseln: Niemand kommt dran – und gleichzeitig können die Daten nicht verloren gehen.

Aber auch das muss rechtzeitig im Handy eingerichtet werden.



Ein Backup von allen WhatsApp Chats in der Cloud

Wichtig: Backups

Die umständlichste Variante wäre ein regelmäßiges manuelles Backup: Smartphone mit dem Rechner verbinden und alle Daten sichern. Auf diese Weise

lässt sich ein Smartphone auch leicht wiederherstellen (oder ein neues Smartphone einrichten).

Allerdings muss man dann darauf achten, solche Backups wirklich regelmäßig durchzuführen. Bequemer sind die Backups in der Cloud. Bei Android mit Google Drive, bei iOS mit iCloud – die entsprechenden Optionen für die automatischen Backups sind in iOS oder Android zu aktivieren.

Vielen liegen vor allem ihre Chats am Herzen. Wer sicherstellen möchte, dass seine Chat-Verläufe selbst bei einem Verlust des Handys nicht verloren gehen, sollte in der Messenger-App die Backup-Funktion aktivieren. Bei den meisten Apps, wie WhatsApp, muss dieses automatische Backup in der App explizit aktiviert werden – aus Sicherheitsgründen. Bei Telegram werden sie ohnehin in der Cloud gespeichert, bei Threema ist ein Backup eher kompliziert.

Vorsicht vor Amazon-Betrügern

Das Internet ist voller Möglichkeiten. Da bleibt es nicht aus, dass auch Verbrecher ihr Unwesen treiben. Der Online-Händler Amazon ist da gerade besonders geplagt. Worauf ihr achten solltet, lest ihr hier.

Aktuelle Betrugsmaschen

Phishing ist bei so gut wie jedem Online-Händler ein Risiko. Cyberkriminelle versuchen, eure Zugangsdaten zu erfahren und diese entweder zu verwenden oder für gutes Geld im Darknet zu verkaufen. Amazon ist allerdings so verbreitet und bietet so viele Waren und Dienste an, dass hier der Aufwand besonders lohnenswert zu sein scheint: So gut wie jeder Anwender hat ein Amazon-Konto, damit ist die Ausbeute einer Phishing-E-Mail besonders hoch, selbst wenn nur ein kleiner Prozentsatz der Angeschriebenen antwortet, bleibt eine große Menge an Zugangsdaten übrig.

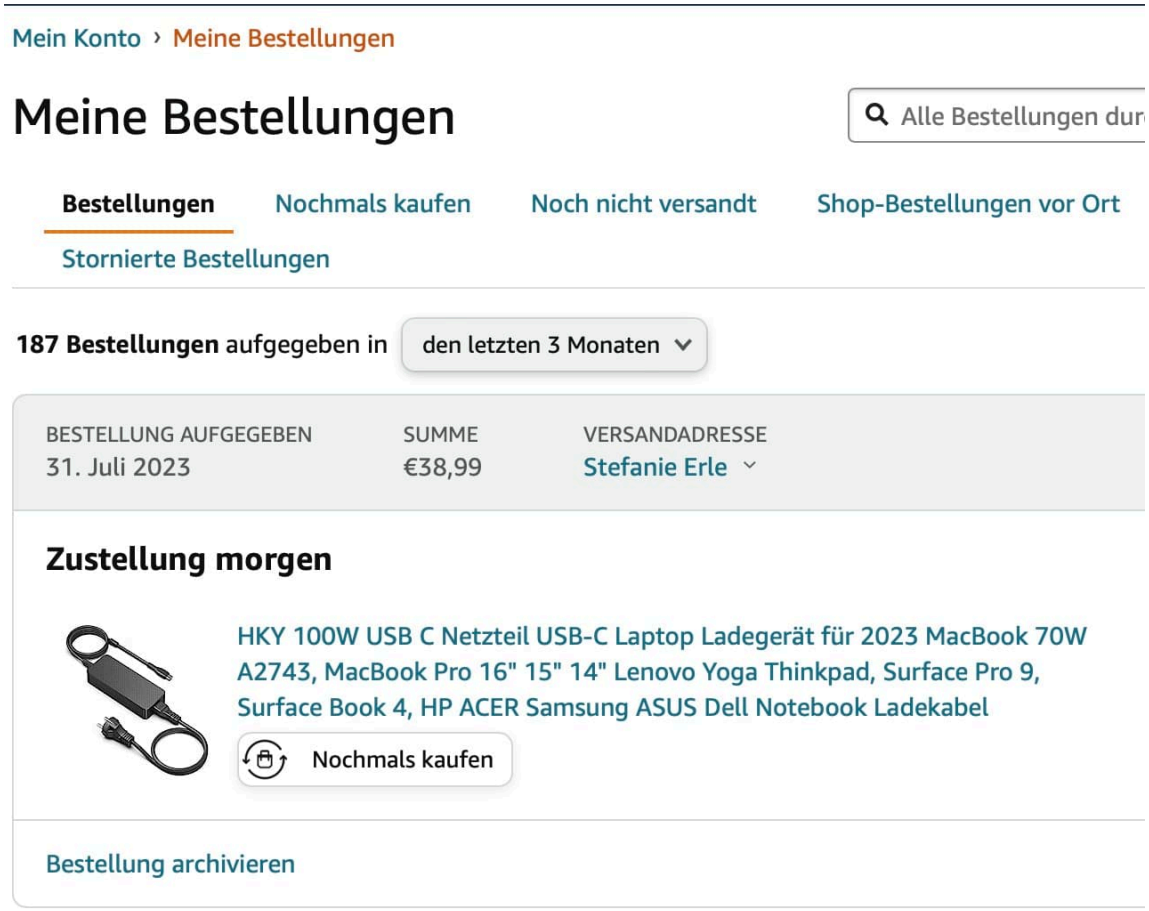
Hier solltet ihr besonders drauf achten:

Ungetätigte Käufe

Wenn ihr eine E-Mail von Amazon bekommt, dass ihr eine teure Ware bestellt habt und die an eine unbekannte Adresse verschickt werden soll, dann widersteht der Panik, die euch zu einem Klick auf den Link in der (Phishing-) E-Mail treibt. Der führt nämlich in den allermeisten Fällen zu einem Portal der Cyberkriminellen, in das ihr eure Zugangsdaten eingeben sollt. Täuschend echt aussehend wie das Amazon-Portal, nur eben nicht von Amazon.

Gescheiterte Zahlung

Die Zahlung für eine Bestellung ist gescheitert? Die Kreditkarte ist abgelaufen oder die Bank hat die Zahlung abgelegt? Das kann mal passieren, in den meisten Fällen aber ist das ein Zeichen für einen Betrug. Auch hier klickt nicht auf den Link, sonst haben die Cyberkriminellen eure Bank- oder Kreditkartendaten.



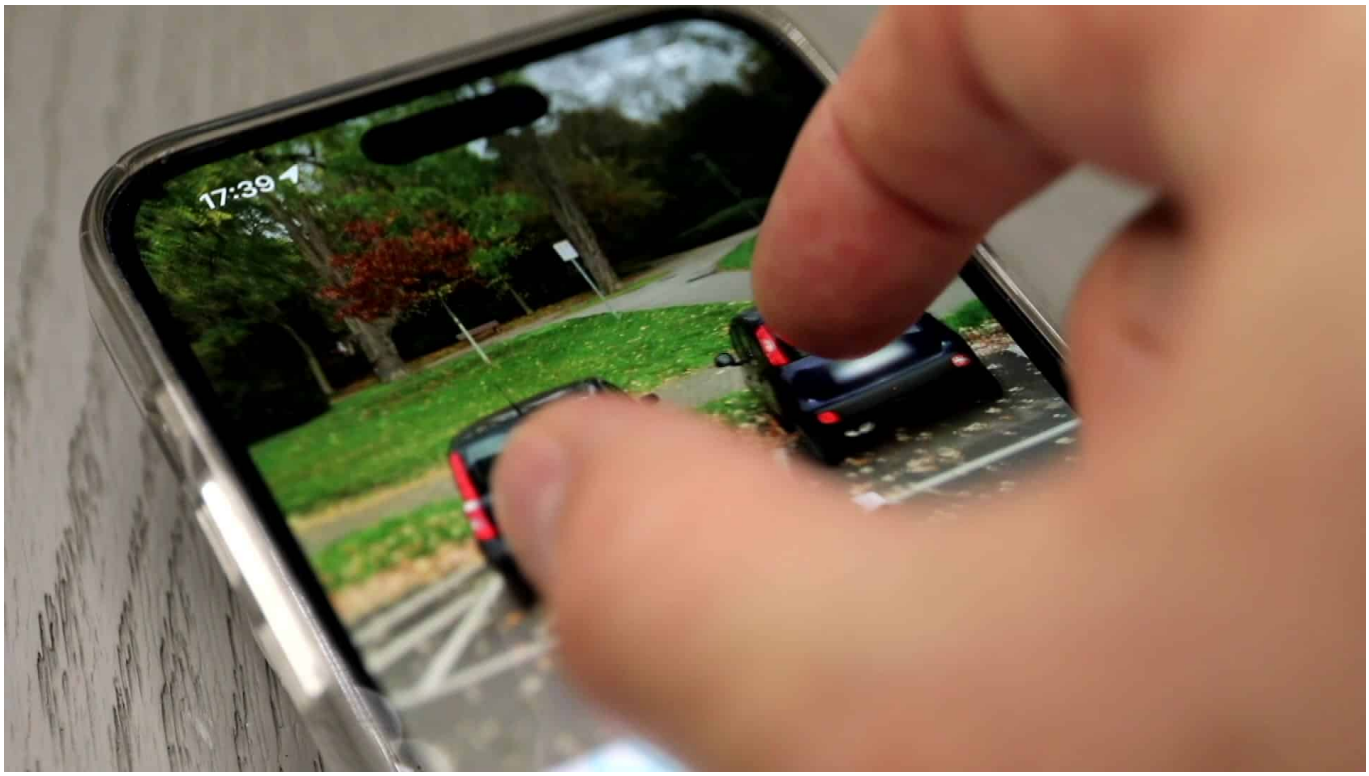
Aufmerksamkeit für mehr Sicherheit

Die Maschen der Betrüger sind gemein, sie sind aber auch meist durchschaubar.

Darauf solltet ihr achten:

- Klickt in keiner e-Mail auf den darin enthaltenen Link, sondern ruft über euren Browser manuell die Amazon-Webseite auf. Auf der klickt auf **Warenrücksendungen und Bestellungen** oben rechts. Damit gelangt Ihr zur Übersicht eurer Bestellungen. Jedes Problem mit einer Zahlung seht Ihr dort auf einen Blick. Und wenn die angebliche Bestellung, die ihr nicht kennt, dort nicht auftaucht, dann gibt es sie auch nicht.
- Nutzt nur offizielle Kanäle: Wenn euch ein angeblicher Amazon-Mitarbeiter anruft und auf eine Bestellung mit einem Problem aufmerksam macht, dann hört euch das an. Wenn ihr dann Informationen preisgeben sollt, dann legt auf und kontaktiert selber den Kundenservice. Das könnt ihr ganz unten auf der Amazon-Seite unter **Wir helfen dir** > **Kundenservice**.

