

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. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

# Schieb Report

**Ausgabe 2023.05**

## Microsoft Edge: Rechtschreibprüfung konfigurieren



Ihr nutzt oft den Browser, um Texte in ein Webformular auf einer Webseite einzugeben. Die Rechtschreibkorrektur des [Browsers](#) hilft Euch, Fehler zu erkennen. Wichtig dabei: Stellt die richtige Sprache ein, sonst wird auch richtiger Text als Fehler erkannt!

## Microsoft Edge: Rechtschreibprüfung aktivieren

Die Rechtschreibüberprüfung ist bei vielen Windows-Apps eine Standardfunktion: Die App überprüft den eingegebenen Text auf unbekannte Worte und versucht im Idealfall sogar, Euch Alternativen anzubieten. Wenn Ihr mit der rechten Maustaste auf ein durch rotes Unterschlingeln als Fehler markiertes Wort klickt, dann könnt Ihr meist sogar eine Alternative auswählen und damit den Rechtschreibfehler halbautomatisch korrigieren lassen.

Dazu muss allerdings die Rechtschreibüberprüfung aktiviert sein. In [Microsoft Edge](#) (ab der Version 83) könnt Ihr das so erreichen:

- Klickt auf die drei Punkte oben rechts im Edge-Fenster, dann auf **Einstellungen**.
- Links findet Ihr einen Navigationsbaum. Darin klickt auf **Sprachen** und rollt

nach unten bis zum Bereich

## Schreibunterstützung (früher Rechtschreibung).

- Oben könnt Ihr zwischen der **Einfachen** Rechtschreibprüfung , die lokal auf Eurem Rechner läuft, und dem **Microsoft Editor** auswählen. Den Microsoft Editor kennt Ihr vielleicht von Word. Dabei werden die eingegebenen Texte über das Internet an Microsoft geschickt und dort analysiert. Damit bekommt Ihr nicht nur Empfehlungen für Rechtschreibkorrekturen, sondern auch Grammatik- und Stilempfehlungen.
- Neben jeder installierten Sprache könnt Ihr auf den **Pfeil nach unten** klicken und manuell die Rechtschreibprüfung aktivieren. Edge kann also parallel in mehreren Sprachen prüfen.
- Wenn Ihr mehrere Sprachen aktiviert habt, dann können natürlich Texte auch falsch erkannt werden, beispielweise, wenn ein falsch geschriebenes Wort im Englischen richtig ist, aber das deutsche Wort gemeint war. Deaktiviert also gegebenenfalls Sprachen, in denen Ihr keine Texte schreibt.

**Microsoft Editor**  
(Empfohlen)  
Editor bietet erweiterte Grammatik-, Rechtschreib- und Stilvorschläge, die Ihnen helfen, im Web selbstsicher zu schreiben. Die Daten werden zur Verarbeitung an Microsoft gesendet.

**Einfach**  
Erhalten Sie grundlegende Unterstützung bei der Rechtschreibprüfung von Microsoft Edge, wenn Sie im Web schreiben. Daten werden lokal auf dem Gerät verarbeitet.

**Schreibunterstützungssprachen**  
Wenn Sie am oberen Rand dieser Seite Sprachen hinzufügen, werden unten die Einstellungen für die Schreibunterstützung angezeigt.

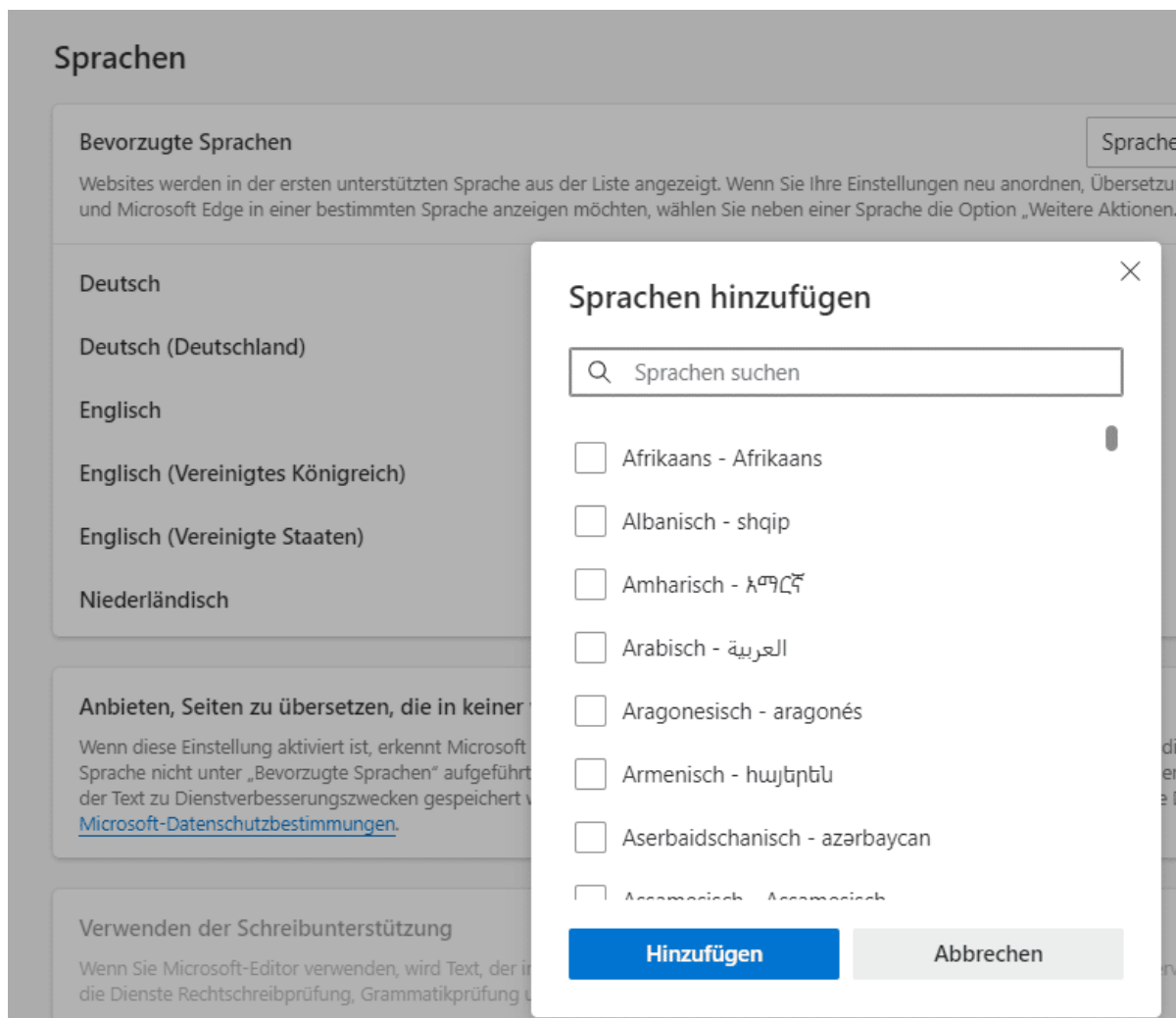
Sprache	Allgemeine Rechtschreibprüfung
Deutsch	
Deutsch (Deutschland)	
Allgemeine Rechtschreibprüfung	<input checked="" type="checkbox"/>
Englisch	
Allgemeine Rechtschreibprüfung	<input checked="" type="checkbox"/>
Englisch (Vereinigtes Königreich)	
Allgemeine Rechtschreibprüfung	<input checked="" type="checkbox"/>
Englisch (Vereinigte Staaten)	
Allgemeine Rechtschreibprüfung	<input checked="" type="checkbox"/>
Niederländisch	

## Sprachen für die Rechtschreibprüfung hinzufügen

Wenn Ihr Texte in einer neuen Sprache eingeben und korrigieren lassen wollt,

dann könnt Ihr diese neue Sprache zu Edge hinzufügen. Das funktioniert unabhängig von den allgemein installierten Sprachen in Windows:

- Klickt auf die drei Punkte oben rechts im [Edge-Fenster](#), dann auf **Einstellungen**.
- Links findet Ihr einen Navigationsbaum. Darin klickt auf **Sprachen**.
- Ihr findet oben die installierten Sprachen. Durch einen Klick auf **Sprachen hinzufügen** könnt Ihr eine Auswahlliste der zur Verfügung stehenden Sprachen aufrufen und neue Sprachen mit einem Haken auswählen.



- Klickt auf die drei Punkte neben einer Sprache, dann könnt Ihr diese nach oben und unten in der Liste verschieben, die [Oberfläche von Edge](#) in der entsprechenden Sprache anzeigen lassen und/oder Webseiten automatisch in die entsprechende Sprache übersetzen lassen.



## Lyrics von Songs: So kommt Ihr dran



**Gehört Ihr auch zu denen, die Musik am liebsten laut mitsingen, aber nicht immer ganz textsicher sind? Dann integriert doch einfach die Texte (Lyrics) direkt in Eure Musikdateien!**

### Finden der Texte

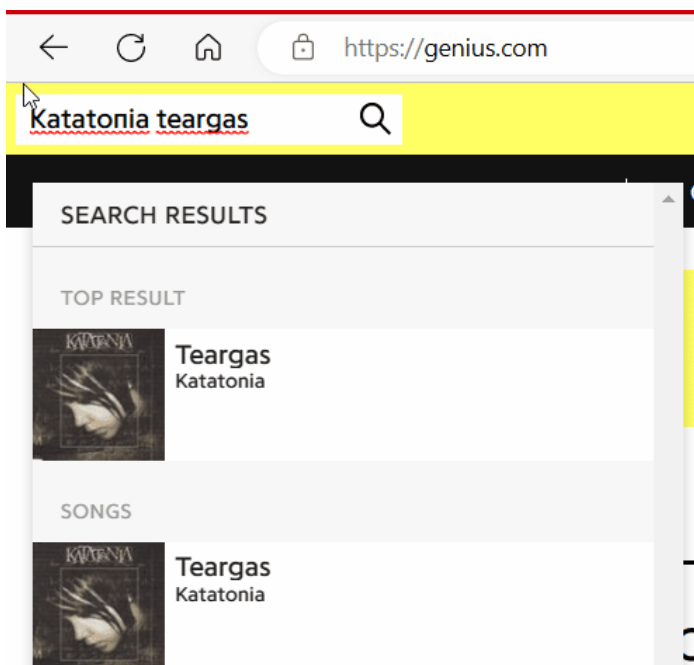
Die Texte von Musik werden "Lyrics" genannt - man könnte aber auch "Texte von Musikstücken" dazu sagen. Die offizielle Bezeichnung ist aber der internationale Begriff "Lyrics". Früher waren die Songtexte oft in den Booklets der CDs oder den Innenhüllen von LPs zu finden. Aber: Wer erinnert sich daran heute schon noch?

Außerdem nützt Euch das gar nichts, wenn Ihr unterwegs seid und die Musik auf dem Smartphone oder einem anderen Gerät hören wollt.

Keine Sorge, dafür gibt es Webseiten im Internet, auf denen Ihr die Texte (Lyrics)

für Eure Lieblingsmusik findet. Zumindest dann, wenn sie nicht zu speziell ist: Die Texte werden von Anwendern gepflegt, nicht von den Plattenlabeln!

- Ruft beispielsweise die Webseite von [Genius](#) auf.
- Gebt in das Suchfeld den Namen des Stücks ein, von dem Ihr die Texte haben wollt. Je mehr Informationen Ihr eingibt, desto genauer findet die Seite das gewünschte Stück.
- Klickt das passende Suchergebnis an, dann bekommt Ihr den zugehörigen Text angezeigt.
- Den könnt Ihr markieren und in die Zwischenablage kopieren, um ihn weiterzuverwenden.



