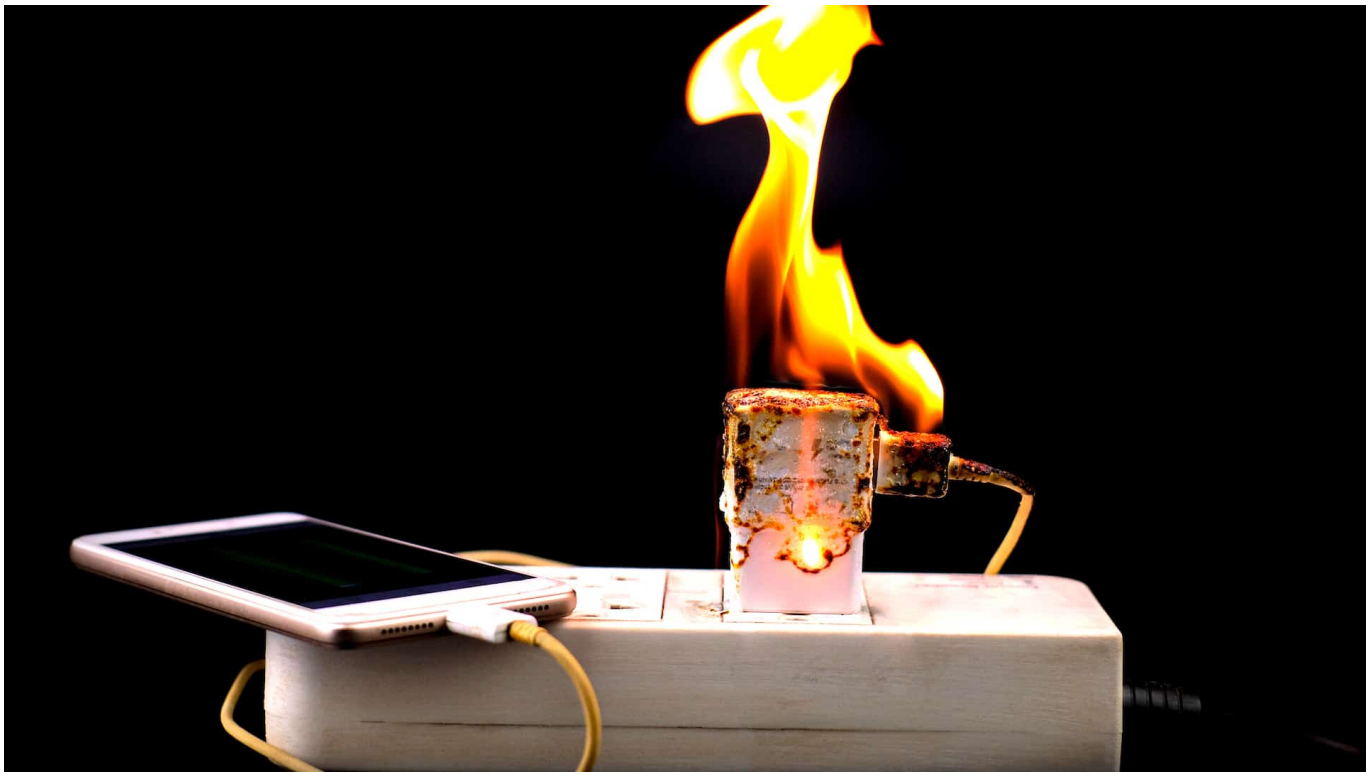
Schieb Report

Ausgabe 2023.28

Hitzefrei fürs Smartphone



Auch Smartphone leiden unter hohen Temperaturen – und schalten im Notfall sogar ab. Wer Schäden vermeiden will, schützt Handy und Akkus vor zu starker Wärme. Deaktivieren von Apps kann helfen - aber auch einige Apps können es.

Bei hohen Temperaturen wie derzeit haben nicht nur wir Menschen gelegentlich Schwierigkeiten – und freuen uns über willkommene Abkühlung. Smartphones, Notebooks, Tablets und vielen Hightech-Elektrogeräten geht es genauso. Vor allem solche, die mit einem Prozessor (CPU) ausgerüstet sind und viel rechnen müssen. Denn die erzeugen selbst auch noch Wärme.

Im Smartphone macht sich das in diesen Tagen besonders deutlich bemerkbar: Wenn die Temperaturen steigen, warnen sie oft sogar selbständig vor Überhitzung; "Das iPhone muss abkühlen, bevor es benutzt werden kann". Manche Geräte melden sich sogar mit einem "Ausgeschaltet, da zu heiß" vollständig ab – und verweigern jede weitere Zusammenarbeit.

In Windows 10 lässt sich herausfinden, welche Apps viel Strom verbrauchen

Auch Prozessoren mögen keine übermäßige Hitze

Nicht umsonst werden Rechenzentren auf eine auch für Computer „angenehme“ Betriebstemperatur heruntergekühlt. Denn wenn es zu warm oder sogar heiß wird, können die Prozessoren (CPUs) nicht mehr vernünftig arbeiten: Sie rechnen falsch, überhitzen – und können sogar dauerhaft Schaden nehmen.

Was viele aber nicht wissen: Hohe Temperaturen sind auf Dauer auch für den Akku schädlich. Zwar besteht kein Grund zur Sorge, dass ein intakter Akku bei Überhitzung direkt Schaden nimmt oder sogar explodiert. Allerdings ist Fakt: Bei Temperaturen oberhalb von 30 bis 35 Grad werden die meisten handelsüblichen Akkus stärker belastet.

Warnhinweis unter iOS, wenn das Smartphone erhitzt

Akkus können bei Hitze Schaden nehmen

Denn dann kommt es aufgrund der Temperaturen zu chemischen Reaktionen der flüssigen Elektrolyte im Lithium-Ionen-Akku. Die Folge: Manche Akkus entladen schneller, sie altern schneller und das Aufladen dauert länger. Daher ist es wichtig, für die nötige Kühlung zu sorgen – auch und vor allem während des Ladevorgangs.

Das gilt erst recht für den Fall, wenn so ein Smartphone in der Hosentasche steckt und neben der Außentemperatur auch noch der direkten Körpertemperatur ausgesetzt ist. Werden danach besonders rechenintensive Anwendungen (Apps) benutzt, etwa Games oder Video-Schnitt, die dann selbst auch noch mal Wärme im Inneren der Geräte erzeugen, kann es schon mal leicht zum problematischen Hitzestau kommen.

Viele Smartphones haben eingebauten Hitzeschutz

Moderne Smartphones lassen das aber nicht einfach geschehen, sondern überwachen die Arbeitstemperatur des fragilen Prozessors. Droht eine Überhitzung, erscheint in modernen Betriebssystemen wie iOS oder Android ein Warnhinweis – und die Arbeitsgeschwindigkeit (Takt) wird reduziert. Das Smartphone arbeitet dann langsamer, was weniger Wärme produziert und das Problem erst mal reduziert.

Manchmal werden Smartphones aber auch abgeschaltet – wenn es zu heiß wird. Denn anderenfalls kann es – was allerdings zum Glück recht selten vorkommt -, sogar zu dauerhaften Schäden am Gerät kommen. Da ist eine Notabschaltung eine vernünftige Alternative.

Wichtig: Unnötige Wärmestaus vermeiden

Deswegen sollten Smartphone-Benutzer ihr Gerät vor allem bei Hitze pfleglich behandeln – und prinzipiell gilt das für alle Hightech-Geräte mi Akku. Es gibt ein

paar Tricks, die dem Smartphone helfen, nicht in die Überlastung zu geraten.

1. **Nicht dauerhaft in der Hosentasche tragen:** Zu der ohnehin hohen Außentemperatur kommt noch die Körpertemperatur dazu – das sorgt nicht für eine mögliche Abkühlung des Geräts.