Google Streetview: Neue Aufnahmen von Deutschland



Nach 13 Jahren Pause hat Google jetzt damit begonnen, wieder neue Aufnahmen aus Deutschland bei Streetview online zu stellen. Aufnahmen von 2022 bis heute.

Google Streetview: Kennen Sie. Das ist dieser praktische Service von Google in Google Maps, mit dem man sich überall auf der Welt umschauen kann. So richtig umschauen, dank Panoramafotos. Fast die ganze Welt lässt sich so mit Google Streetview anschauen.

Nur in Deutschland macht das keinen rechten Spaß, denn weil es hier bei der Einführung des Dienstes 2010 so viel Ärger gegeben hat – viele wollten nicht, dass ihre Häuser online zu sehen sind –, hat Google irgendwann gesagt: Schnauze voll. Keine neuen Aufnahmen mehr. Die Folge: Kleinere Orte aus Deutschland sind gar nicht in Google Streetview.

Das Deutsche Fußballmuseum war bislang nicht auf Streetview - jetzt schon

Streetview: Aufnahmen für 13 Jahre eingefroren

Und die, die drin sind, sind auf dem Stand von vor 13 Jahren eingefroren. Die Städte sehen heute teilweise komplett anders aus. Das ändert sich jetzt aber, denn Google hat damit angefangen, wieder neue Aufnahmen in Deutschland zu veröffentlichen.

Das deutsche Fußballmuseum in Dortmund: Bereits 2015 eröffnet – hat es in Google Streetview bislang nicht gegeben. Jetzt ist es endlich zu sehen.

Oder der berühmte Kö-Bogen in Düsseldorf: So sieht er in Wirklichkeit aus... Doch Google Streetview hat uns bis vor wenigen Tagen noch diese Ansicht aus der Vergangenheit präsentiert: Da steht noch der berühmte Tausendfüßler, eine Brücke aus den 60er Jahren.

Der Hanburgische Datenschutzbeauftragte hält die Streetview Aufnahmen für legal

Update erst für großen Städte

Was bringt ein Onlinedienst, der 13 Jahre alte Fotos zeigt? Überhaupt nichts – das verwirrt nur.

Das hat wohl auch Google eingesehen und die Blockade für Deutschland aufgehoben. Endlich gibt es die dringend nötigen Updates.

Von 22 Städten aus NRW hat Google bereits neue, aktuelle Bilder online gestellt. Weitere werden folgen – auch kleinere Orte.

13 Jahre lang gab es in Deutschland keine Updates. In allen anderen Ländern der Welt allerdings hat Google die Aufnahmen in Google Streetview regelmäßig aktualisiert.

Der Grund: Bedenken wegen Datenschutz. Viele Deutsche waren und sind skeptisch – und befürchten, Google könnte in die Wohnungen spionieren oder ihre Privatsphäre sei verletzt. Aufgrund solcher Bedenken hagelte es bei der Einführung von Google Streetview 2010 formale Widersprüche. So viele wie in

keinem anderen Land der Welt.

Schon lange nicht mehr da: Der Tausendfüßler in Düsseldorf

Ende der verpixelten Fassaden?

Die Folge: Verpixelte Fassaden. Das sieht nicht nur blöd aus, sondern bedeutet für Google auch einen enormen Aufwand. Deshalb gab es in Deutschland seit 13 Jahren keine neuen Aufnahmen. Doch jetzt fahren sie wieder auf deutschen Straßen, die Google-Autos mit Kamera – und machen neue Aufnahmen. Laut Google noch bis Oktober.

Der Hamburgische Datenschutzbeauftragte – zuständig, weil Google dort seinen Hauptsitz in Deutschland hat – klärt auf: Die Aufnahmen zu machen und zu veröffentlichen ist rechtlich zulässig. Weil ein übergeordnetes, allgemeines Interesse besteht. Wichtig nur: Gesichter und Nummernschilder müssen verpixelt werden. Das passiert auch. Automatisch. Selbst bei Werbung.

Bessere Bildqualität

Ich persönlich begrüße es, dass Streetview wieder Aufnahmen in Deutschland macht. Die Aufnahmen sind nicht nur aktuell, sondern auch in deutlich besserer Qualität.

Die Kameras machen heute erheblich bessere Bilder als noch vor 13 Jahren.

Was kein Wunder ist: Das ist bei unserem Smartphone ja genauso.

Google spekuliert wohl darauf, dass sich die Zeiten geändert haben – und heute weniger Menschen Bedenken haben. Und wie es aussieht, ist es wohl auch so.

Heute fallen die Reaktionen oft positiver aus. Viele begrüßen die Aktualisierungen.

Dennoch: Wer widersprechen will, kann das in einem Online-Formular für die neuen Aufnahmen machen. Oder per E-Mail. Ein alter Widerspruch von früher gilt nicht mehr.

Wenn iOS-Updates Speicher blockieren

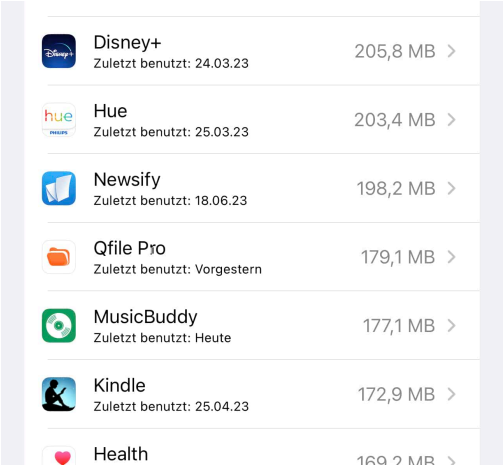
iOS-Updates sind generell gut. Sie schließen Sicherheitslücken und bringen neue Funktionen. Wenn aber der Speicher eh schon knapp ist, dann können sie auch stören. Wir zeigen euch, wie ihr Speicher- und Updatebedarf aufeinander abstimmt!

Unvollständige Updates löschen

iOS lädt die Update-Dateien im Normalfall schon dann herunter, wenn Apple sie zum Download bereitstellt. Die Installation erfolgt dann in einer Ruhephase des Geräts. Der Prozess ist so einfach, dass dabei nichts schiefgehen sollte. Was natürlich nicht immer der Fall ist: Wenn der Download nicht einwandfrei funktioniert, dann habt Ihr gegebenenfalls ein unvollständiges Update im Speicher. Beispielsweise, wenn der Server die Verbindung abbricht oder eure Internetverbindung unterbrochen ist.

Das führt dazu, dass das Update nicht mehr heruntergeladen werden kann und zusätzlich noch Speicher auf eurem iPhone belegt. So könnt ihr die unvollständige

Datei löschen:



- Tippt in den **Einstellungen** von iOS auf **Allgemein**.
- Öffnet durch ein Tippen auf **iPhone-Speicher** die Übersicht des belegten Speichers.
- Ein iOS-Update findet ihr in der Liste der Apps unter i**OS** . Hier müsst ihr manuell suchen, denn die Liste ist nicht alphabetisch sortiert.
- Tippt das Update an, dann auf **Update löschen**.
- Startet das iPhone einmal neu.
- Der Speicher wird freigegeben und der Download ist wieder möglich.

Deaktivieren von Updates

Vorab: Das solltet ihr nur im absoluten (Speicher-) Notfall machen: Updates haben ihren Sinn und schützen euch. Manchmal ist der Speicher aber so knapp, dass der Download zu Problemen führt. Wenn ihr nicht direkt Zeit habt, diesen aufzuräumen, dann kann ein zeitweises Deaktivieren der Updates euch ein wenig Luft verschaffen:

- Tippt in den Einstellungen auf **Allgemein** > **Software-Update**.
- Tippt dann auf **Automatische Updates** und deaktiviert **iOS-Updates laden**.
- Aktiviert diese Funktion auf jeden Fall, wenn der Speicher wieder ein wenig Luft habt!

Wenn es euch nicht darum geht, Speicher zu sparen, ihr aber den Updates nicht traut und abwarten möchtet, ob ein Update Probleme verursacht, dann könnt ihr stattdessen nur **iOS-Updates installieren** deaktivieren. Dann werden die Updates geladen, aber erst nach Eurer Freigabe installiert.

Outlook: Kalender freigeben - aber richtig

Wenn ihr in einem Team gemeinsam arbeitet, dann kommt es oft auch darauf an, gemeinsam Termine abzustimmen. In Outlook könnt ihr Kalender freigeben. Da können kleine Fehler aber große Auswirkungen haben!

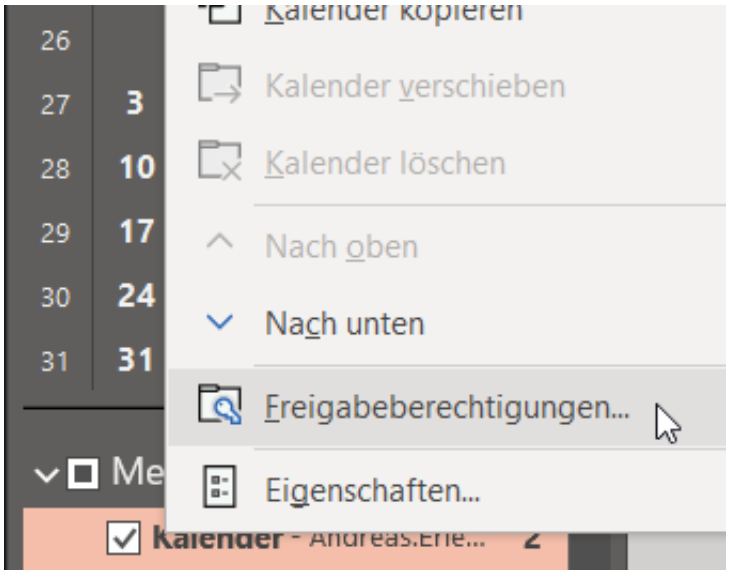
Zugriff auf Kalender in Outlook

Um auf einen fremden Kalender in Outlook zugreifen zu können, habt Ihr drei Möglichkeiten:

- Das Abonnieren eines Kalenders: Das bezieht sich meist auf öffentlich verfügbare Kalender wie Feiertage, Bundesligaspiele oder Schulferien.
- Das Einbinden eines anderen Postfaches: Damit habt ihr dann kompletten Zugriff auf alle Elemente des Postfaches, das macht Sinn, wehr ein Funktionspostfach neben Eurem eigenen, persönlichen Postfach

verwaltet, beispielsweise das Info@-Postfach einer Webseite.
- Die Freigabe des Kalenders des Benutzers mit unterschiedlich starken Berechtigungen und die Nutzung dieser Berechtigungen durch einen anderen Anwender.