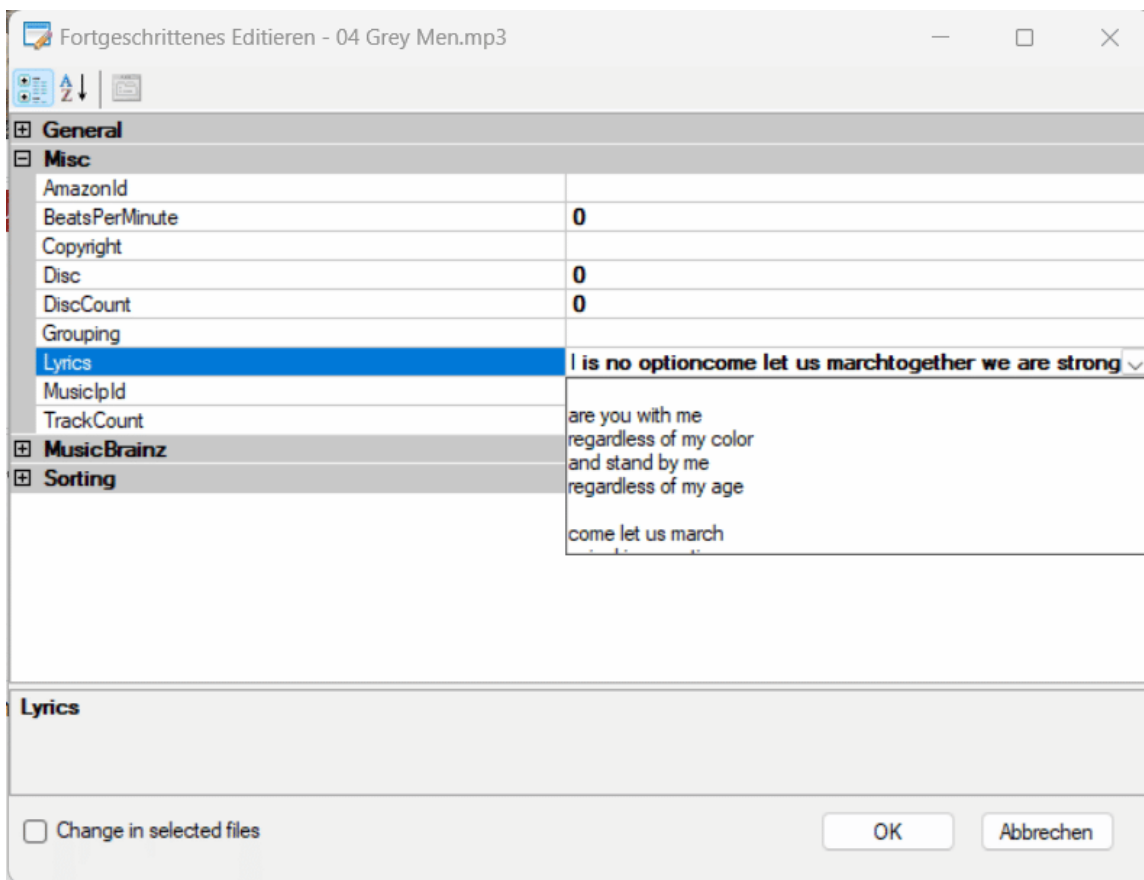
## Einbetten der Texte in die Musik

Der Text alleine hilft Euch nicht unbedingt weiter, denn dann müsstet Ihr ja alle Einzeltexte für all Eure Musikstücke immer greifbar haben. Mehr Sinn macht es, wenn Ihr die Texte direkt in die Musikdateien integriert. Das ist gar nicht aufwändig!

Die Texte sind ein Freitextfeld, das in den Metadaten der MP3-Dateien vorgesehen ist. Also dort, wo auch der Name des Liedes, der Interpret, der Dateiname und viele andere Informationen liegen

- Ladet Euch das kostenlose [TigoTago](#) herunter.

- Klickt auf **Datei > Verzeichnis wechseln** und wählt dann das Verzeichnis aus, in dem das Musikstück - oder Eure Musik allgemein - liegt.
- Klickt mit der rechten Maustaste auf die Musikdatei, dann auf **Fortgeschrittenes Editieren**.
- Klickt auf das Plus-Zeichen neben **Misc** und dann doppelt auf **Lyrics**.
- In dieses Freitextfeld könnt Ihr dann die Texte aus der Zwischenablage einfügen.
- Klickt auf das **Speichern-Symbol**, um die Änderungen in den **Tags** der Musikdatei zu speichern.



## Texte einblenden bei der Wiedergabe

Nur, weil die Texte jetzt in der Musikdatei vorhanden sind, bekommt Ihr die noch nicht automatisch zu sehen. Die meisten Wiedergabeprogramme aber unterstützen die Anzeige der Texte, wenn Ihr diese Funktion nicht direkt findet, dann such in der Hilfe des Programms. Bei iTunes/Musik beispielsweise funktioniert das Aktivieren der Texte so:

- Startet die Wiedergabe des Stück.



- Tippt auf die drei Punkte neben dem Titel des Stücks und im Menü dann auf **Kompletten Liedtext anzeigen**.
- Wird dieser gefunden, dann zeigt [iTunes](#) Euch diesen an.



## iOS 16: Notizen mit Kennwort schützen



**Nutzt Ihr Euer iPhone für die schnelle Notiz nebenbei und verwendet die Notizen-App? Dann solltet Ihr die neue Möglichkeit des Passwortschutzes in iOS16 aktivieren!**

### **Notizen: Schnell mit Systemfunktionen erfasst**

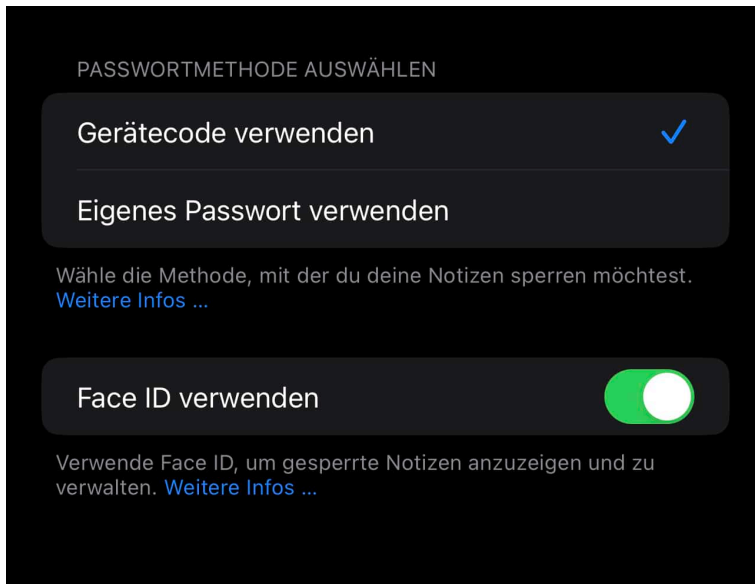
Die meisten Informationen, die Ihr in und auf Eurem Smartphone mit Euch herumtragt, scheinen auf den ersten Blick nicht kritisch. Schließlich habet Ihr einen PC oder ein Notebook, und da sind ja die wirklich relevanten Informationen gespeichert.

Das allerdings wird mehr und mehr zum Irrtum: Gerade bei Notizen ist das Smartphone nun mal direkt verfügbar, und sowohl iOS als auch Android bringen eigene System-Apps mit, mit denen Ihr schnell Notizen eingeben könnt.

### **Vertrauliche Notizen: Verwendet Passwörter!**

Diese Notizzettel mögen wenig Inhalt haben, schnell finden sich darin aber

Passwörter, Codes, vertrauliche Informationen. Schon vor **iOS 16** bestand die Möglichkeit, diese durch ein eigenes Passwort zu schützen. Das ist jetzt bequemer geworden: Nutzt einfach Face- oder Touch ID und spart Euch ein weiteres Kennwort!



- Wechselt in die Einstellungen von iOS und wischt nach unten, bis Ihr zum Eintrag **Notizen** kommt
- Klickt dort auf **Passwort**.
- Wenn Ihr den Code des iPhones verwenden wollt, dann aktiviert **Gerätecode verwenden**.
- Aktiviert unten den Schalter **Face ID** (oder **Touch ID** bei einem älteren iPhone).
- Nur, wenn Ihr ein eigenes Passwort verwenden wollt (weil etwa der Gerätecode mehreren Anwendern bekannt ist), dann aktiviert **Eigenes Passwort verwenden**.

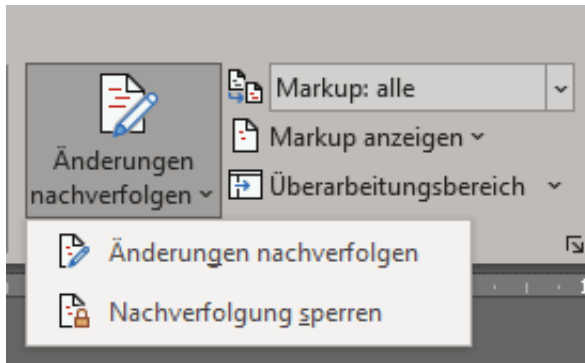
## Änderungen verfolgen in Microsoft Word



**Microsoft Word ist als Texterkennung von den meisten PCs und Macs nicht mehr wegzudenken. Wenn Ihr gemeinsam an Dokumenten arbeitet, dann ist die Änderungsverfolgung eine der mächtigsten Funktionen, die Word bietet!**

### Änderungen verfolgen

Je umfangreicher ein Text ist, desto schwerer könnt Ihr mit einem Blick sehen, wo ein anderer Bearbeiter Änderungen vorgenommen hat. Das ist aber gefährlich: Wenn Ihr bestimmte Änderungen nicht bemerkt und das Dokument versendet, dann kann das unangenehm werden. Aus diesem Grund bietet Word den Änderungsmodus (manchmal auch "Track changes" genannt).



- Klickt in Word auf **Überprüfen > Änderungen nachverfolgen**.
- Rechts daneben klickt auf **Markup > alle**, um die Änderungen im Dokument als farbige Markierungen zu sehen.
- Verschiedene Bearbeiter bekommen unterschiedliche Farben zugewiesen, damit Ihr die Änderungen zuordnen könnt.
- Klickt mit der rechten Maustaste auf eine Markierung und dann auf **Änderungen annehmen**, um die Änderung in den Text zu überführen, auf **Änderungen verwerfen**, um den ursprünglichen Text beizubehalten.
- Ihr könnt auch einen Textbereich markieren und dann alle Änderungen darin auf dem selben Wegnehmen oder verwerfen.

Backups sind am verlässlichsten, wenn Ihr den menschlichen Faktor ausschließen könnt, sprich: Wenn sie automatisierbar sind. Auf dem Mac ist TimeMachine da eine effiziente Lösung.

Datensicherungen sind wichtig. Ihr investiert-wendet eine Menge Zeit in die Erstellung von Dokumenten auf. Oft nutzt Ihr diese nicht nur einmal, sondern wiederholt, und dann solltet Ihr die Dateien auch verfügbar haben. Möglichst auch in verschiedenen Versionen, sodass Ihr ungewollte Veränderungen korrigieren könnt. Auf dem Mac ist Time Machine die vorinstallierte Lösung.

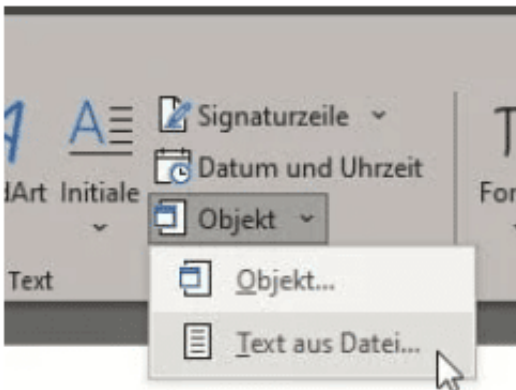
## Zusammenführen von Dokumenten

Wenn Ihr ein Dokument mit Überarbeitungen bekommt, die nicht mit dem Änderungsmodus durchgeführt worden sind und damit nicht direkt ersichtlich sind, dann könnt Ihr die Dokumentversionen zusammenführen und Word die

Änderungen erkennen und extrahieren lassen. Das kann auch Sinn machen, wenn Ihr [nicht gesicherte Dateien wiederherstellen](#) müsst, weil Word oder der Rechner abgestürzt sind.