1. **Helligkeit senken**: Eine hohe Bildschirmhelligkeit kann zur Überhitzung beitragen. Die Senkung der Helligkeit kann daher dabei helfen, die Temperatur des Geräts zu reduzieren.
2. **Hintergrund-Apps schließen**: Apps, die im Hintergrund laufen, können auch die Temperatur des Handys erhöhen. Es ist daher ratsam, alle nicht benötigten Apps zu schließen.
3. **Aktualisierungen aussetzen**: Manchmal kann eine laufende Aktualisierung dazu führen, dass sich das Handy überhitzt. Falls möglich, sollte man solche Aktualisierungen aussetzen, bis das Gerät abgekühlt ist.
4. **Handy nicht direktem Sonnenlicht aussetzen**: Die direkte Sonneneinstrahlung kann die Temperatur des Handys stark erhöhen. Es ist daher ratsam, das Gerät im Schatten zu lassen, wenn es nicht benutzt wird.
5. **Hülle entfernen**: Manchmal kann die Handyhülle dazu beitragen, dass sich Wärme staut. Wenn das Handy zu heiß wird, kann es helfen, die Hülle zu entfernen.
6. **Nicht während des Ladens benutzen**: Das Handy wird oft heiß, wenn es während des Ladens verwendet wird. Daher sollte man es während des Ladevorgangs möglichst nicht benutzen.
7. **Verwenden Sie spezielle Kühl-Apps**: Es gibt verschiedene Apps, die dazu beitragen können, die Temperatur eines Handys zu senken, indem sie die CPU-Taktrate drosseln oder andere Maßnahmen ergreifen.
8. **Telefon neustarten**: Wenn nichts anderes hilft, kann ein Neustart des Telefons manchmal dazu beitragen, die Temperatur zu senken.
9. **Gerät ausschalten**: Wenn das Gerät extrem heiß ist, kann es helfen, es für eine Weile auszuschalten (etwa durch Flugmodus) und abkühlen zu lassen.

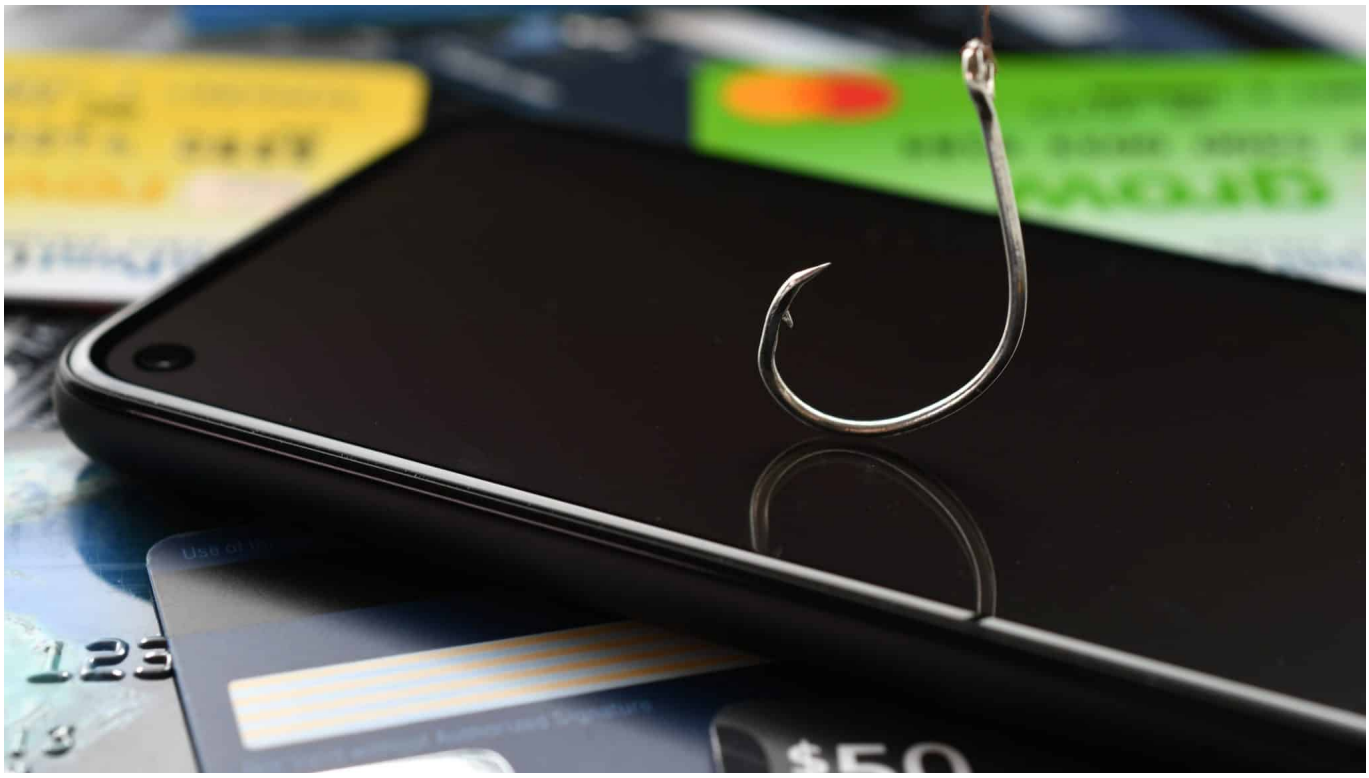
Per App die Temperatur runterkühlen

Kaum zu glauben, aber auch für das Herunterkühlen des eigenen Handys gibt es eine App. Hier sind einige Beispiele:
1. **Coolify**: Diese App analysiert dein Smartphone und identifiziert Apps, die

übermäßig viel CPU-Leistung benötigen und dadurch das Gerät überhitzen lassen. Sie drosselt automatisch die CPU-Nutzung dieser Apps, um die Temperatur zu senken.
2. **Cooler Master**: Diese App überwacht die Temperatur deines Smartphones in Echtzeit und benachrichtigt dich, wenn es zu heiß wird. Du kannst auch manuell den Kühlungsmodus aktivieren, um die Temperatur zu senken.
3. **CPU Monitor**: Diese App zeigt dir die aktuelle CPU-Auslastung deines Smartphones an. Du kannst sehen, welche Apps die meiste CPU-Leistung verbrauchen, und sie gegebenenfalls beenden, um die Temperatur zu senken.
4. **Greenify**: Diese App ermöglicht es dir, Hintergrundprozesse und Apps zu verwalten, die dein Smartphone überhitzen könnten. Du kannst bestimmte Apps in den Ruhezustand versetzen, um die CPU-Belastung zu reduzieren und die Temperatur zu senken.
5. **Battery Doctor**: Diese App bietet nicht nur Funktionen zum Verlängern der Akkulaufzeit, sondern auch zur Überwachung und Kühlung deines Smartphones. Sie kann die CPU-Temperatur überwachen und benachrichtigt dich, wenn sie zu hoch wird.

Bitte beachten, dass diese Apps zwar helfen können, die Temperatur des Smartphones zu senken, aber alle anderen Tipps zum Abkühlen weiter oben auch unbedingt beachtet werden sollten.

Vishing: Phishing-Angriffe per Sprachanruf



Cyberbetrüger entwickeln ständig neue Maschen, um Menschen zu täuschen. Neuster Trend: Vishing. Rufnummer und teilweise sogar die Stimmen der Anrufer werden gefälscht. WDR-Digitalexperte Wie man sich gegen solche Betrugsmaschen schützen kann.

Wohl fast jeder hat schon mal einen Anruf von einem vermeintlichen Mitarbeiter von Microsoft erhalten, der vorgibt, sich um ein Sicherheitsproblem kümmern zu wollen. Ziel solcher Anrufer ist es, den Opfern Malware (Schad-Software) unterzujubeln und/oder ihnen sensible Daten zu entlocken.

Damit keine Zeit bleibt, mal kritisch nachzufragen machen die Betrüger Druck: Es ist dringend – es drohen Verluste auf dem Konto oder die Sicherheit von Familienmitgliedern ist gefährdet.

Vorsicht: Bei Anrufen mit unterdrückter Nummer sollte man immer besonders aufmerksam sein

Vishing: Voice und Phishing

Doch solche als „Vishing“ – von „Voice“ (Stimme) und „Phishing“ (Abfischen) – bezeichnete Betrügereien nehmen nicht nur zu, sondern werden immer ausgefeilter.