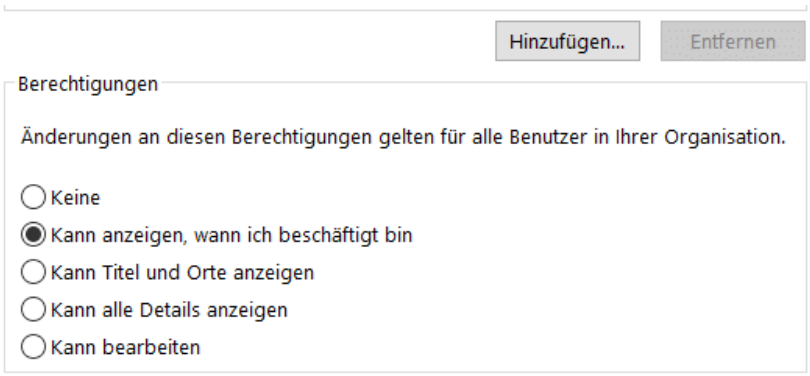
Der letzte Fall ist der, der euch am häufigsten begegnen wird: Im Team wollt Ihr die Termine (und manchmal auch Details) der Kollegen sehen.



Freigabe von Kalendern

Um einen Kalender in Outlook freizugeben, geht wie folgt vor:

- Klickt in Outlook auf das Symbol des **Kalenders** unten in der Symbolleiste.
- Links in der Spalte seht Ihr dann Euren Kalender.
- Klickt mit der rechten Maustaste darauf, dann auf **Freigabeberechtigungen**.
- Outlook zeigt Euch die aktuellen Berechtigungen für andere Benutzer in einer Liste an.
- Klickt auf **Hinzufügen**, um eine neue Freigabe hinzuzufügen.



Wichtig sind hier die Berechtigungsstufen, die ihr für den hinzugefügten Benutzer festlegen müsst:

- **Keine:** Der Benutzer sieht nur eine graue Linie als euren Kalender, aber nicht mal die Frei-/Belegt-Zeiten.
- **Kann anzeigen, wann ich beschäftigt bin**: Der Benutzer sieht die Balken von Terminen und die Art des Termins (Belegt, unter Vorbehalt, außer Haus), aber keine Titel.
- **Kann Titel und Orte anzeigen**: Die Option gibt euch Zugriff auf die Details der Termine im Kalender, aber nicht auf Teilnehmer, Anhänge oder andere Inhalte. Das wird die am meisten verwendete Freigabeform sein.
- **Kann alle Details anzeigen**: Jedes einzelne Detail des Kalenders liegt den Benutzern offen, die diese Berechtigung haben, inkl. aller anhängenden Dokumente. Dier solltet ihr genau abwägen, ob das nicht zu weitgehend ist. Beispielsweise, wenn vertrauliche Dokumente in den Terminen hängen.

All diese Freigaben sind rein lesende Freigaben, der Benutzer, der sie erhält, kann an eurem Kalender nichts ändern. Das geht erst, wenn ihr **Kann bearbeiten** anwählt.

Wenn es sich bei dem einzurichtenden Vertreter handelt (und keine Benutzergruppe), dann könnt ihr eine zusätzlich Option anwählen: **Stellvertreter**. Dieser hat dann nicht nur alle Rechte auf die Elemente des Kalenders, sondern kann zusätzlich auch noch in Eurem Namen Termine versenden.

Was ist eigentlich Gamification?

Kinder erkunden die Welt spielend - und lernen auch durch Spielen. Wenn wir Erwachsenen das tun, wird das oft als "Gamification" bezeichnet. Aber was bedeutet der Begriff genau?

Die Anwendung von Gamification kann vielfältig sein und reicht von einfachen Mechanismen wie Punktesystemen und Abzeichen bis hin zu komplexen Systemen mit Ranglisten, Fortschrittsbalken, Herausforderungen, Avatar-Individualisierung und sozialen Interaktionsmöglichkeiten. Die Techniken und Elemente werden geschickt eingesetzt, um die Benutzerbindung zu verbessern und sie dazu zu ermutigen, bestimmte Handlungen auszuführen, Informationen zu lernen, produktiver zu sein oder auf andere Weise an der gewünschten Aktivität teilzunehmen.

Um Gamification effektiv einzusetzen, müssen Entwickler und Designer das Verständnis für die Zielgruppe und ihre Motivationen vertiefen. Die Auswahl der

richtigen Elemente, die zum Kontext der Anwendung passen, ist entscheidend. Einige häufige Gamification-Elemente sind:

1. Punkte und Belohnungen: Punkte werden den Benutzern für bestimmte Aktionen oder Leistungen vergeben und können dann gegen Belohnungen, wie z. B. virtuelle Gegenstände, Upgrades oder Zugang zu weiteren Funktionen, eingelöst werden.
2. Fortschrittsbalken und Levels: Die Darstellung des Fortschritts in Form von Leveln oder Balken kann den Anreiz erhöhen, kontinuierlich weiterzumachen und das nächste Ziel zu erreichen.
3. Abzeichen und Auszeichnungen: Die Vergabe von Abzeichen für spezifische Erfolge oder Meilensteine fördert den Wettbewerb und die Erfüllung von Herausforderungen.
4. Wettbewerbe und Ranglisten: Die Möglichkeit, gegen andere Benutzer anzutreten und sich auf Ranglisten zu platzieren, erhöht den Anreiz, sich zu verbessern und seine Position zu verteidigen.
5. Storytelling und Narration: Die Verwendung von Geschichten und Erzählungen kann die emotionale Bindung verstärken und den Benutzern helfen, sich besser mit dem Kontext der Anwendung zu identifizieren.
6. Soziale Interaktion: Die Integration von sozialen Elementen, wie z. B. die Möglichkeit, Erfolge mit anderen zu teilen oder Freunde einzuladen, kann den Community-Aspekt stärken und das Engagement steigern.

Gamification erfordert sorgfältige Planung

Es ist wichtig zu beachten, dass Gamification nicht immer für jeden Anwendungsfall geeignet ist. Es erfordert eine sorgfältige Planung und Umsetzung, da übermäßige oder unangemessene Gamification auch zu einer Ablenkung oder gar Frustration der Benutzer führen kann. Die Gamification-Elemente sollten organisch in den Kontext integriert werden und das Hauptziel ist es, eine positive und sinnvolle Erfahrung zu schaffen, die das gewünschte Verhalten fördert, ohne die Authentizität oder den eigentlichen Zweck der Anwendung zu beeinträchtigen.

In der heutigen Zeit, in der Technologie eine immer wichtigere Rolle in unserem Leben spielt, findet Gamification breite Anwendung in den verschiedensten Bereichen. Von Lernplattformen und Bildungs-Apps, die Schülerinnen und Schüler motivieren, sich aktiv am Lernprozess zu beteiligen, über Fitness-Apps, die Nutzerinnen und Nutzer zu einem aktiven Lebensstil anspornen, bis hin zu Kundenbindungsprogrammen in Unternehmen, die Kunden zur wiederholten Nutzung von Produkten oder Dienstleistungen anregen möchten. Gamification

bietet ein innovatives Instrument, um das Engagement und die Zufriedenheit der Nutzer zu steigern und sie auf spielerische Weise in den Prozess einzubinden.

Digitale EUR: Sollten wir wirklich ganz auf Bargeld verzichten?

In 2025 kommt der digitale Euro: Eine komplette digitale Variante, die wir in der "Wallet" speichern - und damit alles bezahlen können (sollen). Was dahinter steckt und was das fürs Bargeld bedeutet.

Rechnung bezahlt mit Karte oder mobil: An der Supermarktkasse hält man nur Handy oder Uhr an die Kasse, und selbst auf dem Flohmarkt oder bei Kleinanzeigen überweisen viele das Geld ganz einfach per Paypal. Ein bisschen schwierig wird es vielleicht beim Trinkgeld, da sucht mancher schon mühesam nach ein paar Münzen und ärgert sich, warum das nicht auch digital geht.

Bargeldlos zu zahlen, das ist einfach und super bequem und hat sich in den vergangenen Jahren auch bei uns an vielen Stellen durchgesetzt.

Bargeld wird digital

Brauchen wir eigentlich noch Bargeld

... oder können wir komplett drauf verzichten?

Noch brauchen wir Bargeld. Schon allein deswegen, weil längst nicht alle Händler in Deutschland auf bargeldloses Bezahlen eingestellt sind –In Skandinavien ist das bereits anders. Da gibt es Landstriche, da wird kein Bargeld mehr angenommen: von den Händlern. Aber in Deutschland ist es noch lange nicht so weit. Viele auch Verkäufer und Dienstleister hängen hier am Bargeld. Laut der Deutschen Bundesbank wurden im Jahr 2021 insgesamt 1,2 Billionen Euro in Deutschland gezahlt. Davon immer noch 67% in bar und nur 1% mit Zahlungsmethoden wie PayPal und co. Aber das digitale Zahlen nimmt zu. .

Finden viele von uns ja auch sehr bequem, aber Trinkgeld und auch Geldgeschenke gehen natürlich besser mit Münzen und Scheinen.

Und Bargeld hat den Vorteil: Es ist komplett anonym. Niemand weiß, wer den 20-EUR-Schein vorher besessen hat. Wer, wen, wann, wofür bezahlt hat. Das ist

bei Kredit- und Plastikkarten anders, auch beim Mobile Payment: Da fallen stets Daten an. Mal bei der Bank, mal bei der Kreditkarte oder bei Paypal, Google oder Apple, wenn wir mit deren Zahlungssystemen bezahlen.

Hier handelt es sich also nie um komplett anonyme Zahlungsvorgänge. und Beim Bezahlen mit Karte oder Mobile Payment fallen jedes Mal Gebühren an. Ein, zwei, drei Prozent, die sich die Banken, Paypal oder die Kreditkartenfirmen in die Tasche stecken. So wird Geld immer weniger wert, je öfter es diesen Prozess durchläuft. Mit Bargeld zahlen heißt auch: Am Bankensystem weitgehend vorbei bezahlen.

Bargeld birgt auch Risiken

Okay, Bargeld ist anonym, direkt, am System vorbei. Aber ist das denn gut oder schlecht? Klingt ja auch nach viel Missbrauchspotential?

Es ist nicht gleich Missbrauch, wenn ich mich wohler fühle, etwas bar zu zahlen. Ein Trinkgeld. Das Geburtstags- oder Hochzeitsgeschenk. Der Schrank auf dem

Trödelmarkt. Oder weil es sich für mich besser anfühlt, weil ich keine Daten bei einem großen Konzern hinterlassen möchte... Jeder hat andere Befindlichkeiten. Es kann ja auch sein, dass gerade meine EC-Karte schon überlastet ist – und ich bar bezahlen muss, weil es für einz, zwei Tage nicht anders ginge. Es gibt viele gute Gründe.