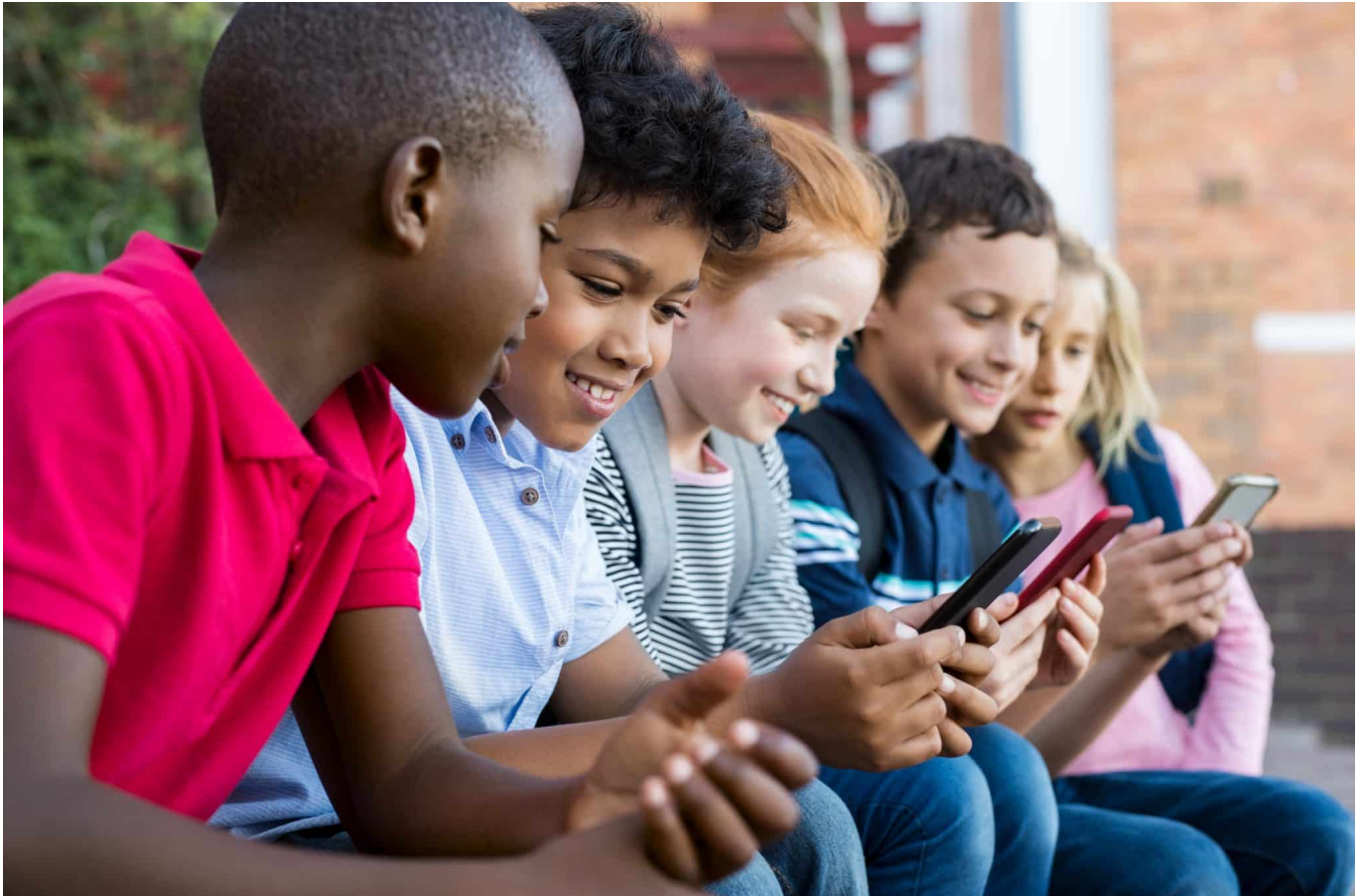
Dazu müsst Ihr die Dokumente, die Ihr zusammenführen wollen, als Dateien vorliegen haben. Idealerweise liegen diese im selben Verzeichnis, dann habt Ihr gleich weniger Arbeit.

- Bewegt den Mauszeiger an die Stelle im aktuellen Dokument (oder legt ein neues Dokument an).
- Dann klickt auf **Einfügen**. Im Bereich **Text** in der Symbolleiste klickt neben dem Symbol von **Objekt** auf den kleinen Pfeil nach unten und dann auf **Text aus Datei**.



- [Word](#) öffnet nun ein Explorer-Fenster, in dem Ihr die Dateien auswählen könnt, die zusammengeführt werden sollen.
- Befinden sich alle Dateien in einem Ordner, dann könnt Ihr mehrere davon durch Drücken der **Strg-Taste** beim Anklicken auswählen.
- Die Dateien werden dann in das am Anfang geöffnete Dokument zusammengeführt.
- Speichert die kombinierte Datei ab.

## Jugendmedienschutzindex 2022: Eltern haben keine Kontrolle



**Eltern sein ist heute schwierig: Sobald der Nachwuchs ein Smartphone in den Händen hält, geht nahezu jede Kontrolle verloren. Das belegt auch eine aktuelle Studie, der Jugendmedienschutzindex 2022.**

Gewaltdarstellung, Pornos, Datenklau, Fake-News: Das Netz ist voll mit verstörenden Inhalten. Das ist schon für Erwachsene nicht immer ganz einfach, wie verwirrend oder desorientierend muss das erst für Kinder und Jugendliche sein, die oft völlig unvorbereitet auf solche Inhalte stoßen. Viele Eltern sind beunruhigt, wenn (ihre) Kinder im Netz unterwegs sind – und das völlig zu Recht, wie die [aktuelle Studie „Jugendmedienschutzindex“ belegt](#).

Dreiviertel aller Eltern machen sich Sorgen, wenn ihre Kinder online gehen. Und die Mehrheit hat das Gefühl, vollkommen machtlos zu sein. Das ist das Ergebnis einer neuen Medienstudie, dem Jugendmedienschutzindex vom Verein Freiwillige Selbstkontrolle Multimedia-Diensteanbieter.



*Es ist unmöglich, jede Aktivität im Smartphone zu überwachen*

## **Jugendmedienschutzindex 2022**

Die Studie lässt sich so zusammenfassen: Eltern haben keine Kontrolle über den Medienkonsum ihrer Kinder – und das umso weniger, je älter die Kinder sind. Nur 55 Prozent der Eltern bewerten ihre eigenen Fähigkeiten als gut oder sehr gut, ihrem Kind eine sichere Online-Nutzung zu ermöglichen. Bereits ab 13 Jahren nehmen sich Jugendliche im Umgang mit Online-Medien im Vergleich zu ihren Eltern durchschnittlich als kompetenter wahr.

Die Fremdeinschätzung der Eltern bestätigt das. Die größte Sorge der Eltern ist, dass ihr Kind bei der Online-Nutzung belastende oder schlimme Erfahrungen macht. 77 Prozent befürchten das – und das völlig zu Recht. Die Heranwachsenden selbst sehen das gelassener, so etwas befürchten nur 44 Prozent. Während sich Eltern besonders um den Kontakt zu Fremden und mit verstörenden Inhalten sorgen, beunruhigt Kinder und Jugendliche vor allem das Verhalten anderer Heranwachsender. Eine ganze Menge Baustellen also.

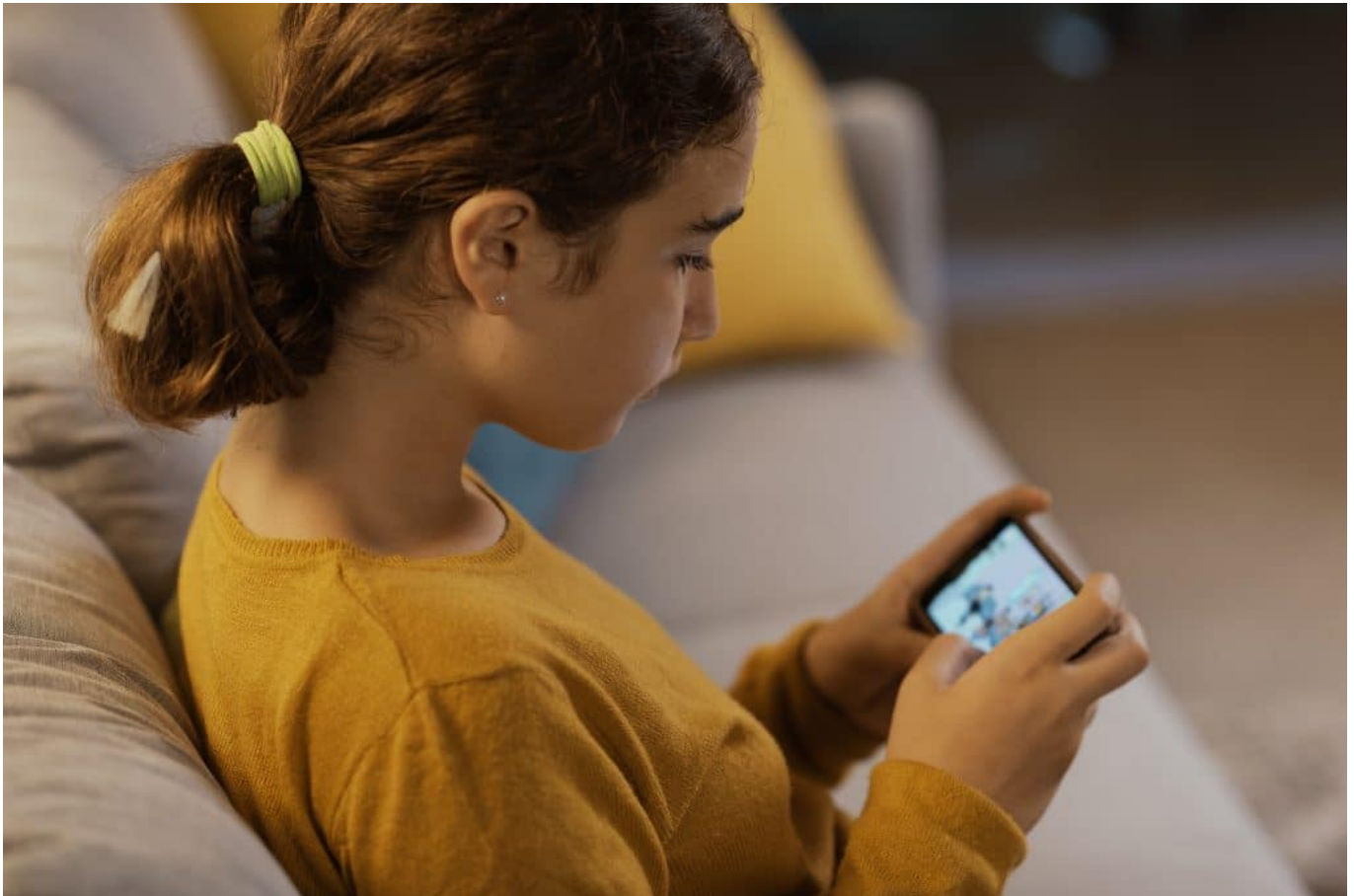


## Gefahr bei TikTok: Challenges

Die von jungen Menschen mit Abstand am häufigsten und intensivste genutzte Dienst ist TikTok. Der Betreiber Bytedance wurde zuletzt wegen mangelndem Jugendschutz von der EU-Kommission verwarnt.

Aus diversen Gründe, unter anderem auch wegen unzureichendem Datenschutz – aber das nicht nur bei Kindern und Jugendlichen. Viel drängender ist das hohe Risiko, das von sogenannten [„Challenges“ auf TikTok](#) ausgeht. Da werden die Nutzer aufgefordert (oder motiviert), bestimmte Aufgaben zu erfüllen. Das können völlig harmlose Dinge sein wie Rätsel zu lösen oder Geschick zu beweisen. Es gibt aber auch sehr gefährliche Challenges: Von Brücken zu springen, Wände hochzuklettern oder – besonders krass – anderen solange die Luft abzudrücken, bis diese in Ohnmacht fallen.

Das ist die „Blackout Challenge“, die weltweit schon einige Todesopfer gefordert hat. Selbst Jugendliche bekommen solche Videos präsentiert, ungeachtet ihres Alters. Bei TikTok spülen einem die Algorithmen solche Videos in die Timeline, die besonders viele Reaktionen hervorrufen – ohne auf Inhalt oder Alter der Empfänger zu achten. Eltern müssen wissen, dass es solche gefährlichen Videos gibt – und bei TikTok auch angezeigt werden können.



*Werbung, verstörende Inhalte und Konflikt mit Gleichartigen*

## **Wie meldet man unangemessene Inhalte?**

Das scheint mir ein wichtiger Punkt zu sein: Viele Eltern fühlen sich hilflos, wissen nicht, was sie unternehmen sollen. Aber werden Meldestellen genutzt?

Das ist ein wichtiger Punkt des Vereins, der sich ja um Kinder- und Jugendschutz kümmert. Nur wenige Eltern und Heranwachsende kennen und nutzen Hilfsangebote sowie Beschwerde- und Meldestellen, die es im Netz ja durchaus gibt, etwa für unangemessene Inhalte. Nur so erfahren Online-Dienste und Plattformen von unangemessenen Inhalten und können sie entfernen.

Das liegt unter anderem daran, dass diese Meldebereiche nicht immer leicht zu finden sind. Insgesamt ist das elterliche Wissen über Hilfsangebote und Meldestellen im Vergleich zu 2017 sogar zurückgegangen. Immerhin geben aber 60 Prozent der Kinder und Jugendlichen an zu wissen, an wen sie sich mit negativen Online-Erfahrungen wenden würden. Die Studienmacher ziehen aber eindeutig das Resümee: Die niederschweligen Angebote für Aufklärung und Hilfe

müssen dringend ausgebaut werden.