Seitdem sich mit Hilfe von KI-Anwendungen mit vergleichsweise geringem Aufwand die Stimme nahezu jeder beliebigen Person imitieren lässt (wenige Sekunden Sound-Schnipsel reichen dazu aus), veranstalten Betrüger immer öfter Fake-Anrufe, bei denen die Opfer vermeintlich die Stimme eines Familienangehörigen in Not hören – oder einen Vorgesetzten oder Mitarbeiter einer Bank.

Darüber hinaus sind Cyber-Betrüger heute oft in der Lage, ihre wahre Rufnummer zu verschleiern: Im Display erscheint im besten Fall „unbekannter Anrufer“ oder sogar die echte Rufnummer einer Behörde, der Polizei oder einer Bank. Ein Trick, der sich „Caller ID Spoofing“ nennt und es erlaubt, dass auf dem Anrufer-ID-Display eine legitime Rufnummer erscheint, zum Beispiel die der Hausbank oder von Unternehmen wie Microsoft.

Phishing: Die Methoden werden immer ausgefeilter

Neue besonders gefährliche Vishing-Masche

Doch nun haben IT-Forscher der auf iT-Sicherheit spezialisierten Firma „Threatfabric“ eine dramatisch erweiterte, sehr komplexe Vishing-Masche aufgedeckt, die derzeit noch vor allem in Südkorea zu beobachten ist – früher oder später auch zu uns nach Deutschland kommen wird. Die IT-Sicherheitsexperten warnen sogar ausdrücklich davor, denn die Masche sei nach ihrer Analyse mühelos auch in Europa umzusetzen.

Die Angreifer tricksen ihre Opfer aus – und beantragen im Namen der Opfer einen Kredit. Dazu locken die Cyber-Betrüger die potenziellen Opfer auf eine gewohnt unauffällige Phishing-Webseite, die starke Ähnlichkeiten mit dem Google Play Store aufweise. Da, wo man sich als Android-Nutzer mit neuen Apps versorgt.

Hier werden die Opfer animiert, eine erst schädliche App zu laden. Diese App erfragt die nötigen Berechtigungen, öffnet die eigentliche Phishing-Seite und lädt weiter Malware vom Control-Server herunter. Die zweite Stufe sammelt Daten ein,

schleust sie an die Cyberkriminellen aus und bindet infizierte Geräte in das Peer-to-Peer-VoIP-Netz ein.

Letscall setzt dabei auf WebRTC-Technik, um VoIP-Verkehr umzuleiten und die Opfer mit den Call-Center-Mitarbeitern zu verbinden. Eine weitere, dritte Malware ergänzt die zweite Schadcode-Datei um Anruf-Funktionen, die die Betrüger für die Rufumleitungen nutzen

Schutzmaßnahmen gegen Vishing

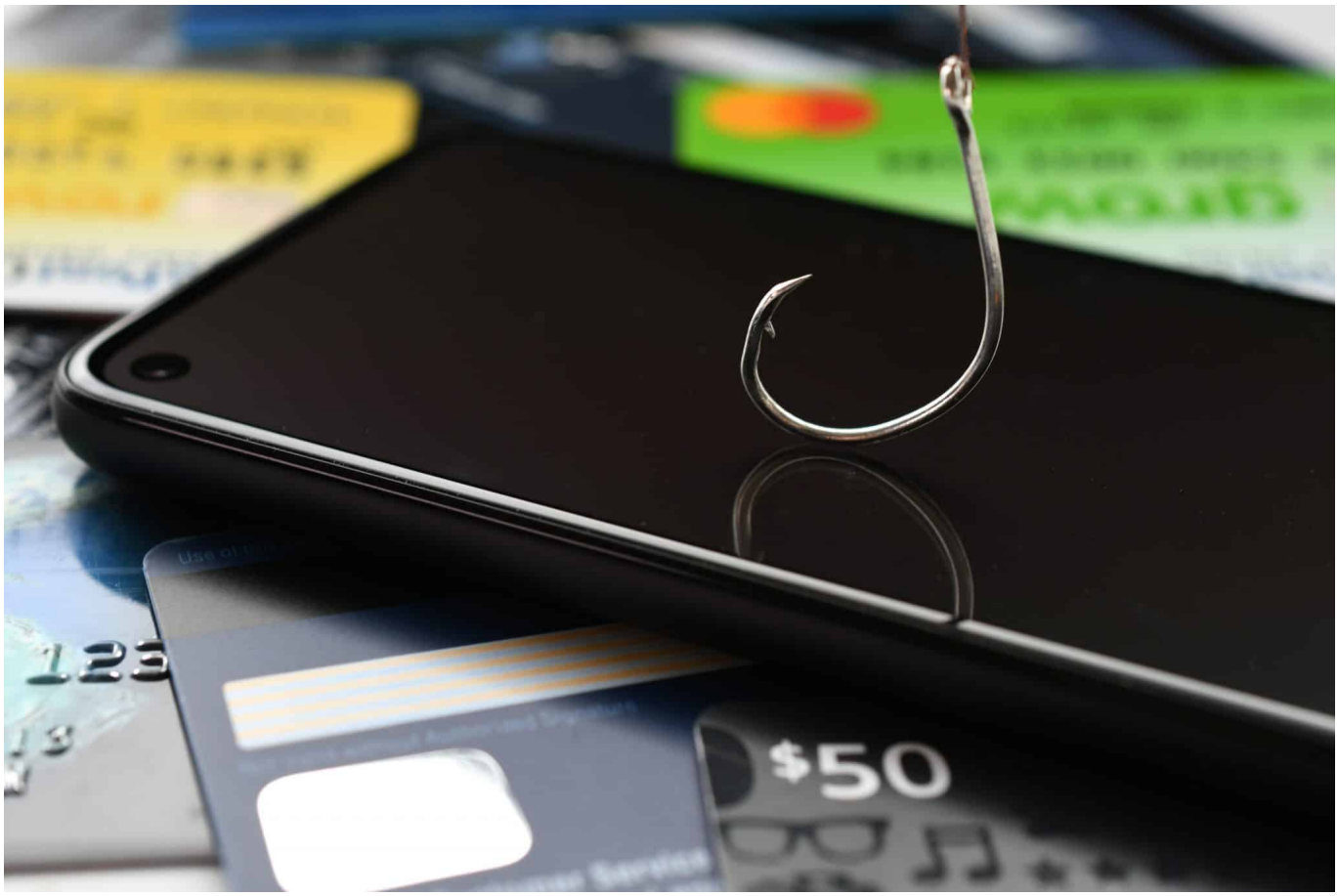
Es ist also generelle Vorsicht angeraten:

1. Vorsicht bei Anrufen von unbekannten Nummern.
2. Keine Weitergabe von persönlichen oder finanziellen Daten über das Telefon, wenn Sie den Anruf nicht initiiert haben.
3. Bestätigen Sie die Identität des Anrufers, indem Sie auflegen und die Organisation selbst anrufen, unter Verwendung einer Nummer von einer vertrauenswürdigen Quelle.

4. Installieren Sie, wenn möglich, eine Anrufschutz-App auf Ihrem Handy.

Vishing ist eine ernsthafte Bedrohung in unserer immer stärker vernetzten Welt, aber mit Wachsamkeit und gesundem Menschenverstand können Sie sich davor schützen.

Vishing: Die unsichtbare Bedrohung am Telefon - Wie Sie sich schützen können



Betrüger schlafen nie und ihr neuester Trick ist alarmierend effektiv. Sie geben sich als vertrauenswürdige Institutionen aus und manipulieren uns über Telefonanrufe, um an unsere wertvollen persönlichen Daten zu gelangen.

Willkommen in der Welt des **Vishing**. Erfahren Sie, was es ist, wie es funktioniert und vor allem, wie Sie sich davor schützen können, das nächste Opfer zu werden.

Vishing: Voice und Phishing

Vishing ist eine Kombination der Worte "Voice" und "Phishing" und bezieht sich auf eine Betrugsart, bei der Angreifer sich der Telefonkommunikation bedienen, um sensible persönliche Informationen oder Finanzdaten von ahnungslosen Opfern zu stehlen. Diese Methode unterscheidet sich von anderen Arten von Phishing, bei denen E-Mails, Textnachrichten oder gefälschte Websites

verwendet werden, indem sie stattdessen Sprachanrufe verwendet.