Aber es stimmt schon: Es besteht auch ein MissbrauchsRisiko: Anonymität und Unmittelbarkeit von Bargeld erleichtern illegale Aktivitäten, etwa Schwarzgeldkassen und Geldwäsche. Fast nirgendwo in Europa kann noch so viel mit Bargeld bezahlt werden, selbst Grundstücke oder Autos, wie in Deutschland. Auch Steuerhinterziehung und Schwarzmarkttransaktionen werden mit Bargekd erheblich vereinfacht. Da wäre es natürlich schon im Interesse der Allgemeinheit, wenn das eingeschränkt würde.

Wenn beim Bezahlen Daten anfallen

Bei den digitalen Bezahlungsmethoden fallen immer Daten an. Warum soll das da ein Problem sein: Es fallen doch heute überall Daten an?

Das stimmt – aber gerade meine Bezahldaten sagen viel über mich aus: Was kaufe ich? Gebe ich viel Geld für Sportartikel aus – oder für Pasta? Oder regelmäßig für Lieferdienste? Wie und wo kaufe, was bin ich bereit auszugeben. Kreditkartenfirmen haben schon eine Menge Daten und wissen viel über ihre Kunden. Einige nutzen das auch, um gezielt Werbung zuzusenden. Aber da lässt sich natürlich viel mehr zusammentragen. Auch, wie umsichtig ich mit meiner Gesundheit bin.

Aber Apple und Google Pay z.B. verraten einem Händler nicht, wer da gerade gekauft und bezahlt hat. Der Händler hat weniger Daten als wenn ich meine Kreditkarte zücke – der Händler bekommt nur ein Signal: Bezahlt. Dafür haben aber Google oder Apple mehr Daten. Bei Paypal bekommt der Händler immer alle Daten vom Kunden, neben der Mail-Adresse auch die Adresse und vieles andere mehr. Und Paypal sebst sitzt auch auf einem fetten Datenberg.

Und die Daten landen natürlich in den USA. Wo wir nicht wissen, was mit ihnen passiert. Anders könnte das mit dem so genannten digitalen Euro werden, der in den Startlöchern steht, Schon sehr bald brauchen wir kein Apple Pay, Paypal oder Kreditkartenkonto mehr, um digital zu zahlen. Denn es kommt das digitale europäische Bargeld.

Was kann der digitale Euro?

Er soll 2025 kommen, als gesetzliches Zahlungsmittel und überall akzeptiert, also gleichwertig mit „echtem“ Bargeld. Er wird von der Europäischen Zentral Bank EZB ausgegeben werden und mit Bargeld gleichgestellt. Er soll sicher, effizient und einfach zu verwenden sein. Das sind schon mal wichtige Kriterien. Anders als beim Bitcoin, der extremen Kursschwankungen unterworfen ist, wird es das beim digitalen EUR nicht geben: Ein digitaler EUR ist wie eine EUR-Münze. Gleich viel wert. Der digitale Euro würde in einer elektronischen Geldbörse verwahrt, die man zum Beispiel als Wallet-App im Smartphone bei sich trägt. Das ist dann keine Verbindung mit einem Bankkonto wie bei Paypal, oder Google und Apple Pay, sondern digitales Geld im Smartphone.

Aber was macht der dann besser? Da sind doch die gleichen Probleme wie bei den bisherigen Methoden, oder?

Keineswegs, denn rechtlich ist der digitale EUR dann dasselbe wie Bargeld.

Aber einiges ist auch noch unklar, etwa wie viel Daten da anfallen, was der Staat nachvollziehen kann, etc….Weniger anonym als Bargeld, aber weniger Daten als bei Paypal, Kreditkarte und Co.

Und technisch soll der digitale Euro auch anders laufen, als es beim bisherigen bisherigen Mobile Payment ist: Verbraucher können ihren Einkauf bezahlen, ohne eine Bank, einen Kreditkartenanbieter oder Zahlungsdienstleister zwischenschalten zu müssen. Wie beim Bargeld soll das auch offline möglich sein, ohne internetverbindung. Und weil der digitale EUR ein gesetzliches Zahlungsmittel ist, muss man auch nicht fragen: „Geht digitaler EUR?“ Denn Händler im gesamten Euro-Währungsgebiet wären grundsätzlich verpflichtet, den digitalen Euro anzunehmen. Keine Diskussionen!

Der digitale Euro ist eine Form von elektronischem Geld, das von der Europäischen Zentralbank herausgegeben wird. Der digitale Euro ist das elektronische Pendant zu physischen Euros und kann genauso verwendet werden, wie Sie es von Bargeld gewohnt sind, nur in digitaler Form.

Bezahlen mit dem digitalen Euro

Bevor wir auf die Schritte zur Verwendung des digitalen Euro eingehen, lassen Sie uns zuerst den Begriff "Wallet" oder "digitale Geldbörse" klären. Eine digitale Geldbörse oder Wallet ist eine Software-Anwendung, in der digitale Währungen sicher gespeichert und verwaltet werden können. Sie ermöglicht es den Nutzern, digitale Währungen zu empfangen, zu senden und zu verwalten.

Hier ist eine schrittweise Anleitung, wie das Bezahlen mit dem digitalen Euro und einer Wallet funktioniert:

Schritt 1: Einrichten einer digitalen Wallet Das Bezahlen mit dem digitalen Euro erfordert zunächst das Einrichten einer digitalen Wallet. Es gibt verschiedene Anbieter, aus denen Sie wählen können, je nachdem, welche

Funktionen Sie benötigen. Die Einrichtung einer Wallet umfasst im Allgemeinen die Erstellung eines Kontos und das Einrichten von Sicherheitsmaßnahmen wie Passwörtern und biometrischer Authentifizierung.

Schritt 2: Digitalen Euro in Ihrer Wallet aufladen Nachdem Sie eine Wallet eingerichtet haben, müssen Sie diese mit digitalem Euro aufladen. Dies kann in der Regel durch den Kauf von digitalem Euro mit herkömmlichem Geld auf einer Bank oder einer Krypto-Börse erfolgen. Der digitale Euro wird dann in Ihrer Wallet gespeichert.

Schritt 3: Zahlung tätigen Um eine Zahlung mit digitalem Euro zu tätigen, müssen Sie normalerweise die Adresse des Empfängers (entweder manuell eingegeben oder durch Scannen eines QR-Codes) in Ihrer Wallet-App eingeben und dann den zu sendenden Betrag angeben. Sobald Sie die Transaktion bestätigen, wird der Betrag in digitalem Euro von Ihrer Wallet an die Wallet des Empfängers gesendet.

Schritt 4: Transaktionsbestätigung Nach der Durchführung der Transaktion erhalten Sie in der Regel eine Bestätigung in Ihrer Wallet-App. Dies kann einige Minuten dauern, da Transaktionen in der Regel von einem Netzwerk validiert werden müssen. Sobald die Transaktion bestätigt wurde, wird der Betrag von Ihrer Wallet abgezogen und auf die Wallet des Empfängers übertragen.

Es ist zu beachten, dass die genauen Details, wie die Bezahlung mit dem digitalen Euro funktioniert, variieren können, je nachdem, welche Wallet und welchen Service Sie verwenden. Daher ist es immer wichtig, die Anweisungen des jeweiligen Anbieters zu befolgen.

Fazit

Bargeld s wird es auch weiter geben. Eine Abschaffung ist nicht geplant. Das sagt die EZB auch klipp und klar. Es ist gut, dass die EZB den Weg mit dem digitalen Geld geht. Echte Alternative zu den US-Konzernen und Playern. Und auch bei den Verkäufern wird es Ausnahmen geben, die sagen dürfen, nein ich nehme nur Bares, Der kleine Kiosk oder Händler auf dem Trödelmarkt, der bisher nur Bargeld annimmt, weil er kein Kartenlesegerät hat, soll nicht zum digitalen EUR gezwungen werden. Aber ehrlich gesagt denke ich, das wird sich schnell durchsetzen.

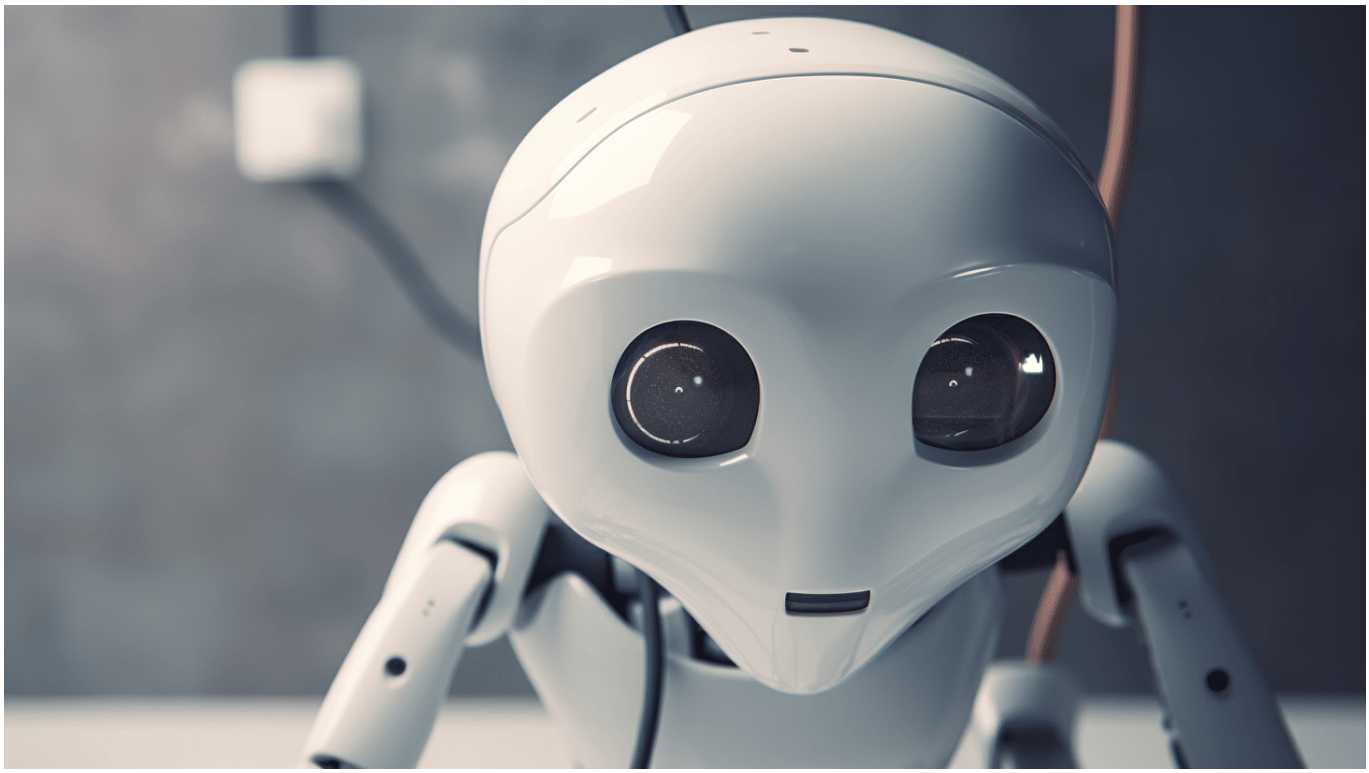
Denn wer auch selbst mit digitalem EUR bezahlt, kann „zur Not“ auch mit der App Geld annehmen. In China ist das längst Usus. Nicht mit einer von der Zentralbank ausgegebenen digitalen Währung, denn mit der App „Wechat“ von Tencent: Die hat jeder auf dem Handy, weil damit alles gemacht werden kann. Auch Bezahlen. Das wird mit dem digitalen EUR auch gehen, dass man sich gegenseitig Geld zuschickt – ohne Gebühren.