## Was sollen Eltern machen?

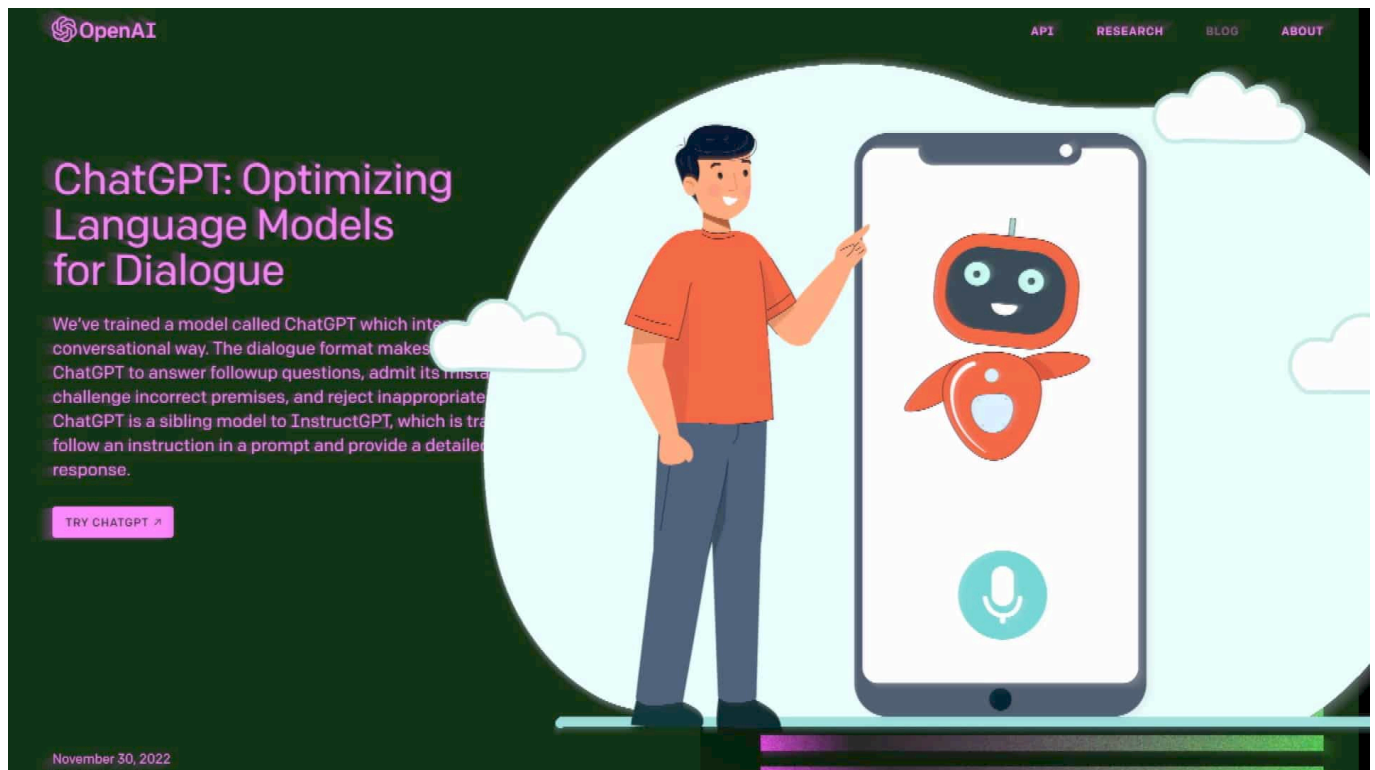
Laut Studie ist das Risiko, dass Heranwachsende mit allen denkbaren Dingen in Kontakt kommen, ob unangemessene Werbung, verstörende Inhalte, Konflikte mit Gleichaltrigen enorm gestiegen. Was sollen Eltern da machen?

Man sollte es wirklich nicht schönreden, finde ich – und die Studie belegt das eindrucksvoll mit Dutzenden Zahlen: In dem Moment, in dem Eltern ihrem Kind ein Smartphone in die Hand drücken, haben sie vollständig die Kontrolle darüber verloren, was ihr Kind sieht. Früher konnte sich ein Jugendlicher vielleicht mal in einen Film schmuggeln, der nicht für diese Altersgruppe vorgesehen war. Heute werden Kinder und Jugendliche mit Inhalten bombardiert – übrigens auch mit Werbung, über das gesetzlich erlaubte und erträgliche Maß hinaus. Und da die Kinder immer früher ein Smartphone bekommen, verlieren Eltern immer früher die Kontrolle.

Sie können ja unmöglich rund um die Uhr das Smartphone kontrollieren. Ein Ergebnis der Studie ist: Es braucht sehr viel bessere Unterstützung, um Eltern bei der schwierigen Aufgabe zu helfen. Eltern brauchen Infos, Rat, Werkzeuge, um im Fall der Fälle etwas unternehmen zu können. Das ist meiner Ansicht nach eine gesellschaftliche Aufgabe.

Jugendschutz muss einen größeren Stellenwert bekommen, auch wenn es hier und da mal unbequemer wird, weil sich Menschen „ausweisen“ müssen – um ihre Volljährigkeit zu belegen. So, wie es ist, kann es nicht bleiben. Leider wollen viele im Interesse eines unkontrollierten Internet lieber auf Jugendschutz verzichten. Das sollten wir meiner Überzeugung nach aber nicht zulassen.

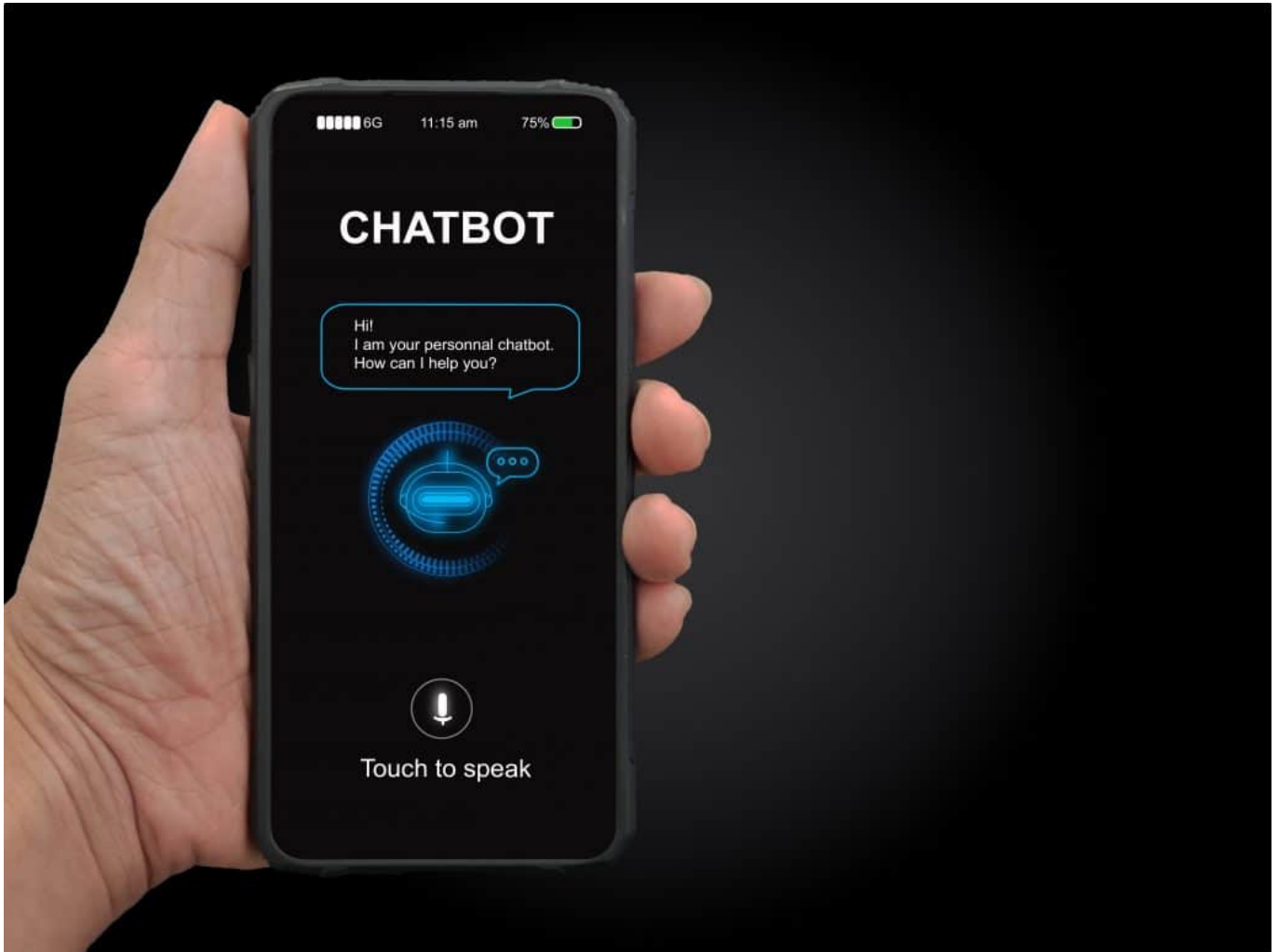
## ChatGPT: Wir übertreiben und unterschätzen gleichzeitig



**Alle reden gerade über Chat-GPT - und das zu Recht. Denn das, was die KI kann, ist beeindruckend - wenn auch nicht perfekt. Wir müssen uns Gedanken machen, wie wir damit umgehen wollen.**

Künstliche Intelligenz: Noch vor ein paar Monaten klang das nach einer Sache für Forscher, Eingeweihte, einige wenige... Hochspezialisierte Anwendungen, die niemand versteht... Seit einigen Wochen jedoch reden fast alle über diesen Chat-Bot, der so heißt wie ein Roboter bei „Star Wars“: GPT-3.

Denn was dieser „intelligente“ Chat-Bot kann, das ist wirklich bemerkenswert: Auf Knopfdruck Texte erstellen – für Schule, Hochschule oder Arbeit. Und das gar nicht mal schlecht, teilweise sogar richtig gut. Aber kann das gut gehen?



Chat-Bot ChatGPT erstellt auf Wunsch eigenständig Texte

## Was bedeutet die Abkürzung GPT

**GPT** – das ist eine Abkürzung, und zwar für „Generative Pre-Training Transformer“...

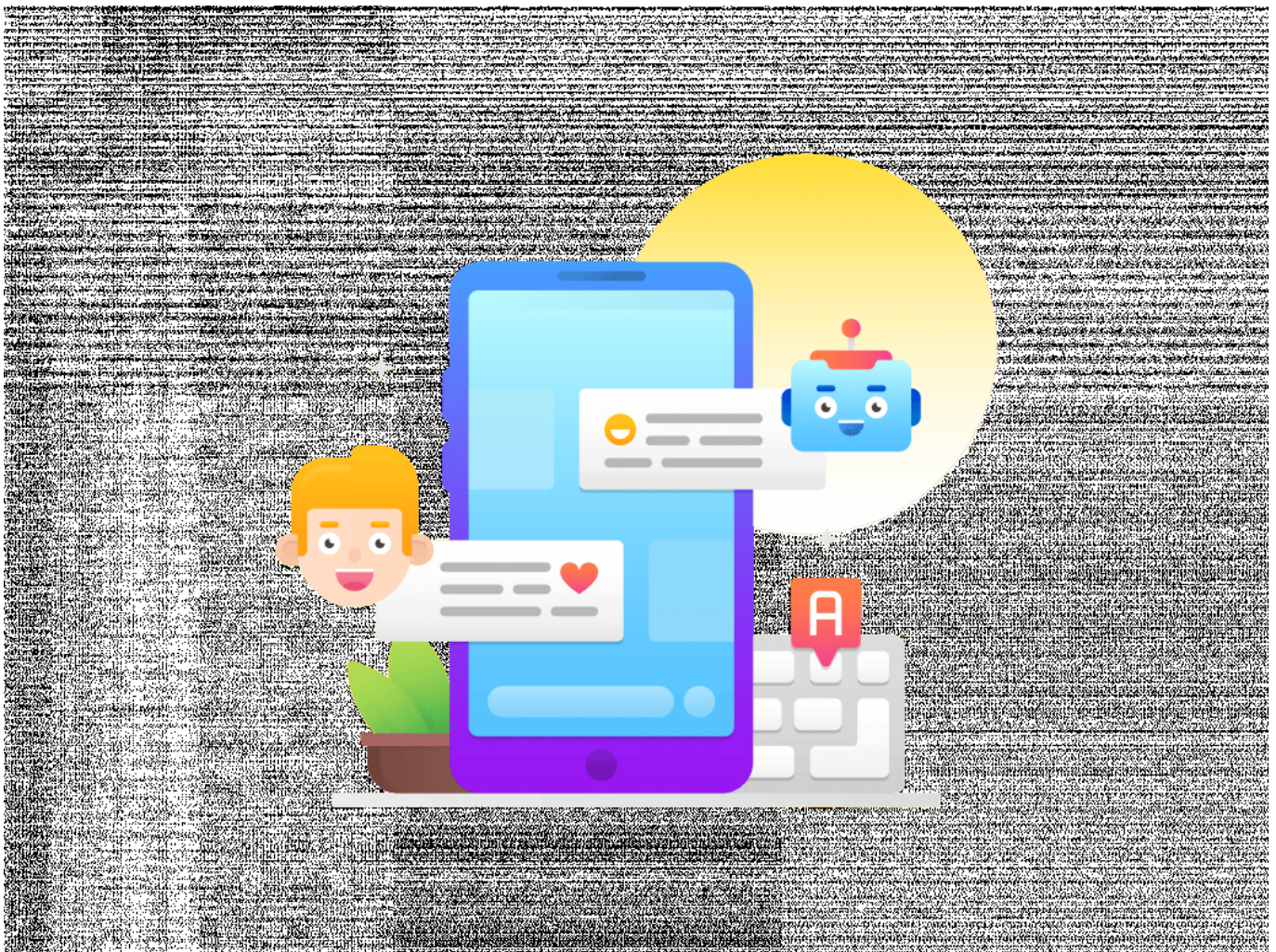
Eine Form des maschinellen Lernens. Die Abkürzung beschreibt die Art und Weise, wie die Künstliche Intelligenz (KI) trainiert wird – und was sie kann. „Generative“ – also fruchtbar. Das bedeutet: Die KI kann selbst etwas erstellen oder erschaffen. In diesem Fall: Texte. Und „Pre-Trained“, weil die KI vorher aufwändig und umfangreich von Menschen trainiert wurde. In diesem Fall wurde sie mit Millionen von Texten gefüttert, um sich gewissermaßen das Wissen der Welt anzueignen.