Lassen Sie uns dies anhand eines Beispiels verdeutlichen:

Vorsicht bei Anrufen von Unbekannten

Ein typisches Szenario für Vishing

Ein typisches Szenario könnte so aussehen, dass Sie einen Anruf von jemandem erhalten, der behauptet, von Ihrer Bank oder einem anderen vertrauenswürdigen Unternehmen zu sein. Der Anrufer warnt Sie vor einem angeblichen Problem mit Ihrem Konto, wie z. B. verdächtigen Aktivitäten oder technischen Problemen, die eine sofortige Klärung erfordern.

In der Regel erzeugen sie ein Gefühl von Dringlichkeit, das die Opfer dazu verleiten soll, ihre Bedenken zu übersehen und schnell zu handeln. Sie werden dann dazu aufgefordert, Ihre Konto- oder Kreditkarteninformationen, Ihr Passwort oder andere vertrauliche Informationen preiszugeben, angeblich um das Problem zu beheben.

Wie sich Vishing erkennen lässt

Es ist wichtig zu verstehen, dass seriöse Institutionen und Unternehmen in der Regel keine unaufgeforderten Anrufe tätigen, um nach persönlichen Daten zu fragen. Wenn Sie einen solchen Anruf erhalten, ist es am besten, das Gespräch zu beenden und die Organisation selbst anzurufen – unter Verwendung einer Nummer, die Sie auf ihrer offiziellen Website gefunden haben oder die auf der Rückseite Ihrer Bank- oder Kreditkarte aufgedruckt ist. Geben Sie niemals persönliche Informationen an jemanden weiter, der Sie unaufgefordert anruft.

Vishing ist gefährlich, weil es oft sehr überzeugend ist. Anrufer können professionell klingen und verfügen möglicherweise sogar über einige Informationen über Sie, um ihre Forderungen glaubwürdiger zu machen. Darüber hinaus sind sie oft in der Lage, ihre wahre Rufnummer zu verschleiern, sodass auf dem Anrufer-ID-Display Ihres Telefons eine legitime Rufnummer erscheinen kann.

Schutzmaßnahmen gegen Vishing

Schutzmaßnahmen gegen Vishing umfassen unter anderem:

1. Vorsicht bei Anrufen von unbekannten Nummern.

2. Nicht weitergabe von persönlichen oder finanziellen Daten über das Telefon, wenn Sie den Anruf nicht initiiert haben.
3. Bestätigen Sie die Identität des Anrufers, indem Sie auflegen und die Organisation selbst anrufen, unter Verwendung einer Nummer von einer vertrauenswürdigen Quelle.
4. Installieren Sie, wenn möglich, eine Anrufschutz-App auf Ihrem Handy.

Zusammengefasst ist Vishing eine ernsthafte Bedrohung in unserer immer stärker vernetzten Welt, aber mit Wachsamkeit und gesundem Menschenverstand können Sie sich davor schützen.

https://www.youtube.com/watch?v=mEsDEVAgUKg

Die unermüdliche Verfolgungsjagd: Elon Musks Privatjet jetzt auf Threads

Wo fliegt die Privatmaschine von Elon Musk gerade herum? Lange konnte man das auf Twitter verfolgen - bis Elon Musk das unterbunden hat. Jetzt kann man dem Privatjet auf Threads folgen.

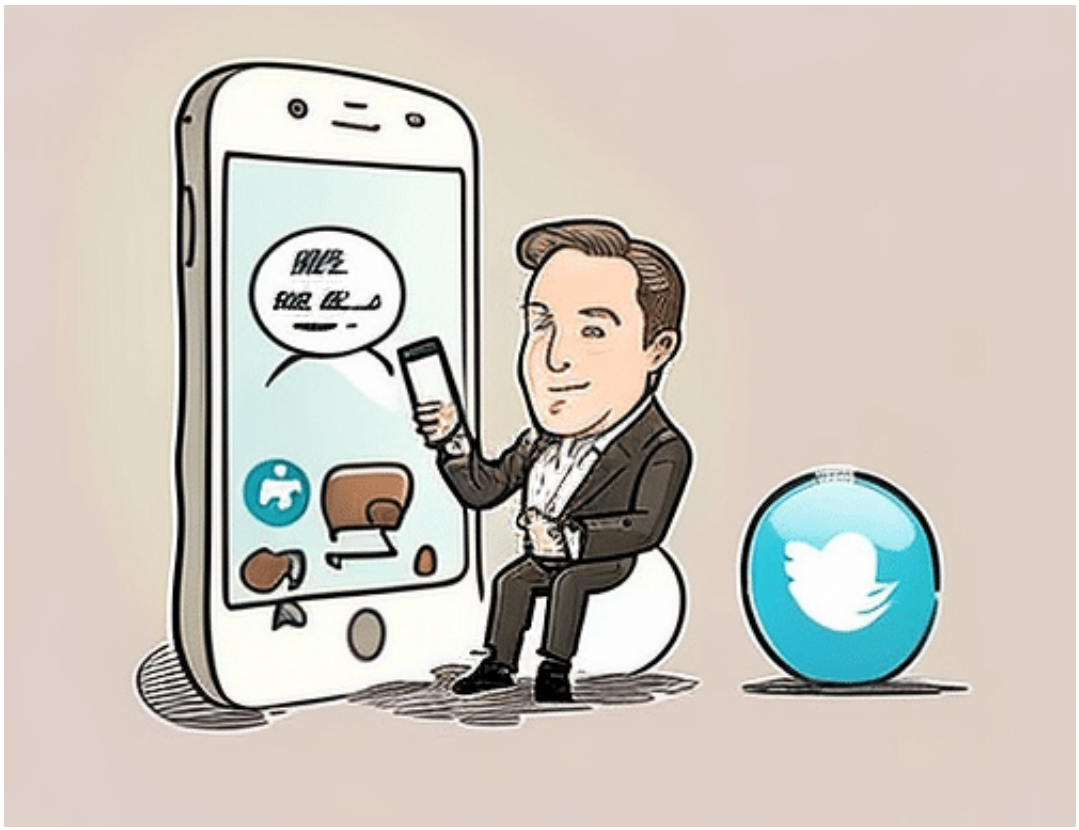
Es ist eine Geschichte, die so alt ist wie die Zeit selbst. Ein junger Held, der sich gegen einen mächtigen Titanen stellt. Nein, ich spreche nicht von David und Goliath, sondern von Jack Sweeney, dem 20-jährigen Kritiker von Tesla-CEO Elon Musk, und seiner unermüdlichen Verfolgung von Musks Privatjet.

Nach einer Sperrung auf Twitter hat Sweeney nun auf Metas Twitter-Alternative Threads eine neue Plattform gefunden, um seine Mission fortzusetzen. Und die Menge liebt es - sein Account @Elonmusksjet hat bereits über 78.500 Follower gesammelt.

Wo ist die Privatmaschine von Elon Musk?

Sweeney, ein moderner Robin Hood der Flugdaten, nutzt öffentlich verfügbare Informationen, um Starts und Landungen von Musks Jet mit der Registrierungsnummer N628TS zu verfolgen. In der Vergangenheit konnte man so etwa ablesen, welches Tesla-Werk gerade die persönliche Aufmerksamkeit des CEO bekam. Ein bisschen wie das Lesen von Teeblättern, nur dass es sich hier um die Flugrouten eines Milliardärs handelt.

Doch diese ungewöhnliche Hobby brachte Sweeney auf Twitter in Schwierigkeiten. Nach der Übernahme der Plattform durch Musk wurde Sweeneys Account dauerhaft gesperrt. Ironischerweise positioniert Musk Twitter seit seiner Übernahme immer wieder als Plattform für freie Rede, sperrte aber dennoch nicht nur Sweeneys umstrittenen Account, sondern auch mehrere Journalisten, die über die Sperre berichteten.



Elon Musk und Twitter

Auf Twitter zeitweise gesperrt...