Fassen wir zusammen: Bargeld ist anonym, hat meist keine versteckten Folgekosten bei Daten oder Gebühren – aber digital ist meist bequemer, schneller und reduziert krumme Geschäfte, was ja eigentlich wieder gut für die Gesellschaft ist. Und in den nächsten Jahren werden verschiedene digitale Bezahlmöglichkeiten wohl überall verfügbar sein. Sollten wir irgendwo am Bargeld festhalten?

Ja als Backup auf jeden Fall. Bargeld erfordert kein technisches Wissen oder Zugang zu technologischer Infrastruktur und funktioniert eben auch bei Stromausfall oder wenn ein Software-Update hängt. Das gab es in den vergangenen Jahren schon ein paar Mal, dass in bestimmten Läden die Software-Terminals ausfielen und es doch nur bar ging. Und beim Trinkgeld finden es meist die Menschen auch schöner, das in bar zu bekommen.

Eine Gesellschaft ganz ohne Bargeld ist durchaus vorstellbar – aber ich glaube nicht, dass sie so schnell kommt.

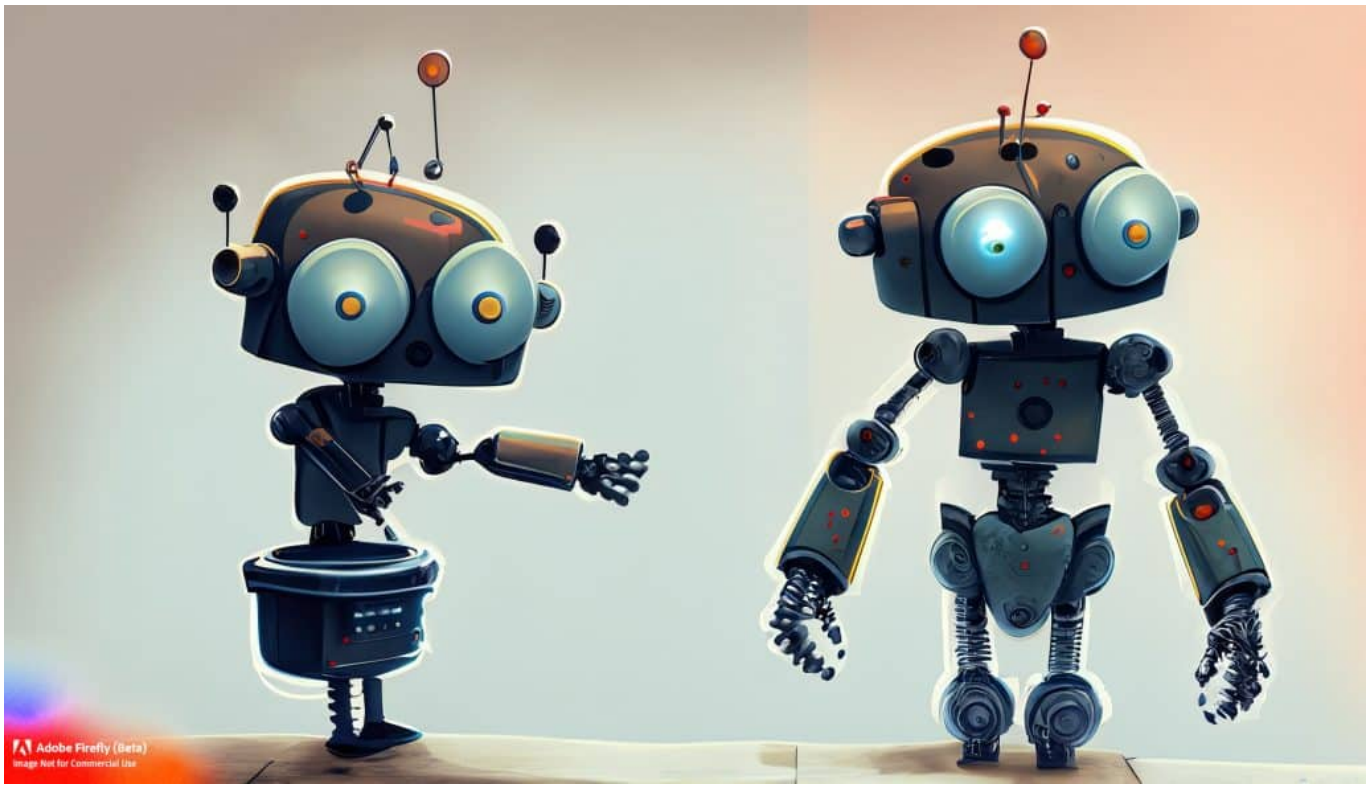
Generative KI: Das endgültige Ende der Wahrheit?



KI kann nicht nur analysieren, sondern auch generieren: ChatGPT erstellt Texte, Midjourney Bilder und ElevenLabs Audios. Selbst Videos können KI-Systeme heute erzeugen. Was ist noch wahr - und was kann man noch glauben?

Fakt ist: Fake-Meldungen verbreiten sich schneller als wahre, seriöse Nachrichten.

Ein Grund: Die Algorithmen, die bestimmen, welche Nachrichten uns in den Sozialen Medien ausgespielt werden, kümmern sich nicht um Wahrheitsgehalt oder Allgemeinwohl, sondern interessieren sich für maximale Erregbarkeit des Publikums. "Erregungsökonomie“ wird das genannt – Fake News, meist überspitzte oder schockierende Nachrichten, triggern die User, sorgen für eine maximale Performance und fahren somit auch einen hohen Profit ein.



GAN: KI-Systeme trainieren sich gegenseitig

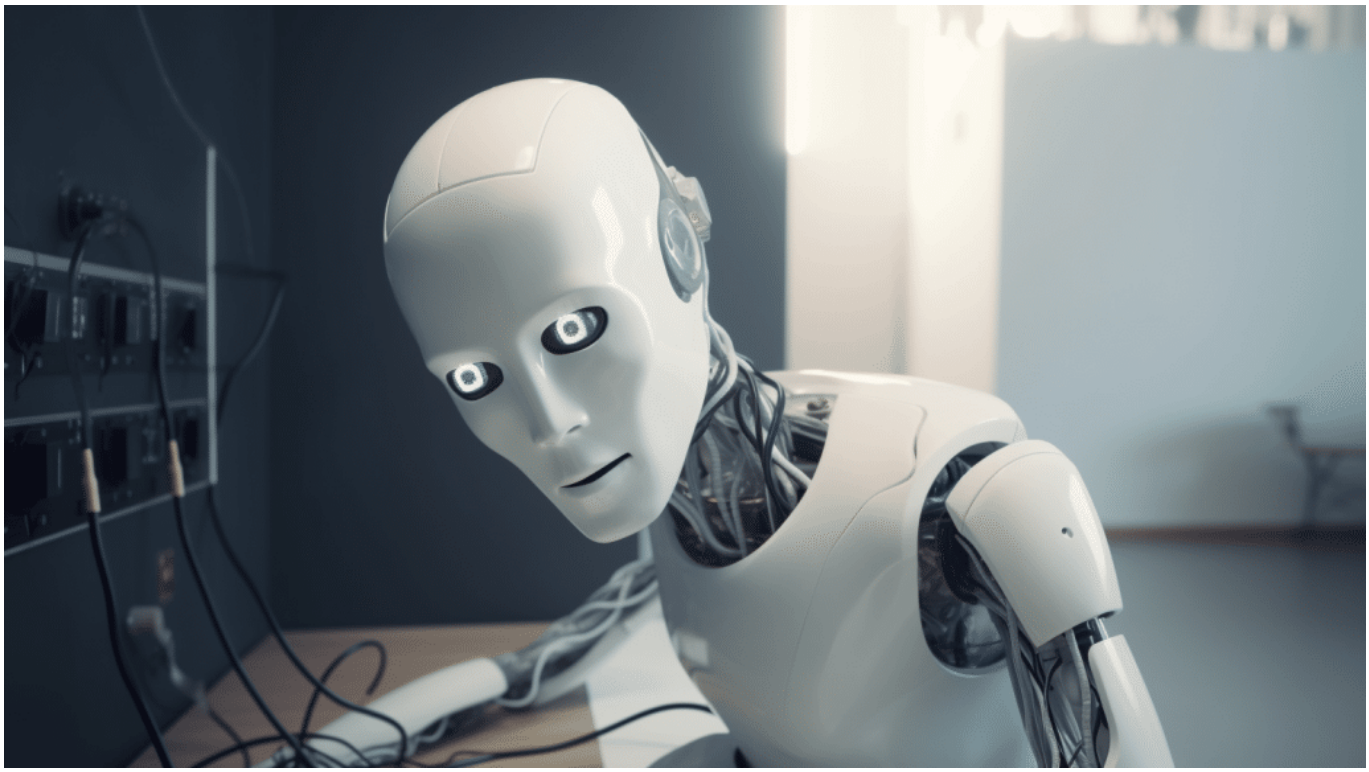
Generative KI

Hinzu kommt: Mit generativen Künstlichen Intelligenzen (KI) wie *ChatGPT*, *Midjourney*, *D-ID* und Co. lassen sich nicht nur Fake News sondern Fake Content jeder Art im Blitztempo erzeugen – und das von sprichwörtlich jedem.

Eine gefährliche, unheilvolle Entwicklung. Denn wir wissen ganz genau, wie wirkmächtig Informationen und Desinformationen sind – damit lässt sich das Weltgeschehen maßgeblich beeinflussen: So behauptete der damalige US-Außenminister **Colin Powell** im Jahr 2003 vor den Vereinten Nationen, der Irak besitze Massenvernichtungswaffen.

Als Beleg präsentierte er dem Sicherheitsrat Satellitenaufnahmen, Tonaufzeichnungen und Augenzeugenberichte. Später stellte sich heraus, dass die Belege manipuliert wurden. Powell entschuldigte sich – und dennoch kann diese Rede, die auf Fehlinformationen und manipuliertem Bild- und Tonmaterial basierte, als Auftakt des Irak-Krieges verstanden werden.

Was vor einigen Jahren nur im Laborbetrieb möglich war, geht heute theoretisch an jedem Laptop mithilfe eines AI-Tools.