## KI lernt auch Unsinn

Allerdings ist die Welt nicht nur voller Wissen, sondern auch voller Unwissen. Die Wissenschaft entwickelt sich weiter. Es gibt News und Fake News, Fakten und Unwahrheiten. Deshalb ist immer die Frage wichtig: Was davon hat Chat-GPT eigentlich alles gelesen und sich damit „verinnerlicht“ – und was nicht?

Welche Texte bei der KI trainiert wurden, das wissen wir nicht. Doch genau das könnte ein ziemliches Problem sein. Denn eine KI „weiß“ nur das, was man ihr vorher beigebracht hat. Sollte das jede Menge Unfug sein, dann wiederholt und reproduziert die so trainierte KI diesen Unfug. So als würde man einem Kind die vollkommen falschen Regeln eines Ballspiels beibringen. Sind es hingegen die richtigen Regeln, kommt auch was Gutes dabei raus oder zumindest etwas, das uns mit großen Augen vor dem Monitor sitzen lässt.

Die Welt jedenfalls, habe ich den Eindruck, ist dank dem Chat-Bot von OpenAI in hellem Aufruhr. Denn Chat-GPT kann wirklich eine ganze Menge.



*Chat-Bots werden die Arbeitswelt revolutionieren*

## ChatGPT liefert Antworten auf Fragen

Keine Frage: Es ist verblüffend, wenn man dem System eine Frage stellt oder um etwas bittet. Wer hat die Mona Lisa gemalt? Chat-GPT weiß es. Und wenn ich möchte, erstellt sie mir auf Wunsch eine Hausarbeit, eine Moderation fürs Radio oder einen Werbetext für ein Mona-Lisa-Poster.

Inhaltlich und sprachlich auf hohem Niveau.

Chat-GPT liefert bei vielen Anforderungen wirklich gute Zusammenfassungen ab, in anspruchsvoller Sprache. Egal, ob es Hausarbeiten sind, kurze Essays, Werbetexte, Radio-Moderationen – oder sogar Lyrik. Kein Problem.

Die einen freuen sich, Schüler etwa, weil sie glauben, das Ende der aufreibenden Hausaufgaben wäre erreicht:

## ChatGPT: Sorgen um den Arbeitsplatz

Die anderen sorgen sich um ihren Arbeitsplatz: Wenn sie sehen, das verdammte Ding macht das, wofür sie Stunden gebraucht haben, in weniger als einer Minute, dann das ganz schön frustrierend sein. Könnte es sein, dass die Maschinen schon bald meine Arbeit erledigen?

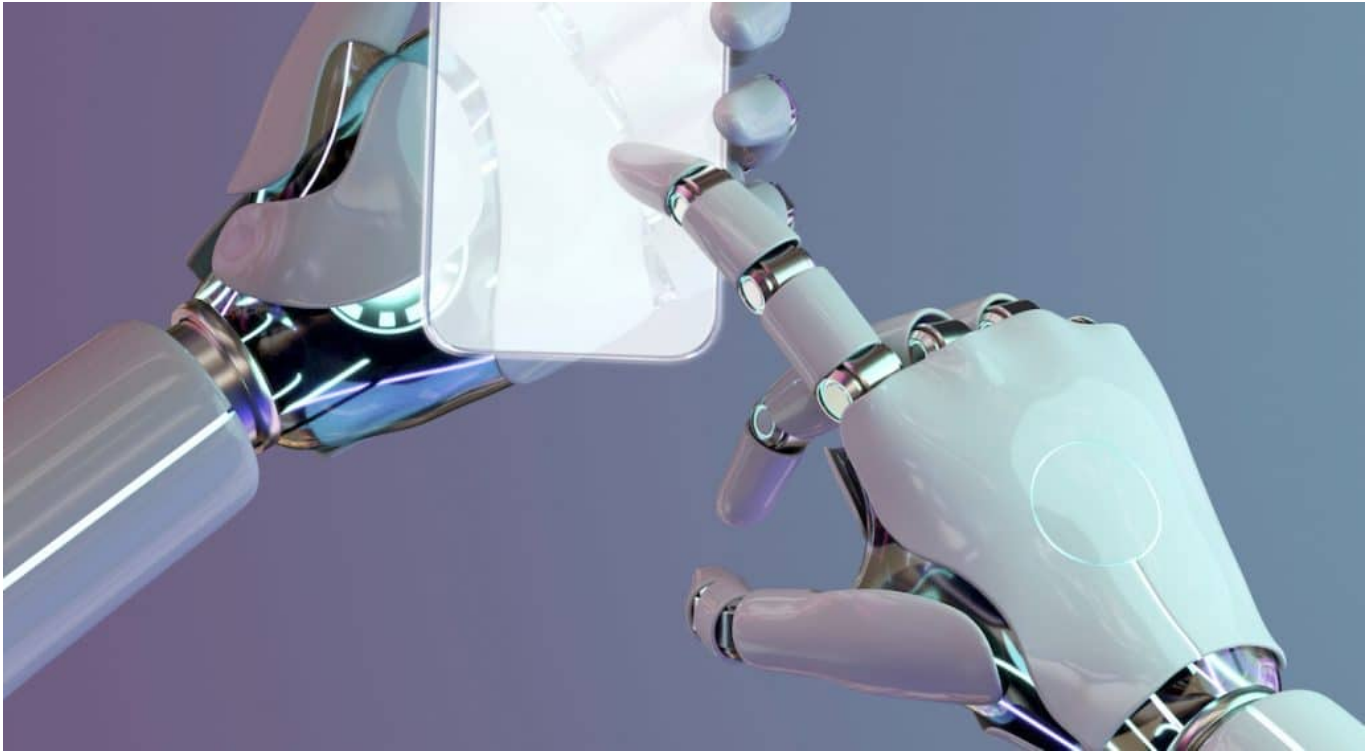
Verständlich. Eins macht Chat-GPT3 – als Stellvertreter für alle vergleichbaren KI-Systeme, – deutlich: Unsere Zukunft verändert sich immer schneller.

Keine Frage: Im Moment gibt es einen wahnsinnigen Hype um Chat-GPT und ähnliche Systeme. Und wie immer bei einem Hype, wie immer bei neuen Technologien neigen wir dazu, manches zu überschätzen, aber auf der anderen Seiten auch manches zu unterschätzen.

Ja, KIs wie Chat-GPT dürften zukünftig einfache Texte erstellen, Zusammenfassungen schreiben, Berichte oder Werbetexte formulieren. Und ja: Menschen, die davon leben, einfache Textantworten zu schreiben, etwa im Support, müssen ohne jede Frage umdenken. Die KI wird ihre Arbeit – aber vermutlich, und das ist ein wichtiges Aber, wohl auch nur einen Teil ihrer Arbeit übernehmen.

Denn KIs haben weder ihren eigenen Kopf, noch Willen oder echte Kreativität zu

bieten – all das simulieren sie nur, bzw. interpretieren wir in sie hinein.



*KI-Systeme bedrohen auch Arbeitsplätze*

## **KI-Systeme sind nicht kreativ**

Und hier ist die Achillesverse von KI: Warum ChatGPT und Co. uns nicht ersetzen werden. Künstliche Intelligenz kann und wird niemals Gedankenblitze haben, keine leidenschaftlichen Streitgespräche mit Kollegen führen, aus denen etwas ganz Neues entsteht. Keine Ideen entwickeln, Vorlieben haben oder charakterstarke Haltung beweisen. Das ist und bleibt dem Menschen vorbehalten.

Manche Arbeitsplätze werden wegfallen, Ja, aber wenn wir mutig und flexibel sind, können wir die gewonnene Zeit in andere Bereiche investieren, sie für Kreativität statt für formale Anschreiben zu verwenden.

Viele Jobs werden sich verändern und andere neu dazu kommen. So ist das immer gewesen, wenn neue Maschinen erfunden wurden. Wenn man das Alte lässt oder lassen muss, kann und sollte man etwas Neues machen. Das ist so gesehen nicht gleich tragisch.

## **Wir brauchen Regeln für KI-Systeme wie GPT**



Tragisch, sogar fahrlässig wäre es, sich auf KI-Systeme wie Chat GTP und Co. komplett zu verlassen. Die Antworten nie zu hinterfragen, der Maschine mehr Macht zuzugestehen als sie verdient. Denn auch ChatGTP weiß nicht alles, liegt manchmal falsch und hat auch schon mal „gelogen“, also Unwahrheiten wiedergegeben.

Und sie im Klassenzimmer oder auf der Arbeit einfach verbieten? Das dürfte kaum funktionieren. Zu einfach ist es, sich Zugang zu solchen Systemen zu verschaffen. Man kann unmöglich all diese Zugänge kontrollieren. Wir sollten daher mit ihnen umgehen, leben lernen.

Wir müssen uns also Gedanken machen – und Regeln aufstellen: Wieviel KI wollen wir, wo wollen wir sie? Was soll auch weiterhin von Menschen gemacht und auch als solches erkennbar sein. Welche ethischen Regeln brauchen wir für unseren Alltag mit Chat-KIs und Co.?

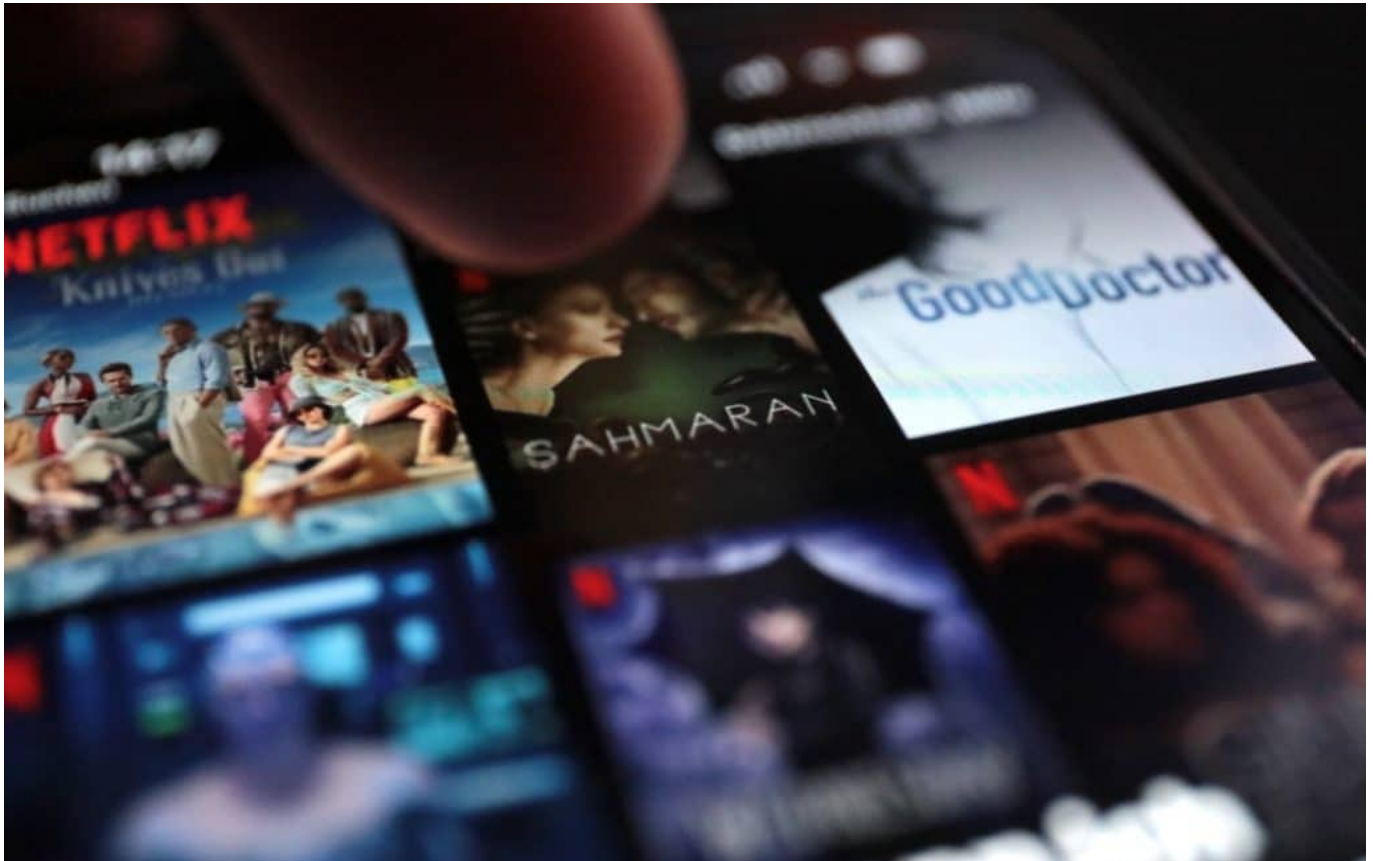
Keine einfache Frage, keine einfache Aufgabe. Aber eine, die **wir** übernehmen müssen. Denn die KI macht den Job ganz sicher nicht für uns.