Sweeney, der sich nicht unterkriegen lässt, kommentierte auch Twitters Ankündigung rechtlicher Schritte gegenüber Meta. Er berichtete, dass Musk ihm ebenfalls mit einer Klage gedroht habe, diese Drohung aber nicht in die Tat umgesetzt habe. Ein weiterer Beweis für Sweeneys unerschütterlichen Geist und seine Entschlossenheit, die Wahrheit ans Licht zu bringen.

Neben Threads veröffentlicht Sweeney die Positionsdaten auch auf den sozialen Netzwerken Mastodon, Bluesky und sogar Donald Trumps Truth Social. Doch es scheint, dass er auf Threads, das an Instagram gekoppelte Netzwerk, das bislang größte Publikum seit der Sperrung des Accounts auf Twitter erreicht hat. Dort hatte Sweeney zuletzt eine halbe Million Follower.

Jetzt sind die Flugbewegungen auf Threads zu sehen

Threads, der von Instagram entwickelte Kurznachrichtendienst, wurde am 6. Juli 2023 offiziell gestartet – allerdings vorerst nicht in Deutschland. Meta befürchtet, in der EU gegen Gesetze zu verstoßen und verschob den Europa-Start deshalb

auf unbestimmte Zeit.

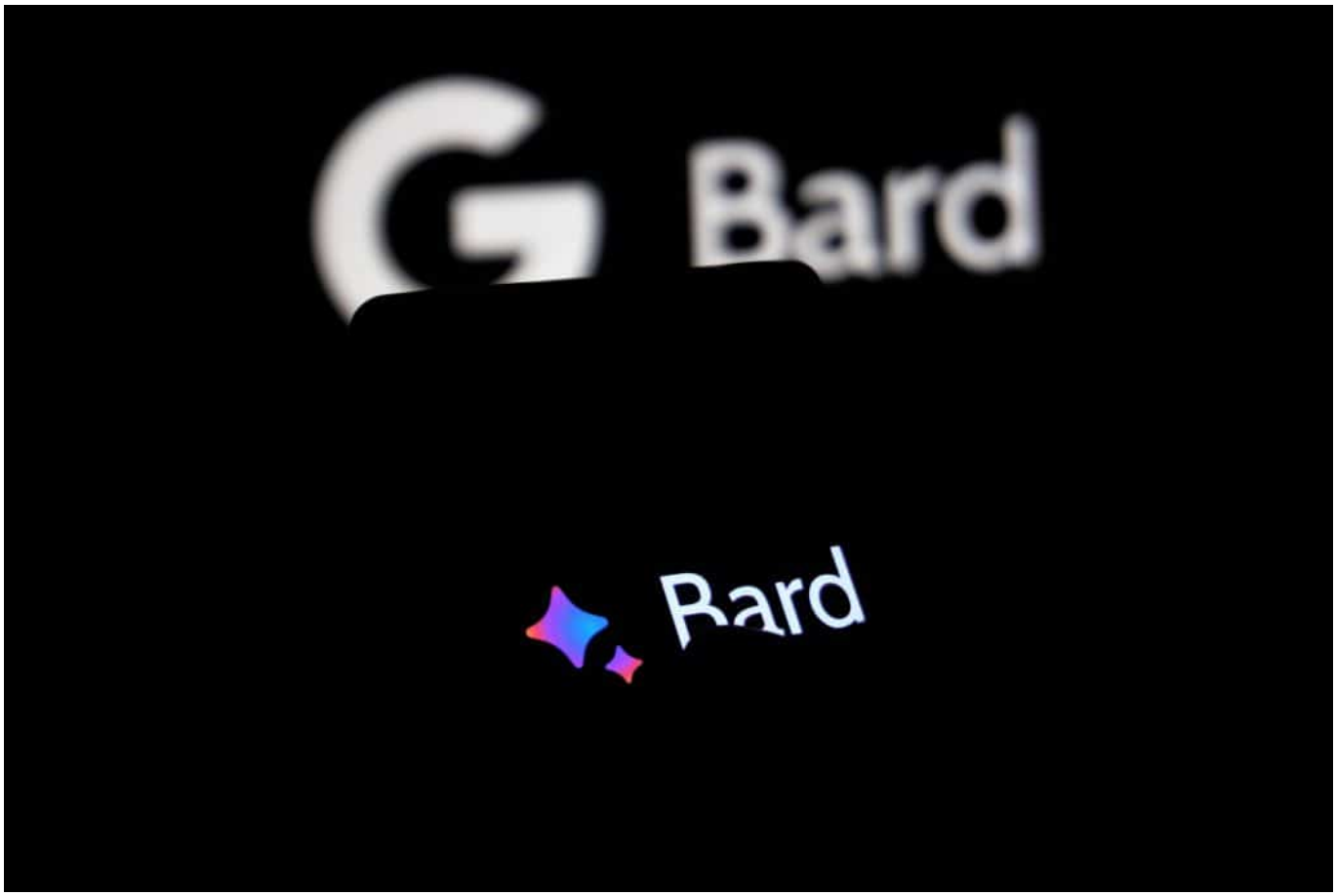
Es bleibt abzuwarten, ob Sweeney sich langfristig auch mit dem Betreiber von Threads anlegt. Neben @Elonmuskjet gibt es bereits den Account @Zuckerbergjet, der zukünftig die Position des Privatjets von Meta-CEO Mark Zuckerberg verfolgen könnte. Wer weiß, vielleicht wird Sweeney bald zum Flugdaten-Flüsterer für die gesamte Tech-Elite.

In einer Welt, in der die Mächtigen oft unantastbar scheinen, ist es erfrischend zu sehen, wie ein junger Mann wie Jack Sweeney sich nicht einschüchtern lässt und weiterhin die Wahrheit ans Licht bringt. Egal, ob Sie ein Fan von Musk sind oder nicht, man kann nicht leugnen, dass Sweeneys unermüdliche Verfolgung von Musks Privatjet eine faszinierende Geschichte ist, die uns alle an den Bildschirmen festhält. Bleiben Sie dran, um zu sehen, wohin die Reise als nächstes geht.

Bard jetzt auch in Deutschland vefügbar

Gleich zwei gute Nachrichten: Ab sofort kann Google Bard auch in Deutschland ganz offiziell benutzt werden. Außerdem kann Bard jetzt auch Bilder verarbeiten, die Tonalität ändern und vorlesen.

Wenn man sich im Bereich der künstlichen Intelligenz (KI) bewegt, sind Vergleiche zwischen den Vorreitern der Branche unvermeidlich. Im heutigen Fokus steht "Bard", eine KI-Anwendung, die in die Fußstapfen von OpenAI's ChatGPT tritt. Sie möchten Bard selbst testen? Lesen Sie weiter, um zu erfahren, wie.



Googles KI Bard kann jetzt auch in Deutschland benutzt werden

Bard und ChatGPT: Konkurrenz belebt das Geschäft

Bard und ChatGPT repräsentieren beide den Höhepunkt der KI-Technologie, aber mit einzigartigen Unterschieden und Stärken.

Bard ist bekannt für seine Fähigkeit, kohärente Geschichten zu generieren, die nicht nur einnehmend, sondern auch in ihrem Kontext einzigartig sind. Im Vergleich dazu hat ChatGPT eine umfassendere Ausbildung genossen und ist in der Lage, auf eine Vielzahl von Anfragen zu antworten und dabei ein menschenähnliches Gespräch zu simulieren.

Bard in Deutschland benutzen

Zum Testen von Bard können Sie die offizielle Webseite von Bard besuchen. Hier ist der direkte Link zur Anwendung: bard.google.com. Die folgenden Schritte helfen Ihnen, Bard auszuprobieren.