Deepfakes: Texte, Bilder, Audios und Videos aus der KI - technisch immer besser

Generative KI erzeugt Fake-News-Material auf Knopfdruck

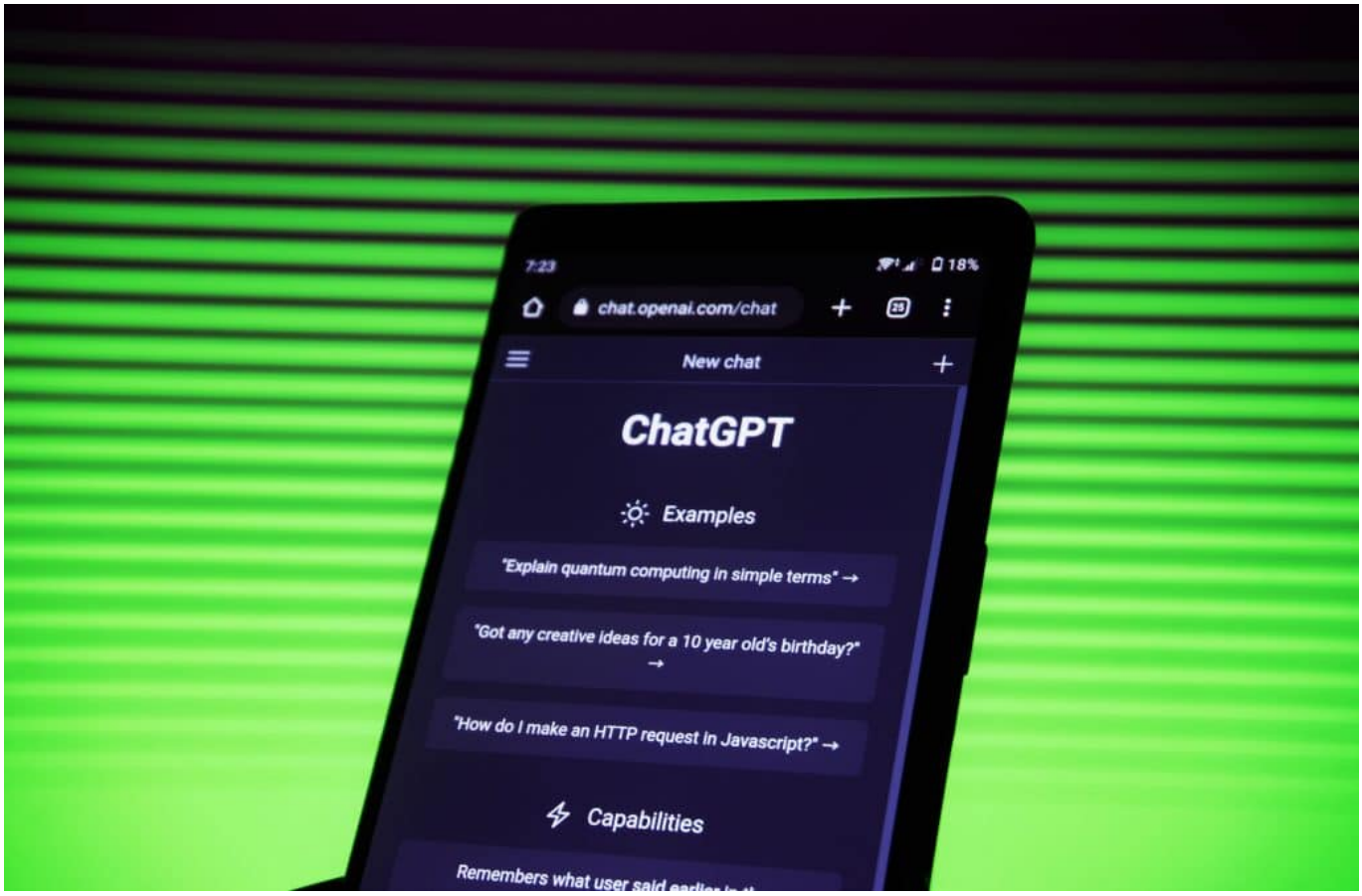
So kann heute praktisch jeder Beweise fälschen: Fotos von angeblichen Treffen, vermeintlich abgehörte Gespräche, vertrauliche Worte – all das lässt sich in guter Qualität mit Hilfe von Künstlicher Intelligenz herstellen. Dazu braucht es weder eine besondere Ausbildung, noch sonderlich viel Kapital: *ChatGPT* formuliert die Texte und kann dabei täuschend echt den gewünschten Schreibstil nachahmen.

Auch Fotos können von KI-Modellen wie *Midjourney* oder *Stable Diffusion* erstaunlich realistisch gefälscht werden. Andere KI-Systeme sprechen auf Wunsch mit der Stimme jedes Menschen auf dem Planeten. Es braucht nur wenige Sätze, um die KI zu trainieren. Und was noch vor wenigen Monaten künstlich klang, ist heute – zumindest in englischer Sprache – schon verblüffend nah an der Realität.

Wenn wir nicht aufpassen, kann generative KI eine unheilvolle Entwicklung in Gang bringen. Nicht etwa, weil die KI-Systeme das wollten oder dafür gemacht wären, sondern weil Menschen es ihnen abverlangen.

Weil irgendwo auf der Welt Menschen die wahrlich beeindruckenden

Möglichkeiten der KI nutzen, um sich zu bereichern, um Macht auszuüben und Schaden anzurichten. Schon geraten die vielen positiven und beeindruckenden Fähigkeiten von KI ins Hintertreffen.



ChatGPT ist schon länger am Start - und bekommt jetzt Konkurrenz

Der Paradigmenwechsel

Fotos, Videos und Audios hatten bislang einen höheren „Trust“, das heißt mehr Glaubwürdigkeit als aufgeschriebene Worte: Wer ein Foto sieht, ist eher bereit etwas zu glauben. Wer etwas mit eigenen Augen sieht oder mit eigenen Ohren hört, ist nur noch schwer davon zu überzeugen, dass etwas anders gewesen sein könnte. Diese Glaubwürdigkeit wird durch den Missbrauch von KI zur Erstellung von Deepfakes untergraben.

In der Folge werden wir unseren Augen nicht mehr trauen. Denn wer will sich schon noch zutrauen, zuverlässig zwischen wahr und falsch zu unterscheiden, wenn Audios, Fotos und Videos nahezu und schon bald absolut perfekt gefälscht werden können?

Da stellt sich eine entscheidende Frage: Was sollen, was können wir noch glauben?

Wir haben diesem Fake-Tsunami bislang nicht wirklich etwas entgegenzusetzen.

Nicht als einzelne User und Medienkonsumenten, aber auch nicht als Gesellschaft. Wir sind einfach nicht darauf vorbereitet. Null.

Sam Altman

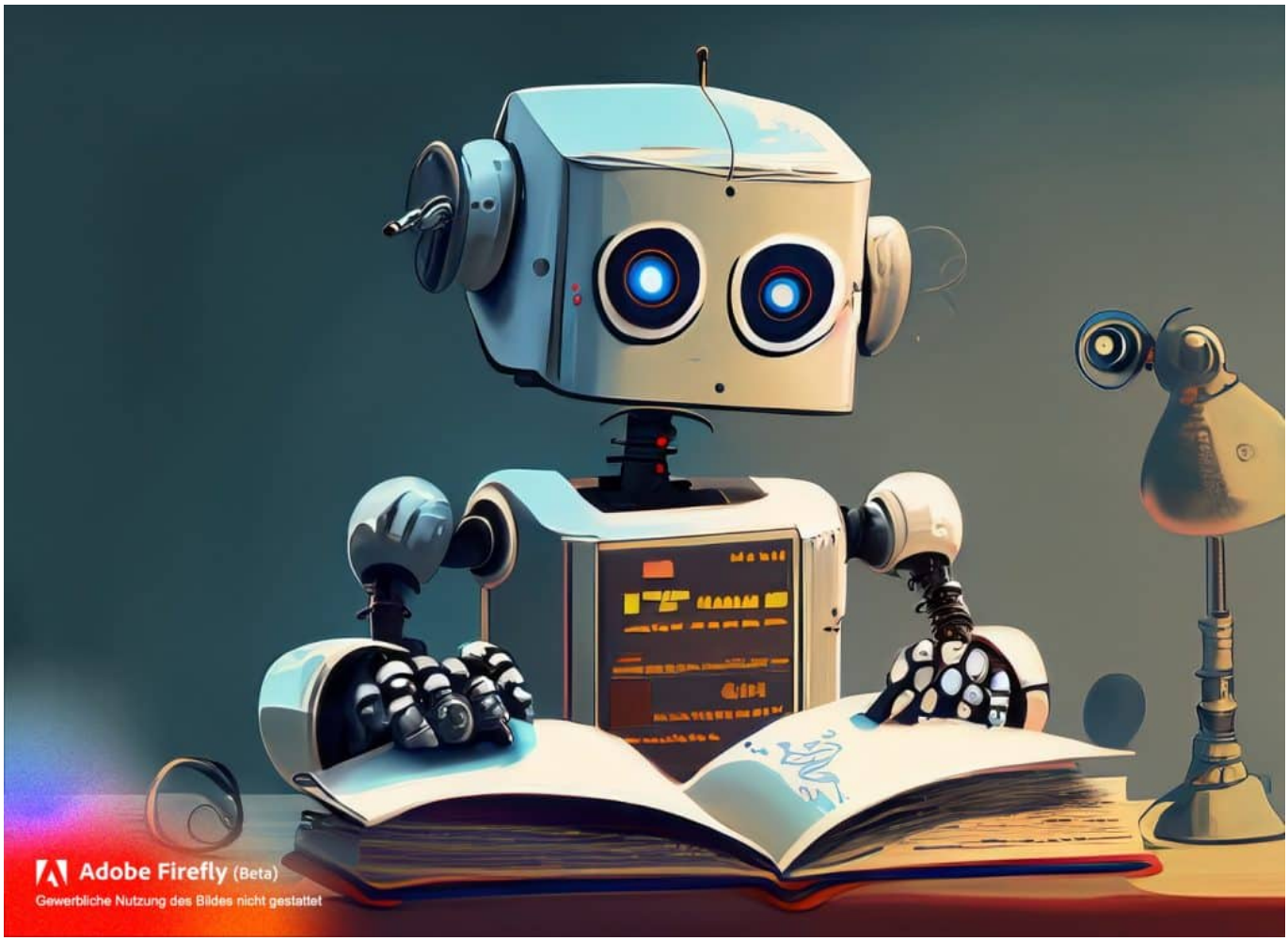
Das Ende der Wahrheit?

Die unvermeidliche Folge: Auch was echt und wahr ist, wird künftig vermehrt angezweifelt.

Und wenn selbst echte Fotos, Audios oder Videos angezweifelt werden (müssen) – wie will man sich da noch orientieren? Selbst vor Gericht wird es zum Umbruch kommen. Denn auch hier könnten Rechtsvertreter vermeintliche Beweise stets mit begründeten Zweifeln anfechten.