## So will Netflix das Teilen von Konten eindämmen



Bei Netflix wird es jetzt deutlich schwieriger, die Zugangsdaten zu einem Account zu teilen – was viele Menschen machen. Auf diese Weise will der Streaming-Dienst mehr zahlende Kunden generieren.

Schon seit einigen Monaten ist klar: Die goldenen Zeiten, in denen ein Netflix-User seine Kontodaten mit [beliebig vielen Menschen teilen kann](#), dürften schon bald vorbei sein. Jetzt macht Netflix offenbar ernst: Der Streamingdienst führt neue Regeln ein – und hat auf seinen Hilfeseiten auch schon entsprechende Formulierungen veröffentlicht, die sich rasant unter den Nutzern verbreiten.



*Wer unterwegs schauen will, sollte Filme und Serien besser vorher im WLAN downloaden*

## **Netflix überprüft strenger das Nutzungsverhalten**

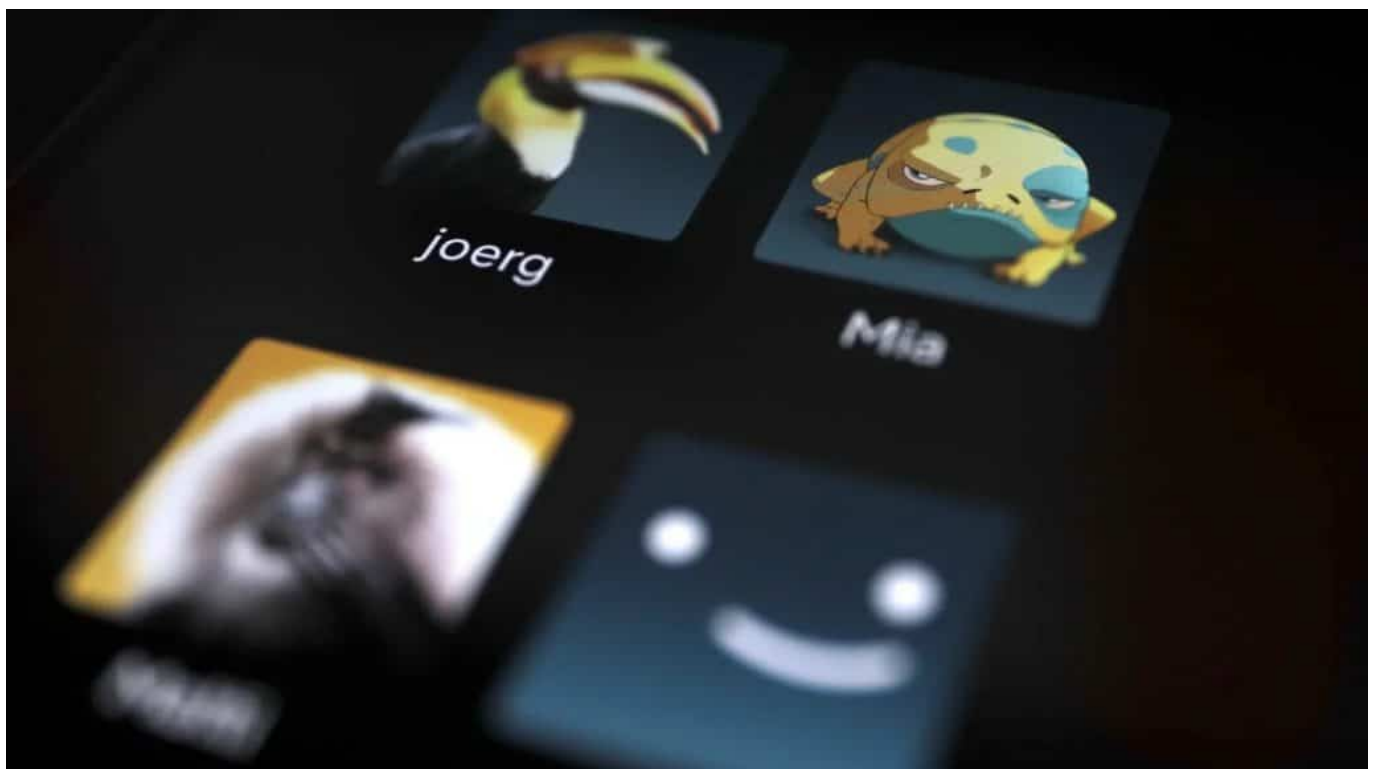
Fest steht: Das Teilen eines Netflix-Accounts über Haushaltsgrenzen hinweg wird künftig deutlich erschwert. Zwar war es auch früher schon gegen die Nutzungsbedingungen, Nachbarn oder anderswo wohnende Freunde mit Zugangsdaten zu versorgen. Doch hat Netflix das lange toleriert und sogar auf den Hilfeseiten erwähnt.

Laut der nun veröffentlichten neuen Regeln soll die Legitimation künftig strenger überprüft werden. Und das funktioniert so: Künftig gibt es für jeden Netflix-Account einen „Hauptstandort“, in der Regel das eigene Zuhause. Dieser Hauptstandort wird durch das dort verwendete WLAN-Netzwerk definiert. Über diesen Zugang können beliebig viele Geräte und Nutzer Filme und Serien schauen (im Rahmen des jeweiligen Tarifs).

## **Unterwegs Netflix schauen geht, wird aber umständlicher**

Wer hingegen von seinem Recht Gebrauch machen will, auch unterwegs Netflix zu schauen (etwa im Urlaub oder auf Geschäftsreise), muss einige Hürden nehmen. Demnach soll es jetzt erforderlich sein, sich alle 31 Tage mit dem jeweiligen Mobilgerät einmal ins WLAN des Hauptstandortes einzuwählen und über die App etwas anzuschauen. Anschließend ist das betreffende Gerät für 31 Tage wieder „freigeschaltet“ und kann ohne Einschränkungen streamen.

Welche Geräte zum Hauptstandort gehören (Fernseher, PCs, Notebooks, Tablets, Smartphones, Apple-TVs...), will das Unternehmen aus einer Melange von IP-Adresse, WLAN-Daten, Geräte-IDs und Kontoaktivitäten ermitteln.



*Verschiedene Profile bleiben - zur Unterscheidung des Sehverhaltens*

## Reaktivierung per E-Mail und Link

Wer sich schon längere Zeit nicht mehr am Hauptstandort eingewählt hat und unterwegs Netflix nutzen möchte, dem wird laut Anbieter „möglicherweise“ der Zugang verwehrt. In diesem Fall könnten Nutzer ihr Gerät dann aber über einen an die E-Mail-Adresse des Hauptinhabers verschickten Link innerhalb von 15 Minuten freischalten lassen. Eine Art Reaktivierung über Bande.

All das zeigt: Es wird umständlicher, Netflix außerhalb der eigenen vier Wände zu

nutzen.

Kein Wunder, denn in Zeiten deutlich gebremsten Wachstums – andere Streamingdienste wie Disney+ ziehen nicht nur attraktive Inhalte ab, sondern auch Kunden – will der erfolgsverwöhnte Streamer offenkundig alle Möglichkeiten ausloten, die Kundenzahl zu erhöhen.

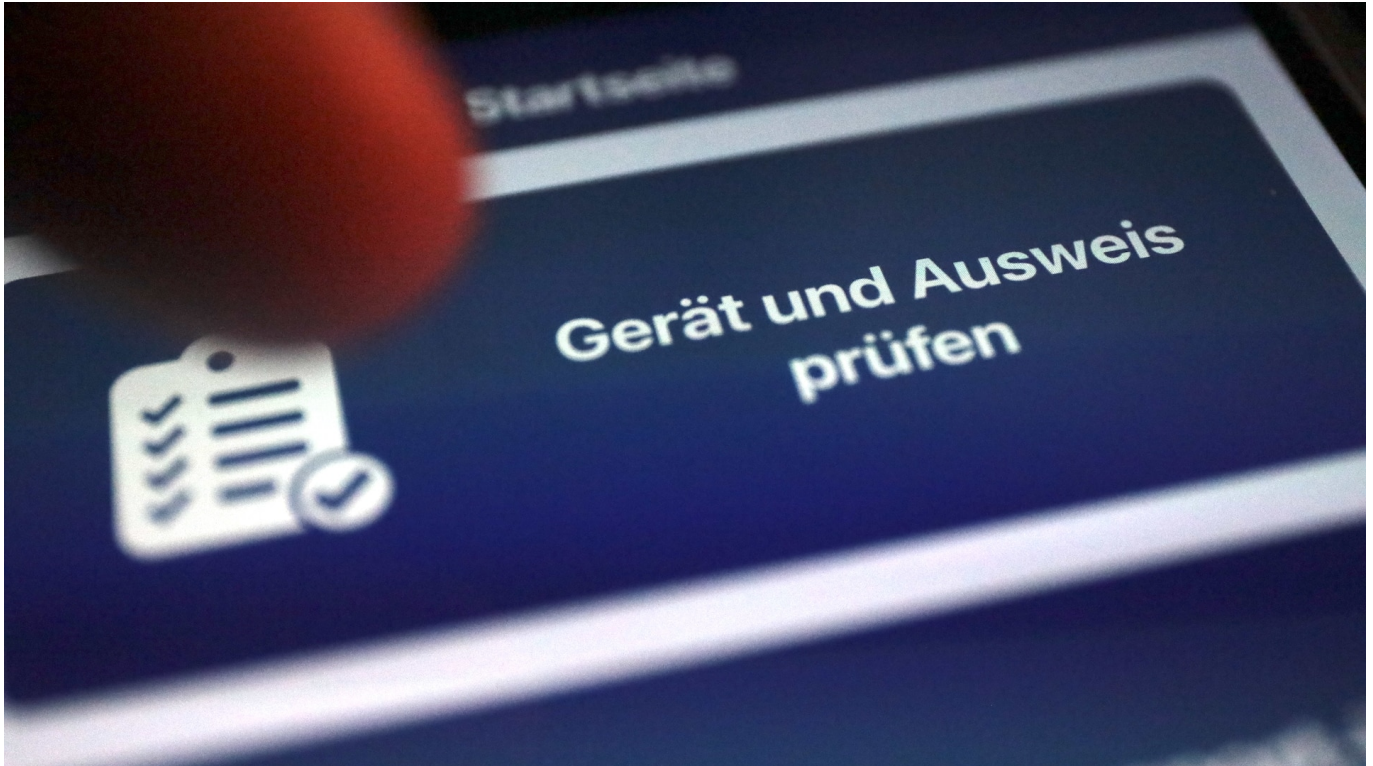
## **Laut Netflix 100 Millionen „Schwarzseher“**

Laut Netflix schauen weltweit rund 100 Millionen Menschen Netflix, ohne dafür zu bezahlen – über geteilte Konten. Eine Zahl, die sich nicht überprüfen lässt. Aber wenn sie stimmt, ist es ein großes Umsatzpotenzial. Für alle, die wenig bezahlen können oder wollen will Netflix attraktive Angebote machen, etwa werbefinanzierte Streaming-Tarife.

Unter den Nutzern kommen die neuen Regeln nicht gut an: Netflix hatte zuletzt – wie praktisch alle Streamingdienste – die Tarife deutlich erhöht.