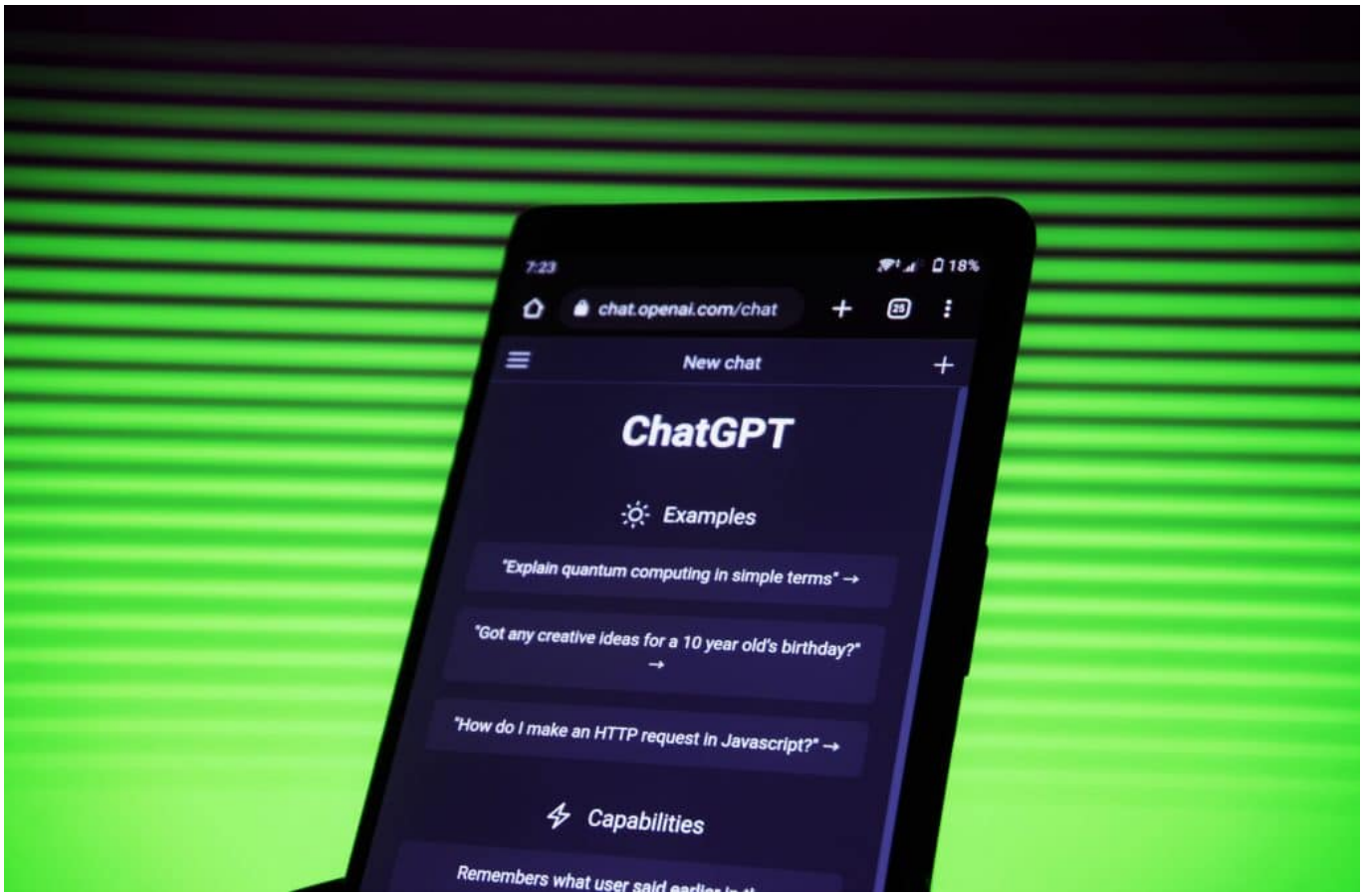
1. **Erstellen Sie ein Konto** – Klicken Sie auf "Sign Up" in der oberen rechten Ecke der Webseite und geben Sie Ihre E-Mail-Adresse sowie ein sicheres Passwort ein. Bestätigen Sie Ihre E-Mail-Adresse über den Link, den Sie in Ihrer E-Mail erhalten.
2. **Einloggen** – Nachdem Sie Ihr Konto erstellt haben, melden Sie sich auf der Webseite an. Sie werden auf die Hauptseite von Bard weitergeleitet.
3. **Bard ausprobieren** – Auf der Hauptseite finden Sie die Schaltfläche "Try Bard". Klicken Sie darauf, um das Bard-Interface zu öffnen.
4. **Erste Anfrage stellen** – Im Bard-Interface finden Sie ein Textfeld, in das Sie Ihre erste Anfrage eingeben können. Beginnen Sie einfach mit einer einfachen Anfrage oder einem Gesprächsthema, das Sie interessiert.
5. **Anfrage absenden** – Nachdem Sie Ihre Anfrage eingegeben haben, klicken Sie auf "Submit" oder drücken Sie Enter, um Ihre Anfrage an Bard zu senden.
6. **Ergebnisse analysieren** – Bard wird Ihre Anfrage analysieren und eine Antwort generieren. Sie können die Antwort analysieren und weitere Anfragen stellen, um ein tieferes Verständnis der Fähigkeiten von Bard zu erhalten.

Im Vergleich zu ChatGPT bietet Bard einen einzigartigen Ansatz für KI-gesteuerte Gespräche. Während ChatGPT auf die Generierung menschenähnlicher Antworten in Echtzeit fokussiert ist, konzentriert sich Bard eher auf die Generierung komplexer, einnehmender Geschichten.

Bard und ChatGPT im Vergleich

ChatGPT, entwickelt von OpenAI, basiert auf der GPT-3-Architektur und wurde mit unzähligen Texten aus dem Internet trainiert. Sein breites Training ermöglicht ihm, auf eine Vielzahl von Anfragen zu reagieren und dabei ein Gespräch zu simulieren, das dem eines Menschen sehr nahe kommt. Dies ist besonders nützlich für Anwendungen, die eine Echtzeit-Kommunikation erfordern, wie z.B. Kundenservice-Bots oder virtuelle Assistenten.

Bard hingegen wurde speziell für die Generierung von Geschichten entwickelt. Es verwendet eine speziell angepasste Version der GPT-Architektur, die auf die Generierung von kohärenten, einnehmenden und einzigartigen Geschichten ausgerichtet ist. Diese Fähigkeit ist besonders nützlich in kreativen Anwendungen, wie zum Beispiel beim Schreiben von Geschichten oder Drehbüchern.



ChatGPT ist schon länger am Start - und bekommt jetzt Konkurrenz

Beide KIs haben Stärken

Während beide KIs ihre eigenen Stärken haben, haben sie auch ihre Einschränkungen. ChatGPT kann manchmal Antworten geben, die zwar grammatikalisch korrekt sind, aber wenig Sinn ergeben, während Bard bei komplexen Anfragen Schwierigkeiten haben kann, die Kohärenz zu wahren.

Zusammenfassend kann gesagt werden, dass sowohl Bard als auch ChatGPT bahnbrechende Werkzeuge in der KI-Technologie sind, die uns einen Einblick in das Potenzial der zukünftigen menschlichen und KI-Interaktion bieten. Es ist spannend zu sehen, was die Zukunft für diese beiden Technologien bereithält.