KI-Systeme lassen sich nicht mehr einhegen. KI ist kein Plutonium, das nur schwer zu schürfen, transportieren und einzusetzen ist.

Viele KI-Systeme kursieren schon als OpenSource. Jeder kann sie verwenden und anpassen. In der Politik kursieren Vorschläge wie eine Kennzeichnungspflicht. Doch das ist nahezu sinnlos: Da verlieren nur die, die sich dran halten. Kriminelle oder Ideologen würden eine solche Kennzeichnung nie vornehmen – oder sie mit Hilfe von KI-Systemen ruckzuck entfernen, sollte sie automatisch vorgenommen werden.



Was, wenn ein Roboter wie der Chatbot ChatGPT ein Buch liest?

Kennzeichnung von echten Inhalten

Viel sinnvoller ist daher eine Kennzeichnung für alles, was vertrauenswürdig ist oder sein soll. Ein Zertifikat für Trust – wie das gute alte Siegel, nur in digitaler Form.

So ein digitales Siegel, für Menschen unsichtbar und unhörbar, ließe sich überall dort hinterlegen, wo es wichtig ist: Dokumente, Geld, Verträge, aber eben auch Fotos, Audios und Videos. Eine unverfälschbare Quellenangabe in Form eines digitalen Wasserzeichens. Ein vertrauensvolles digitales Zertifikat, leicht von jedem zu überprüfen. Kommt das Foto wirklich von *dpa*, der Film vom *WDR*, die Tonaufnahme aus dem Kanzleramt? Mit geeigneten Tools ließe sich das kinderleicht und blitzschnell überprüfen.

Technisch wäre das nicht sonderlich aufwändig. Jede Webseite verfügt heute über ein Zertifikat, damit wir sie mit „https“ ansteuern können und die Kommunikation verschlüsselt erfolgt.

Nur muss strukturell künftig alles auf diese Form von Quellen-Check ausgerichtet werden: Anfangs dort, wo es wichtig und relevant ist: Etwa in Redaktionen oder Behörden. Später dann überall, auch im Browser, in Social Media oder Apps.

So wie sich Dateiformate wie JPG, MP3 oder MOV durchgesetzt haben, müssten sich auch die digitalen Zertifikate durchsetzen. Jede und jeder müsste jederzeit sehen, woher ein Foto, ein Audio oder Video kommt – verlässlich.

Standards nötig

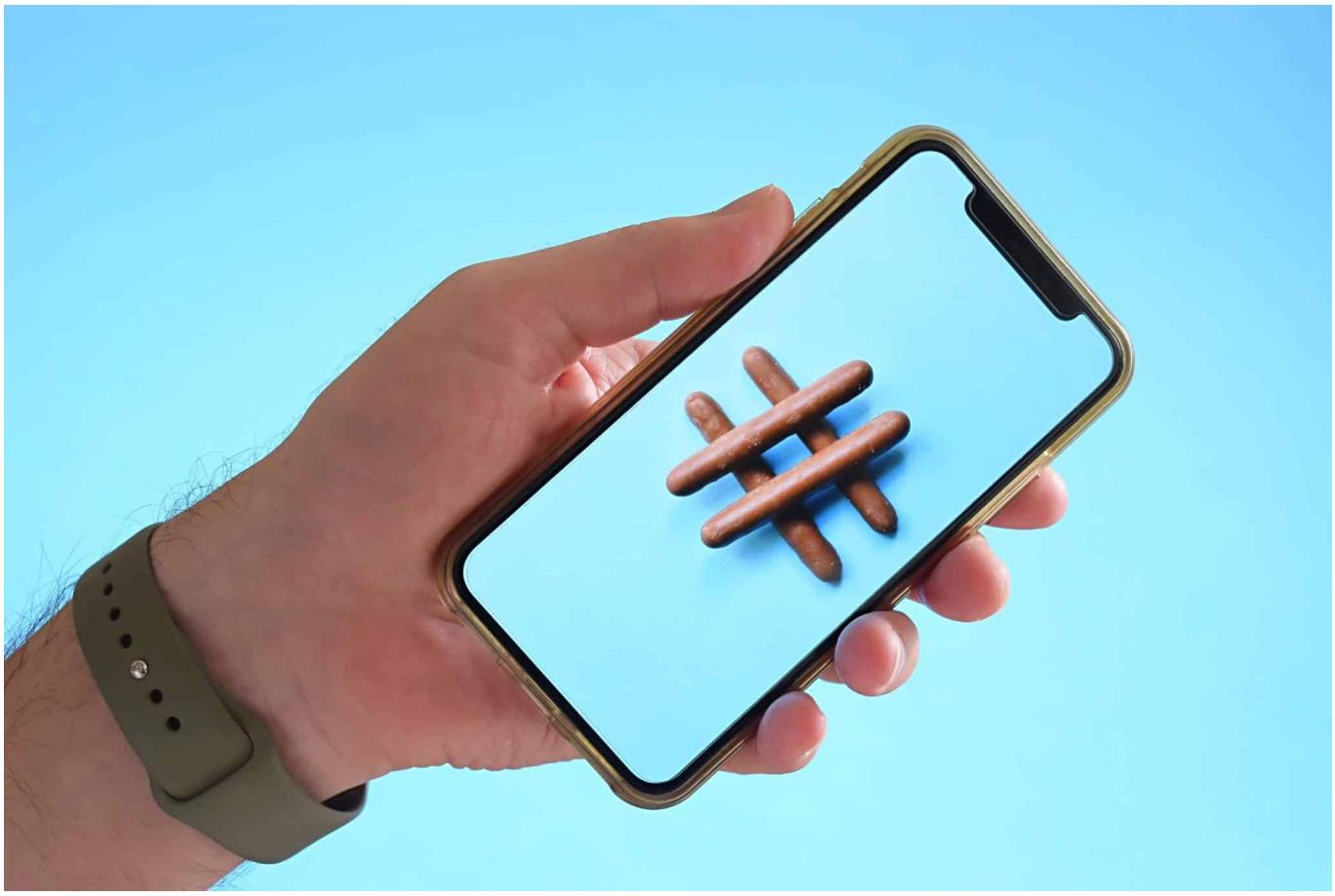
Dazu brauchen wir allgemein akzeptierte und gültige Standards, damit nicht jeder Anbieter sein eigenes Süppchen kocht. Wir müssen damit allerdings sofort beginnen, nicht erst in einigen Jahren, wenn es zu spät ist. Vielleicht ist das dann auch eine gute Gelegenheit, endlich alle verbliebenden Faxgeräte in Amtsstuben und Ministerien zu entsorgen.

Selbst einige Insider fürchten sich vor diesen und ähnlichen Szenarien.

Wenn selbst jemand wie *OpenAI*-Gründer **Sam Altman** vor zu leistungsfähiger KI warnt und Regulierung einfordert – in welcher Branche kommt so etwas schon vor? –, wird deutlich: Es braucht dringend verlässliche Rahmenbedingungen für den Einsatz von KI.

> Denn die unglaublichen Fähigkeiten und Chancen sollten wir nutzen, während Risiken minimiert werden. Das aber geht nur, wenn möglichst international einheitliche Regeln aufgestellt werden – an die sich alle halten, auch Russland und China.

Neue Studien: Filterblasen doch nicht so stark?



Die Algorithmen sozialer Netzwerke wie Facebook sind mitverantwortlich für die oft rasante Verbreitung von Falschinformationen und die gesellschaftliche Polarisierung, sagt man. Aber stimmt das auch? Einige aktuelle Studien kommen zu einem anderen Ergebnis.

Filterblase, die: So wird ein Effekt genannt, den es in den Sozialen Medien gibt. Wenn Menschen hauptsächlich oder nur Informationen erhalten, die ihren bereits bestehenden Ansichten oder Vorlieben entsprechen. Darum ist auch von „Echo-Kammern“ die Rede. Man hört und liest immer wieder mehr oder weniger dasselbe. Ein Werkzeug der Manipulation und der Spaltung, sagen viele. Doch jetzt sind einige Studien gemacht worden, die dieses Bild ein wenig aufweichen – oder zumindest differenziert betrachten. Gibt es also doch keine Filterblasen – oder worauf müssen wir uns einstellen?

Vier Studien untersuchen Filterblasen und Echokammern

Die großen Plattformen wie Facebook und Instagram seien vor allem verantwortlich für die Verbreitung von Falschinformationen, heißt es immer wieder. Ob das stimmt und zu welchem Grad, dazu wurden in den USA mehrere aufwändige Studien durchgeführt.

Es waren vier großen Studien mit sechszehn Unterstudien, also eine sehr komplexe – aber dringend nötige Analyse. Die Wissenschaftler haben vor allem untersucht, welchen Einfluss Algorithmen auf die Verbreitung von Falschinformationen und Polarisierung haben. Zwei der größten sozialen Netzwerke standen dabei im Fokus: Facebook und Instagram.

Beide Plattformen gehören dem Tech-Konzern Meta. Die Studien zeigen unter anderem, dass Facebook und Instagram zweifellos eine entscheidende Rolle dabei spielen, Nutzer zu Inhalten zu leiten (sie ihnen also zu präsentieren), denen sie wahrscheinlich zustimmen. Die Algorithmen wählen also aus, was zum

Stimmungs- und Meinungsbild passt. Die Studien **kommen jedoch zum Ergebnis**, dass die Plattformen die politischen Überzeugungen der Nutzer **nicht** signifikant beeinflussen. ~~können.~~ Das ist überraschend, da man bislang davon ausgegangen ist, dass die Plattformen die Gesellschaft so stark spalten, dass es das Stimmverhalten beeinflusst. Untersucht wurde die Zeit vor und um die letzte Präsidentschaftswahl 2020.

Facebook versorgt die Nutzer mit Infos, die sie mehrheitlich wollen

Wissenschaft und Meta gemeinsam

Eine wichtige Frage ist ja: Wer hat die Studien gemacht?

Die Studien wurden von einem Team aus rund zwei Dutzend Facebook-Forschern und externen Wissenschaftlern durchgeführt. Das ist ungewöhnlich, weil lange Zeit hat sich Meta, also der Konzern hinter Facebook, Whatsapp, Instagram und Co. nicht gerade kooperativ gezeigt, wenn es um solche Studien ging.

Das scheint sich jetzt geändert zu haben. Das hat aber mit dem Cambridge Analytica Skandal 2018 zu tun und den anschließenden Anhörungen vom Kongress und Senat in den USA. Eine der zentralen Kräfte im Team einer der wichtigsten Studien war Talia Jomini Stroud, Direktorin des Center for Media

Engagement an der University of Texas. Die Studien wurden in den wissenschaftlichen Zeitschriften „Science“ und „Nature“ veröffentlicht, also wirklich den angesehensten Blättern, die sorgfältig auswählen, was sie veröffentlichen. Von daher handelt es sich um Studien mit einer soliden Datenbasis und Aussagekraft.