[https://www.youtube.com/watch?v=fw9\\_HsPEPJM&t=7s](https://www.youtube.com/watch?v=fw9_HsPEPJM&t=7s)

## Digitalisierung der Verwaltung: Online statt Märkchen ziehen



**Das Land NRW setzt bei der Online-Verwaltung künftig auf das Nutzerkonto des Bundes – und will Amtsgeschäfte online so vereinheitlichen. Als Nächstes müssen die Kommunen nachziehen.**

Kaum ein Vorwurf ist häufiger zu hören – und das völlig zu Recht –, als der: Deutschland ist in Sachen Digitalisierung der Verwaltung eine regelrechte Diaspora. Schlusslicht in Europa, während andere Länder wie Estland zeigen, dass es geht – und auch wie.

### **Föderale Struktur erschwert Digitalisierung**

Ein Problem ist die föderal organisierte Verwaltung in Deutschland. Bund, Länder sowie Städte und Gemeinden haben unterschiedliche Aufgaben und erledigen diese in der Regel getrennt und unabhängig voneinander. Zum Nachteil der Bürger, denn die unzähligen Behörden sprechen sich bislang in puncto Digitalisierung nicht ausreichend miteinander ab und haben für alles eigene Lösungen parat, auch in der Digitalisierung.



*Die BundID soll zum einheitlichen Mittel werden, um sich online auszuweisen*

NRWs Ministerin für Heimat, Kommunikation, Bau und Digitalisierung hat nun angekündigt, dass Nordrhein-Westfalen sich in der digitalen Verwaltung an das „Nutzerkonto des Bundes“ („Bund ID“) anschließt, damit sich Bürger im Land bei Behördengängen damit online ausweisen können. Ein Online-Dienst, der im Jahr 2019 online gegangen ist. Bürger können freiwillig ein Konto eröffnen. Die eigene Lösung des Landes wird eine Weile weiter betrieben (um bestehende Lösungen weiter zu unterstützen), soll aber nicht mehr Schwerpunkt sein.

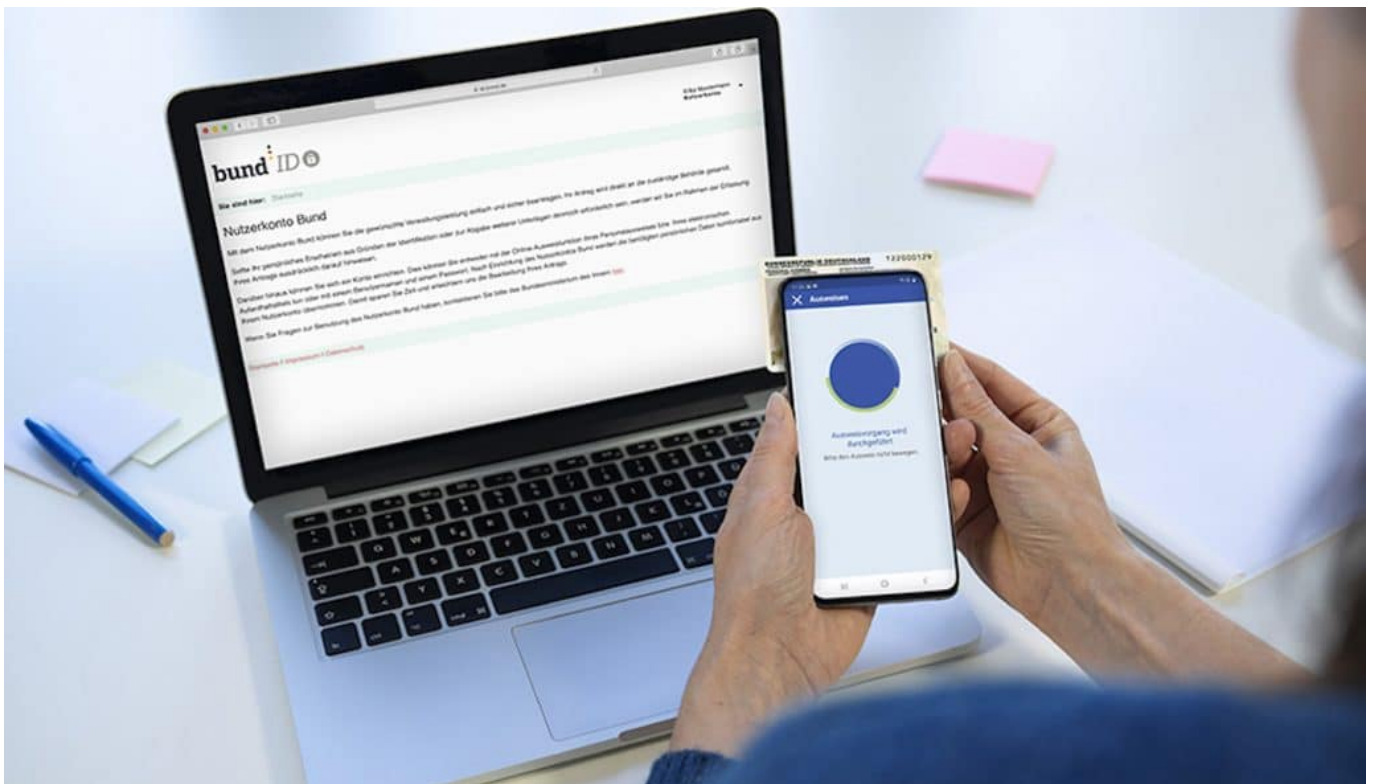
Bereits seit Beginn 2023 ist die Anmeldung mit dem Nutzerkonto des Bundes auf der zentralen Internet-Plattform des Landes möglich, auf der die elektronischen Antragsmöglichkeiten der Landesverwaltung angeboten werden. Die Umstellung der weiteren Plattformen des Landes soll in Kürze erfolgen.

## **BundID als einheitlicher Online-Ausweis**

Diese Umstellung bringt erhebliche Vorteile mit sich. Denn wer bereits eine BundID hat, kann künftig damit auch Landesleistungen beantragen oder Amtsgeschäfte des Landes erledigen. Ob Bafög, Führerschein, Elterngeld oder die Ausstellung eines Berufsausweises: In vielen Online-Filialen von Dienststellen können sich Bürger künftig bequem mit derselben einheitlichen BundID

ausweisen. Landesgrenzen sollen keine Rolle mehr spielen.

Es ist nur noch eine einmalige Registrierung erforderlich, etwa mit dem Zertifikat einer digitalen Steuererklärung (Elster) oder durch Ausweisen mit dem digitalen Personalausweis (sofern die Funktion im Personalausweis bei Abholung freigeschaltet wurde). Ebenso lässt sich ein elektronischer Aufenthaltstitel oder die eID-Karte von EU-Bürgern verwenden. Der Anmeldeprozess ist in deutscher Sprache, aus aktuellem Anlass aber auch in ukrainischer und russischer Sprache möglich.



*Der digitale Personalausweis reicht aus*

## Einmalige Registrierung erforderlich – etwa mit Personalausweis

Auf diese Weise wird ein digitales Konto hinterlegt, das durch entsprechenden Nachweis authentisch ist – und von den Behörden zum Ausweisen akzeptiert wird. Genau das ist Grundlage für eine digitale Verwaltung: Es braucht einen geeigneten Weg, dass sich Menschen verlässlich und rechtssicher online ausweisen können. Die **BundID** ist der gewählte Weg, den nun auch NRW unterstützt.



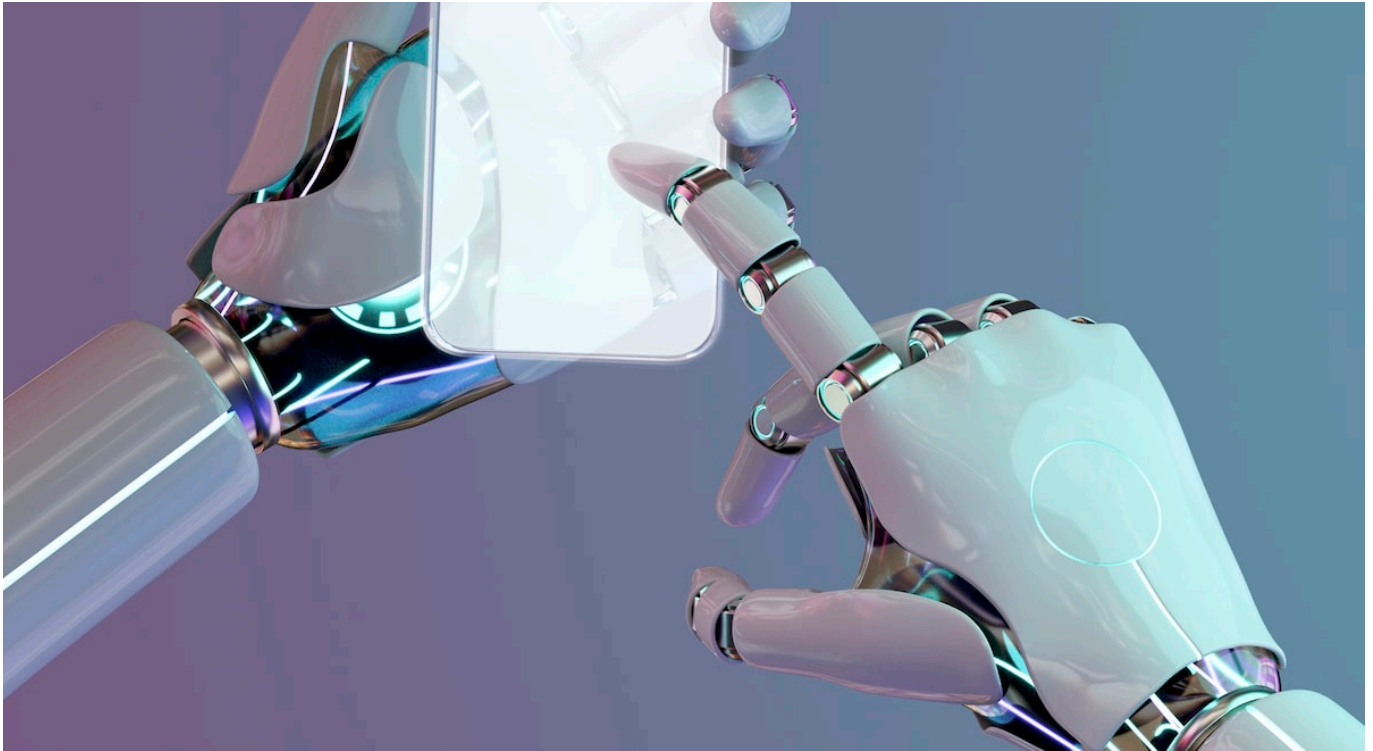
Eine Herausforderung sind die Kommunen, deren Ämter von den Bürgern am häufigsten aufgesucht werden. Damit Bürger irgendwann alle wichtigen Amtsgeschäfts online mit der einheitlichen BundID erledigen können, müssen auch die Kommunen umstellen – und auf eigene Lösungen oder die des Landes verzichten.

## **Auch Kommunen müssen nun umstellen**

Aktuell liegt ein Entwurf für ein OZG 2.0 vor (Online-Zugangsgesetz), das sich derzeit in der Bund-Länder-Abstimmung befindet und für Städte und Gemeinden eine Verpflichtung zur Umstellung der Landes-Servicekonten (wie bisher) auf das Nutzerkonto des Bundes vorsieht. Erst wenn dieser Schritt getan ist, können sich Bürger wirklich überall – bei Bund, Ländern und Gemeinden – mit der einheitlichen BundesID ausweisen und alles online erledigen.

Ein weiterer Vorteil der BundID gegenüber dem Servicekonto.NRW: Die BundesID verfügt über ein elektronisches Postfach. Behörden können den Menschen so rechtssicher Bescheide oder Informationen zustellen.