WhatsApp: Unbekannte Anrufe stummschalten

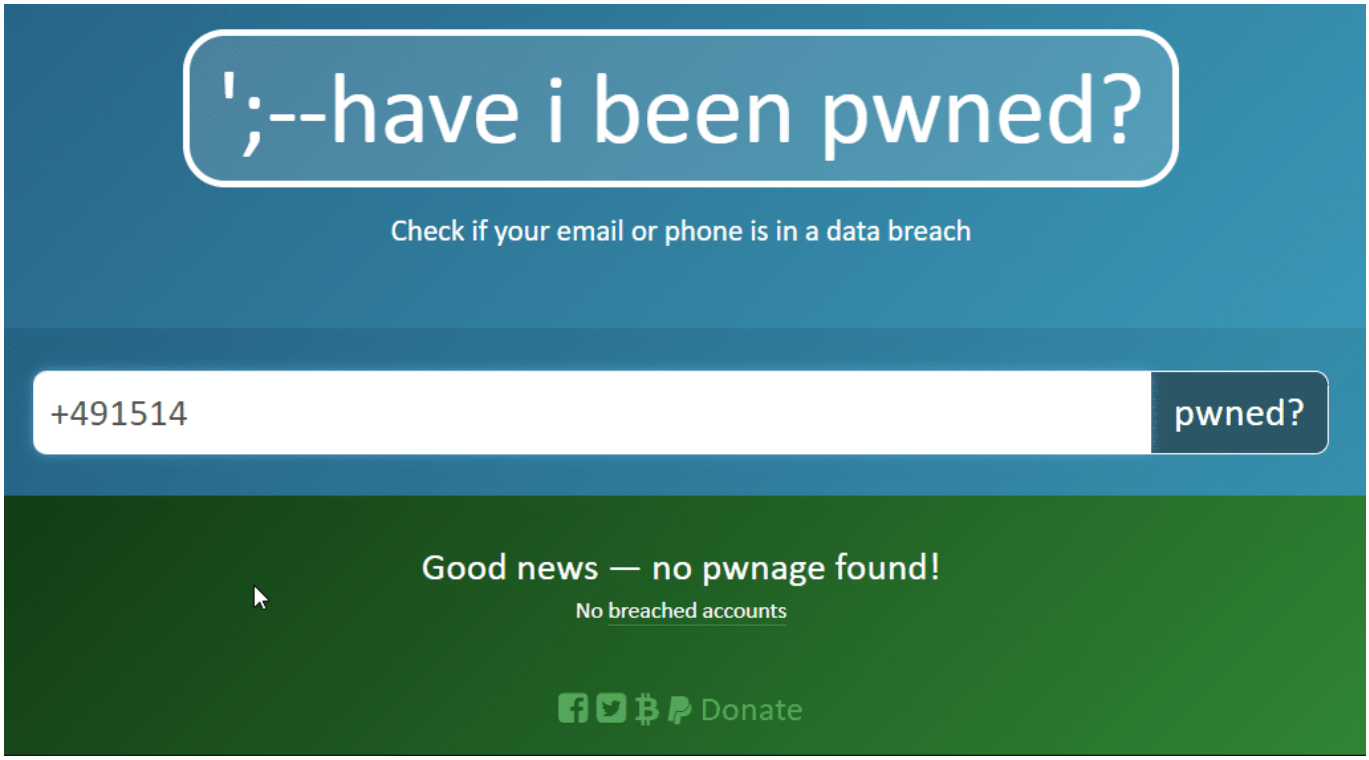
Eure Handynummer verteilt Ihr recht frei: Bei Preisausschreiben, an Bekannte, Handwerker oder auf Webseiten. Die Chance ist hoch, dass die auch in Datenbanken mit geklauten Zugangsdaten zu finden ist. Das hat Konsequenzen!

Ist Eure Mobilnummer gehackt?

Die Datenbanken gehackter Accounts mögen immer wieder neu zusammensortiert werden, am Ende stammen die meisten Daten aber aus diversen großen Hacks. Diese Daten haben aber nicht nur die Übeltäter, sondern auch diverse Seiten, die der guten Seite zuzurechnen sind. Beispielsweise haveipbeenpwnd.com. Auch wenn die eigentlich dafür bekannt ist, dass sie E-Mail-Adressen überprüft auf das Vorkommen in einem Hack: Sie funktioniert auch für Mobilnummern:

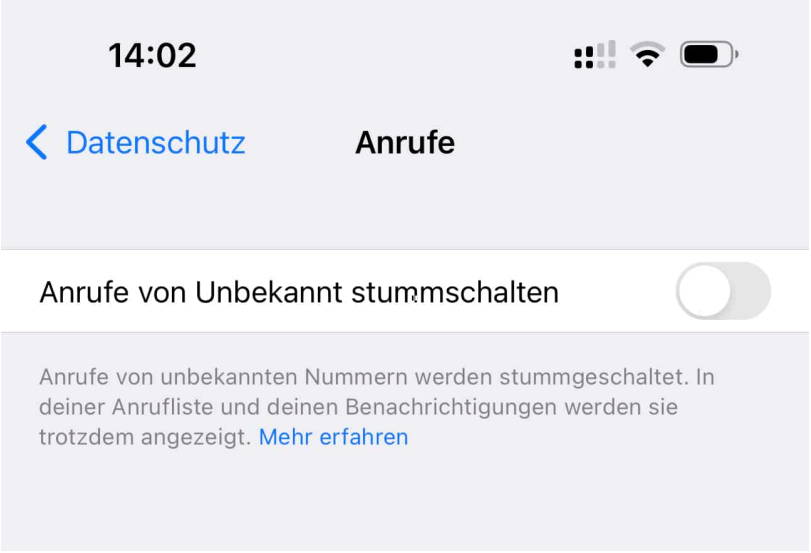
- Ruft die Webseite von haveibeenpwned.com auf.
- Gebt in das Suchfeld die Handynummer (mit führender Länderkennung,

also z.B. +49 für Deutschland) ein und klickt auf **pwned?**.
- Wenn Eure Rufnummer kompromittiert wurde, dann bekommt Ihr eine Warnung angezeigt.