Algorithmus oder Chronologie

Die Forscher haben sich auch genau angeschaut, welche Informationen bei den Menschen ankommen.

Es gibt ja unterschiedliche Methoden in Sozialen Netzwerken. Die einen setzen strikt auf chronologische Feeds, wie etwa Twitter. Da sieht man im Prinzip nur, was Leute posten oder empfehlen, denen man folgt – in chronologischer Reihenfolge. Andere Plattformen wie TikTok setzen auf Algorithmen, die auswählen, was dem jeweiligen User gefallen könnte. Instagram und Facebook setzen auf eine Kombination aus diesen Konzepten. Die Frage ist: Welchen Einfluss hat die eine, die chronologische, und die andere, algorithmische Präsentation von Inhalten.

Was wird ausgewählt, was führt eher zu einer Filterblase. Und da liefert eine der Studien ein interessantes Ergebnis: Ein chronologisch sortierter Nachrichten-Feed (im Gegensatz zum algorithmisch sortierten) erhöht(!) den Anteil von Inhalten aus als nicht vertrauenswürdig eingestuften Quellen um mehr als zwei Drittel. Das bedeutet: Wenn nicht der Algorithmus auswählt, sondern mehr oder weniger der Mensch, weil der ja entscheidet, wem er folgt, erhöht das die Wahrscheinlichkeit enorm, dass Falschinformationen erscheinen.

Die Anzahl der unhöflichen, rüden Inhalte wurde jedoch gleichzeitig um fast die Hälfte reduziert. Es ging also gesitteter zu. Allerdings hatte die chronologische Anzeige keinen nennenswerten Einfluss auf die "Polarisierung" oder das politische Wissen der Menschen.

Fördert Facebook die Trennung der Gesellschaft?

Wirkung nicht so groß wie erwartet

Aber was kann man unter dem Strich dann sagen: Welche Konsequenzen kann und muss man ziehen?

Ein Teil der Studien unterstützt die Argumentation von Facebook, Instagram und Co., dass algorithmisch ausgewählte Inhalte weniger schädlich seien als bisher angenommen. Da scheint auch was dran zu sein, weil die Algorithmen zum Beispiel eher als schädlich eingestufte Inhalte zurückhalten, während das nicht der Fall ist, wenn der User selbst auswählt. Festgestellt wurde auch, dass Facebook "ideologisch stark gespalten ist", wobei die Spaltung weniger durch die Inhalte geprägt wird, die Freunde posten, sondern erheblich mehr durch Facebook-Seiten und -Gruppen.

Die sind vor allem für schädliche Inhalte zuständig. Darum wird man sich wohl mehr kümmern müssen. Kritiker sagen, die Studien zeigten, dass das Problem komplexer ist als bisher angenommen. Es werden also weitere Untersuchungen folgen müssen. Denn eins steht fest: Proaktiv gute, gesunde, sinnvolle Inhalte fördert keine Plattform. Und mit TikTok ist ein Player am Markt, der in China sitzt, kaum zu kontrollieren ist und ausschließlich auf intransparente Algorithmen setzt.

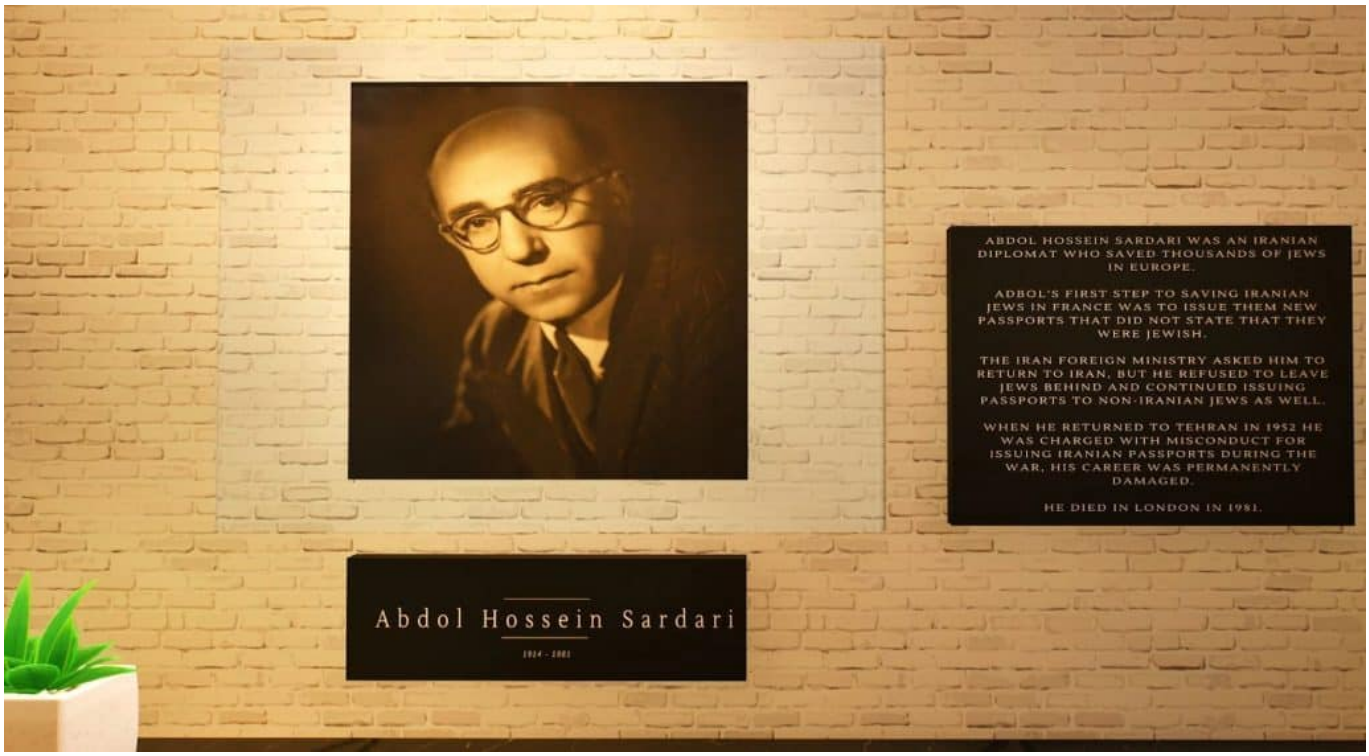
Was die gut gemachten Studien aber auch zeigen, ist~~,~~ dass wir den Unternehmen ~~aus~~ als Zulieferern von Informationen ziemlich ausgeliefert sind.

In Fortnite entsteht ein virtuelles „Holocaust Museum“

Hier hat niemand damit gerechnet: Schon bald wird es im populären Videospiel Fortnite ein virtuelles „Holocaust Museum“ geben, das an die Schrecken der Nazi-Greuel erinnert. Ein mehr als interessanter Ansatz.

Der jüdische Spiele-Entwickler Luc Bernard hat auf Twitter mit Stolz angekündigt, dass es schon in wenigen Wochen ein Holocaust Museum auf der Spieleplattform Fortnite geben wird. Das Unternehmen Epic Games, Betreiber der Plattform, hat dem Entwickler jetzt seine Unterstützung dafür zugesagt. Nötig, damit das bereits entwickelte virtuelle Museum irgendwann dann für alle öffentlich zugänglich ist.

Das virtuelle Museum ist als Ort der Besinnung konzipiert: Der Besucher kann diverse Räume besuchen, sieht Fotos und Porträts – daneben Schilderungen, die den Schrecken des Holocaust beschreiben, etwa die „Kristallnacht“. Eine andere Tafel erklärt, was Juden in Tunesien zugestoßen ist. Fortnite-Benutzer können im eigenen Tempo das Museum erkunden.



Das Holocaust Museum in Fortnite: Dutzende Schautafeln und Informationen in virtuellen Räumen

Ein Video-Game als Ort der Erinnerung

Eigentlich ist die virtuelle Welt in Fortnite, die gerne als Blaupause für das von Meta-Chef Mark Zuckerberg geplante Metaverse genannt wird, alles andere als ein Ort der Ruhe und der Besinnung. Hier treffen sich Menschen aus aller Welt, um miteinander zu spielen und live gegeneinander zu kämpfen. Das grafisch opulente Game bieten dafür unzählige Kulissen und Möglichkeiten.

Doch in Fortnite haben auch schon Live-Konzerte stattgefunden. Manche Spieler entwickeln auch Tänze. Es gibt auch Shops, in denen Player sich mit virtuellen Klamotten oder Werkzeugen ausrüsten können. Fortnite ist eine komplett virtuelle Welt, die aufgrund des offenen Konzepts unzählige Möglichkeiten eröffnet. Spieler können eigene Welten erschaffen, in denen auch eigene Regeln gelten.

Entwickler Luc Bernard nutzt moderne Technologie

Genau das hat sich Luc Bernard, der in Los Angeles lebt, jetzt zunutze gemacht und ein virtuelles Museum gebaut. Erste Eindrücke sind davon bereits im Netz zu sehen. Erst nachdem Betreiber EpicGames diese virtuelle Umgebung für die

Allgemeinheit freischaltet und in der „Map“ sichtbar macht, kann jeder hin.

Bernard hat bereits Erfahrung darin, das wichtige und sensible Thema in Form von Games zu erzählen: Im Februar ist das Videospiel „The Light in the Darkness“ erschienen (ebenfalls Epic Games, für Windows und PS5, kostenlos). Hier geht es um die Erlebnisse einer polnischen Familie in Frankreich während des Holocaust. Wer sich auf das Spiel einlässt, wird – wie in einem gut gemachten Film – emotional in die nacherzählte Geschichte gezogen. Das Spiel ist aufgrund einiger Bilder im Spiel erst ab 18 Jahren freigegeben.

Den Besucher erwarten keine interaktiven Spielereien, sondern Informationen – wie in einem Museum üblich

Sorge: KI könnte das Vergessen beschleunigen

Luc Bernard argumentiert: 80% der Amerikaner waren noch nie in ihrem Leben in einem Museum. Das virtuelle Museum in Fortnite ist eine Chance, viele Menschen mit dem Thema vertraut zu machen, die noch nie etwas darüber gehört haben. Bernard will die Menschen dort abholen, wo sie sind – und argumentiert: Warum sollte der Holocaust nur in Filmen erzählt werden dürfen, nicht aber in einem Game?

Den Entwickler aus Kalifornien treibt noch etwas an: Die Befürchtung, durch Künstliche Intelligenz könne der Holocaust verharmlost werden. Es gibt immer weniger Zeitzeugen, Überlebende, die über die Gräuel berichten können.

Bernard befürchtet, Holocaust-Leugner könnten das Netz früher oder später mit KI-Fotos oder anderen mit KI erzeugten Medien fluten, die den Leugnern in die Hände spielen oder das Leid verharmlosen. Mit seinen Projekten will er dem entgegentreten.

Das Videospiel „The light in the Darkness“ erzählt die Geschichte von polnischen Juden in Frankreich während des Holocaust