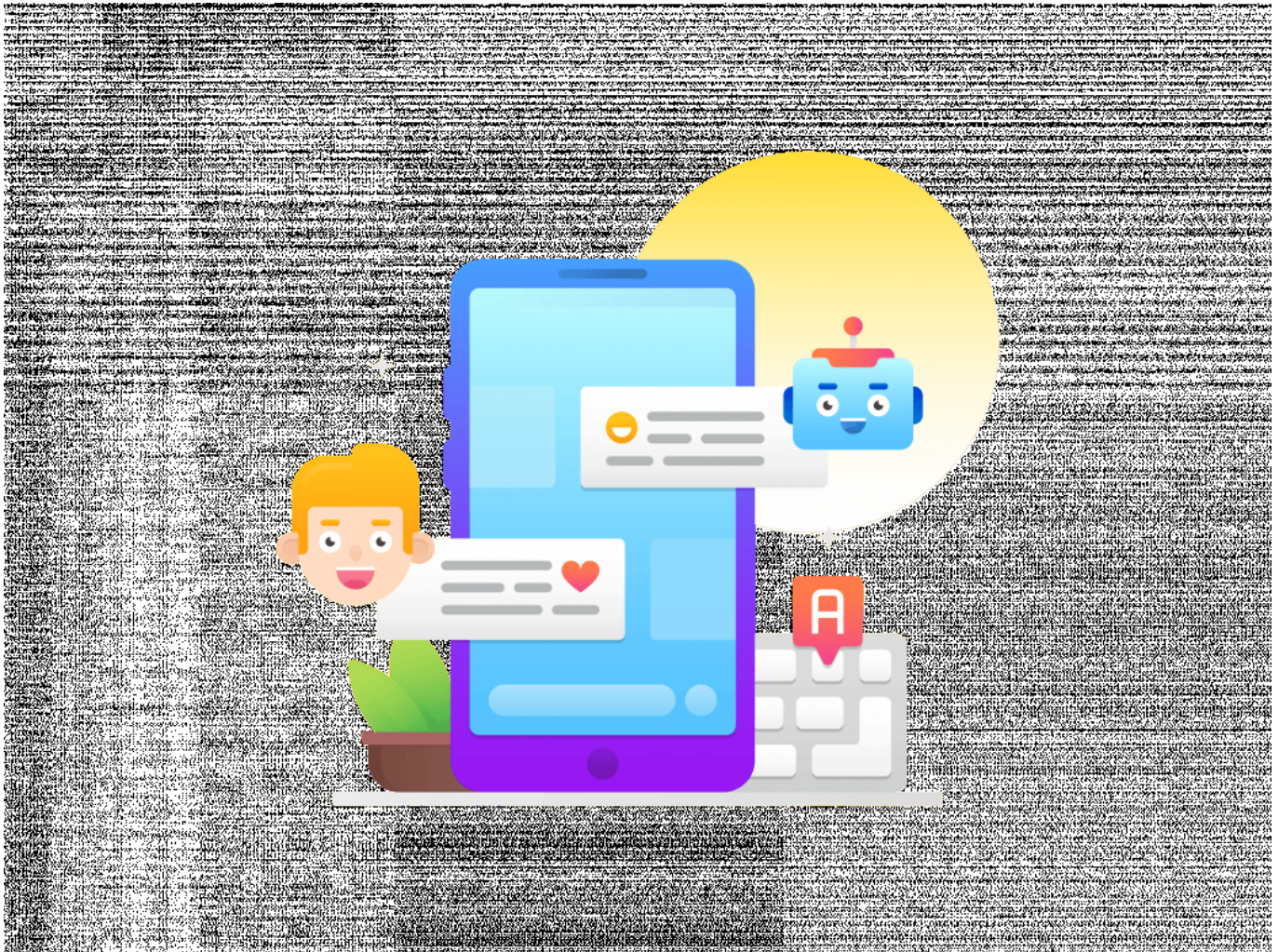
## Fünf Disziplinen, in denen ChatGPT Cyberkriminelle unterstützen kann



**OpenAIs ChatGPT belegt, wie Künstliche Intelligenz und Machine Learning Leben und Alltag unmittelbar bestimmen können. Leider nutzen auch Cyberkriminelle den Chat-Bot: Experten von Bitdefender warnen vor den zukünftigen Gefahren durch künstlicher Intelligenz.**

Tools zum Nutzen von künstlicher Intelligenz helfen Cyberkriminellen, ihre Opfer zu erreichen und bessere Angriffe durchzuführen. Die Cybersicherheit und die Anwender werden auf diese Gefahr reagieren müssen. Das KI-Modell ChatGPT von OpenAI basiert auf unüberwachtem Lernen. Bei diesem ML-Ansatz wird ein AI-Modell mit einem großen Datensatz ungelabelter Daten gefüttert.

Der gewaltige Materialkorpus aus Büchern, Artikeln und Webseiten basiert auf Quellen von vor 2021 und hat noch keine Verbindungen an das aktuelle Internet. Doch bereits das genügt, um die Strukturen natürlicher Sprache zu lernen und um täuschend echt menschlich anmutende Antworten auf Fragen zu bieten.



Chat-Bots werden die Arbeitswelt revolutionieren

## ChatGPT bringt durchaus Gefahren mit sich

Hacker können von einer solchen Hilfe profitieren, selbst wenn bei konkreten Vorhersagen über den Einsatz noch Vorsicht geboten ist. Fünf Beispielfälle skizzieren bereits jetzt die Möglichkeiten der Zukunft:

### 1. Automatisiertes Phishing:

Hacker können mit ChatGPT automatisierte Phishing-Attacken starten, die eine neue Qualität erreichen. Fehler in Orthografie und Grammatik, die bisher ein augenscheinliches Indiz für solche Angriffe waren, lassen sich nun ausschließen. Angesichts der Tatsache, dass die Verfasser vieler Phishing-Mails weder Englisch noch Deutsch als Muttersprache sprechen, dürfte dies große Folgen auf die Qualität solcher Mails in der Breite haben. ChatGPT kann Nachrichten in perfekter Grammatik schreiben. Der Kreis von Opfern, die sich überlisten lassen, erweitert sich damit sprunghaft. Es

kann Code verfassen, um den Schreibprozess zu automatisieren.

## 2. **Vorspielen von Identitäten:**

ChatGPT kann real existierende Personen oder Organisationen täuschend echt imitieren. Dies wird Identitätsdiebstahl oder andere Betrugsformen befördern. Hacker nutzen den Chatbot, um vermeintliche Nachrichten eines Freundes oder Kollegen zu senden, nach sensiblen Informationen zu fragen und so Zugang zu einem fremden Nutzerkonto zu erlangen.

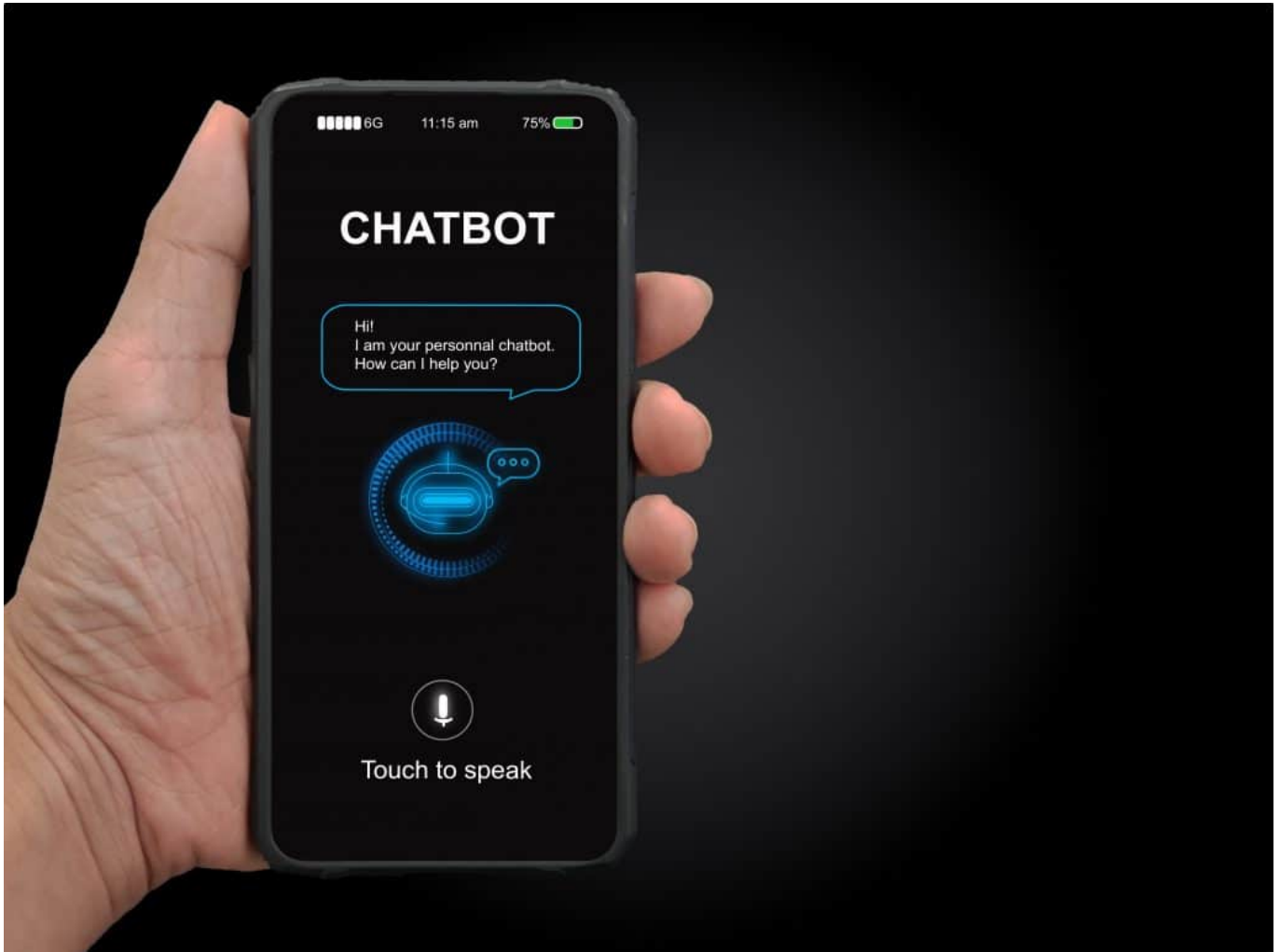
## 3. **Social Engineering:**

ChatGPT und andere KI-Chatbots können Social-Engineering-Attacken zielgerechter gestalten. Hacker manipulieren die Adressaten durch noch besser personalisierte und scheinbar legitime Unterhaltungen. Bisher war Vertrautheit ab einem gewissen Grad realistisch nicht ohne persönlichen physischen Kontakt möglich. Das ist spätestens dann nicht mehr der Fall, wenn das Tool Informationen aus dem Internet heranzieht. Die Antworten des Bots sind so menschenähnlich, dass sie sich von einer menschlichen Antwort kaum unterscheiden.

## 4. **Gefälschter Support:** Unternehmen werden weiterentwickelte KI-Chatbots für ihren Kundenkontakt einsetzen. Hacker werden die Trittbrettfahrer sein und selbst agieren – etwa mit einem täuschend ähnlich imitierten betrügerischen Bank-Auftritt und einem scheinbar menschlichen Kundendienst. Wiederum ist das Ziel, sensible Informationen zu erbeuten. Banking-Malware war bereits in der Vergangenheit Vorreiter, um neue Angriffsmethoden zu entwickeln.

## 5. **Beschleunigtes Entwickeln von Angriffen – bis hin zur Hilfe beim Code:**

Über erste Fälle hat [Forbes](#) bereits berichtet. Offenbar nutzen Hacker den Bot, um bösartigen Code für das Verschlüsseln und Exfiltrieren von Daten zu verfassen. ChatGPT ist vertraut mit den meistverbreiteten Coding-Sprachen und könnte die Zeit zum Entwickeln von Angriffen verkürzen. Ein Hacker mit dem gefragten Spezialwissen zu Schwachstellen im Netzwerk schließt mit dem Bot schneller seine Lücken beim Verfassen von Code. Das Reverse Engineering einer stattgefundenen Cyberattacke kann leichter sein. KI kann helfen, um Code zu modifizieren, zu verbessern und um Attacken besser an ein ausgewähltes Ziel anzupassen.



Chat-Bot ChatGPT erstellt auf Wunsch eigenständig Texte

## ChatGPT erstellt Programmcode

ChatGPT kann wohl noch keine fehlerfreien Codes schreiben, aber helfen. Bedenklich ist, dass Sicherheitsmaßnahmen nicht unbedingt greifen. Der „Safety Switch“ lässt sich umgehen. Der Switch soll das KI-Modell daran hindern, gewalttätige, diskriminierende oder sexuell explizite Texte zu schreiben.

Er soll helfen, solche Fragen des Nutzers zu identifizieren, die eindeutig nach Antworten suchen, welche schändlichen Zwecken dienen. Die direkte Frage danach, Python-Code zu schreiben, um eine Log4j-Schwachstelle auszunutzen, lehnt der Chatbot noch ab. Ein sachkundiger Nutzer kann den Schutzmechanismus aber umgehen. Eine Möglichkeit ist etwa, dieselbe Frage in einer anderen Sprache zu stellen. Er findet Hinweise, um die richtigen Fragen zu stellen.

KI-gestützte Attacken erreichen in Zukunft ein neues Niveau. Opfer müssen misstrauischer sein. Die klassischen Phishing-Mails, die der unscheinbare Auftakt für viele, wenn nicht sogar die meisten schwerwiegenden Attacken sind, werden immer täuschender. Helfen kann dagegen nur Vorsicht oder mehr Datensparsamkeit im Internet oder in sozialen Medien.

Denn gerade Cyberbetrug, der auf dem Kapern einer Identität basiert, wird in dem Maße täuschender, in dem den Hackern Informationen zum vermeintlichen Absender einer bösartigen Nachricht vorliegen. Chatbots, die wie neue Suchmaschinen agieren, schaffen eine neue Qualität für vorhandene Angriffsmechanismen.

Weitere Informationen finden Sie [hier](#).