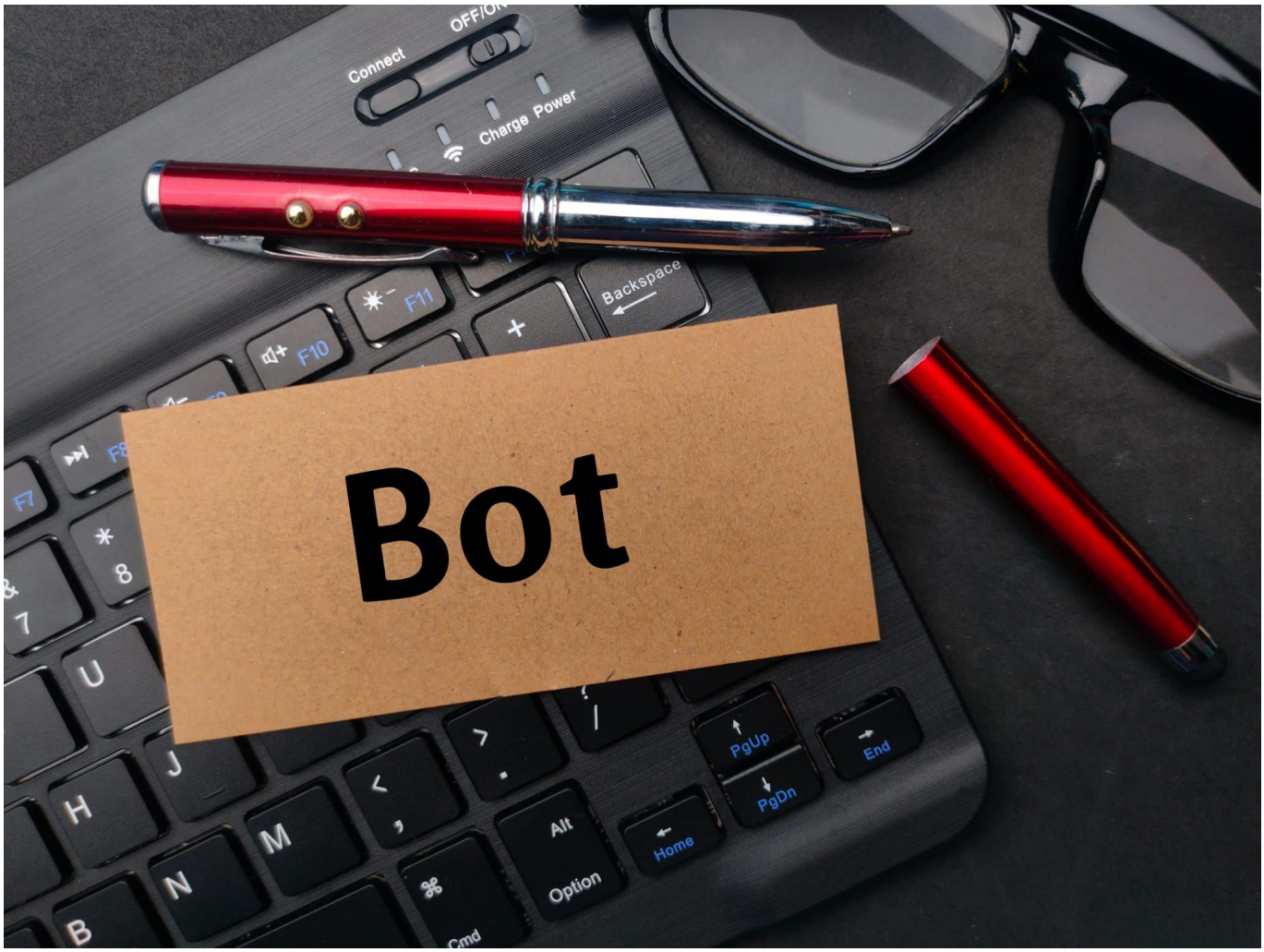
Ärgernis anonyme Anrufe

Vom Missbrauch der Rufnummer für Betrügereien abgesehen: Auch ohne ein Sicherheitsleck kann das nerven. Adresshändler lecken sich die Hände danach, Telefonnummern zu bekommen, die echt sind und möglichst noch einer Alters- oder Einkommensklasse zuordnenbar sind. Die werden dann für teures Geld verkauft und zur Werbung genutzt. Oft per WhatsApp, weil es kostengünstig nutzbar ist. Die Konsequenz: Ihr bekommt dauernd WhatsApp-Anrufe von unbekannten Nummern, die Euch etwas aufschwatzen wollen. Das könnte Ihr mit der aktuellen WhatsApp-Version aber verhindern:



- Klickt in WhatsApp auf **Einstellungen** > **Datenschutz**.
- Klickt dann auf **Anrufe**.
- Um keine Anrufe mehr von unbekannten Teilnehmer - also solchen, die nicht in Euren Kontakten sind - zu erhalten, aktiviert die Option **Anrufe von Unbekannt stummschalten**.
- Keine Sorge: Das betrifft nur die Signalisierung durch Klingeln und Vibration, diese Anrufe werden trotzdem in den Anruflisten angezeigt und gehen Euch nicht verloren.

Chatsonic: Alternativer KI-ChatBot

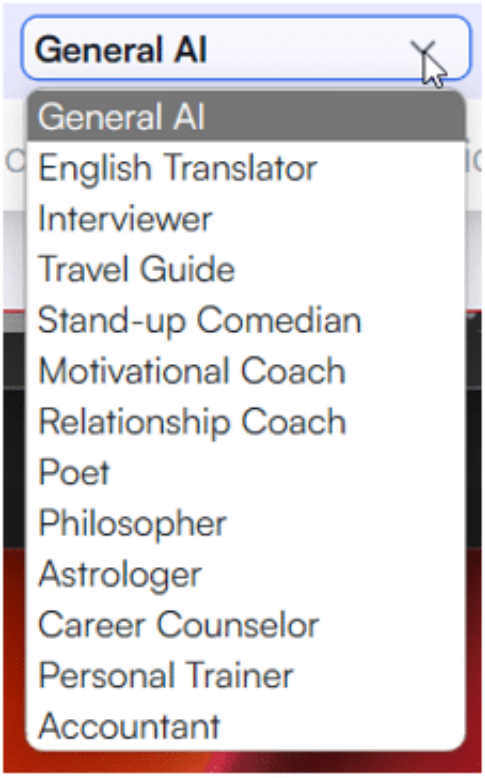


ChatGPT ist nicht der einzige ChatBot auf dem Markt. Auch andere Hersteller haben sich mittlerweile aufgemacht, um Euch mit einer KI für intelligente Dialogen und Artikel zu versorgen.

Nutzung von ChatGPT 3.5 und 4

ChatBots sind vor allem für ihre Konversationsfähigkeiten bekannt: Gebt einen Text ein, der ChatBot sucht sich die Informationen dazu zusammen und bereitet diese in Form von Antworten auf. Interessant wird es, wenn noch weitere Funktionen hinzukommen. Da ist Chatsonic eine interessante Alternative: Das basiert auf der Infrastruktur von ChatGPT 3.5 und 4, integriert aber zusätzlich noch die Möglichkeit, Bilder aus Eingaben zu generieren und auch auf

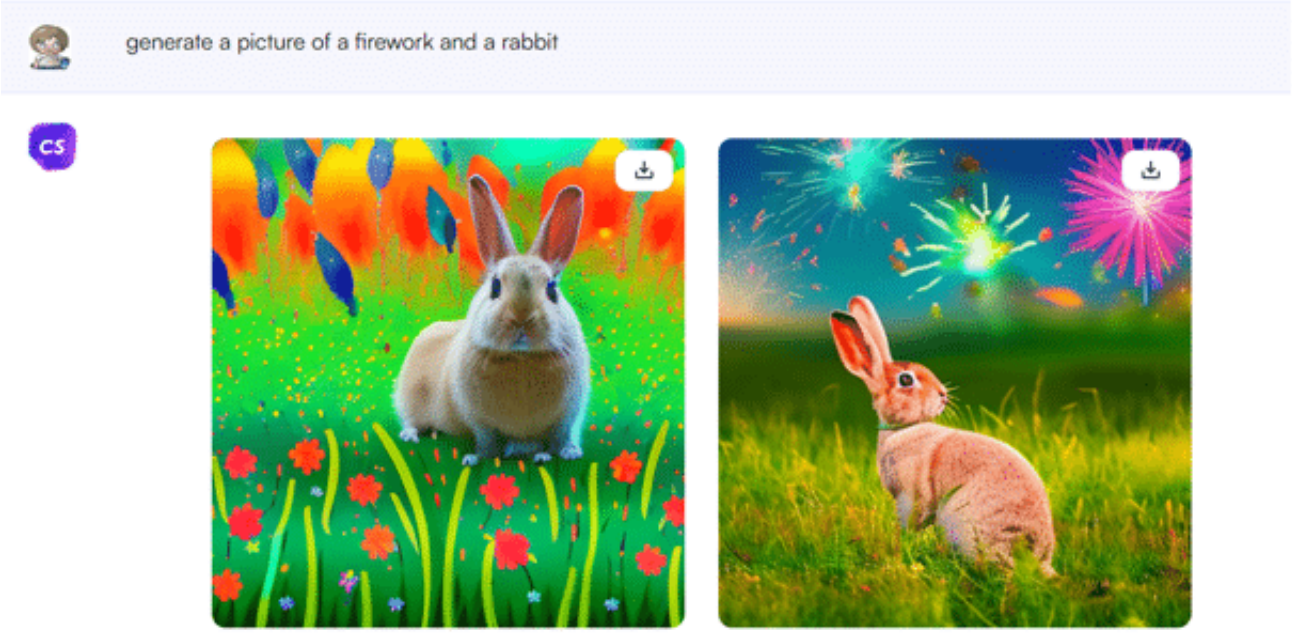
Spracheingaben zu reagieren. 25 Anfragen am Tag sind in Chatsonic frei, das sollte für die meisten Privatanwender ausreichen. Wenn nicht, dann stehen zwei kostenpflichtige Pläne zur Auswahl.



Flapsige Antworten und Generierte Bilder

- Ruft die Webseite von Chatsonic
- Meldet Euch mit Eurem Google- oder Apple-Account an oder legt ein eigenes Konto an.
- Bei Chatsonic könnt Ihr für die Formulierung der Ausgabe aus verschiedenen Typen von AIs auswählen. Das beeinflusst die Art der Antwort. Der **Stand-Up-Comedian** antwortet eher lustig, der **Poet** eher ausschweifend-literarisch und so weiter. Probiert einfach ein paar Einstellungen aus.
- Durch das Aktivieren von **Include latest Google data** aktiviert Ihr eine Besonderheit von Chatsonic: Normalerweise finden eher statische Quellen Verwendung in einem Chatbot. Mit dieser Option greift die KI auch auf aktuelle Google-Suchergebnisse zu.
- Um ein Bild zu generieren, schreibt als Eingabetext „generate an image of“ und dann das Thema. Die so generierten Bilder könnt Ihr herunterladen, wenn Ihr auf den **Download-Button**

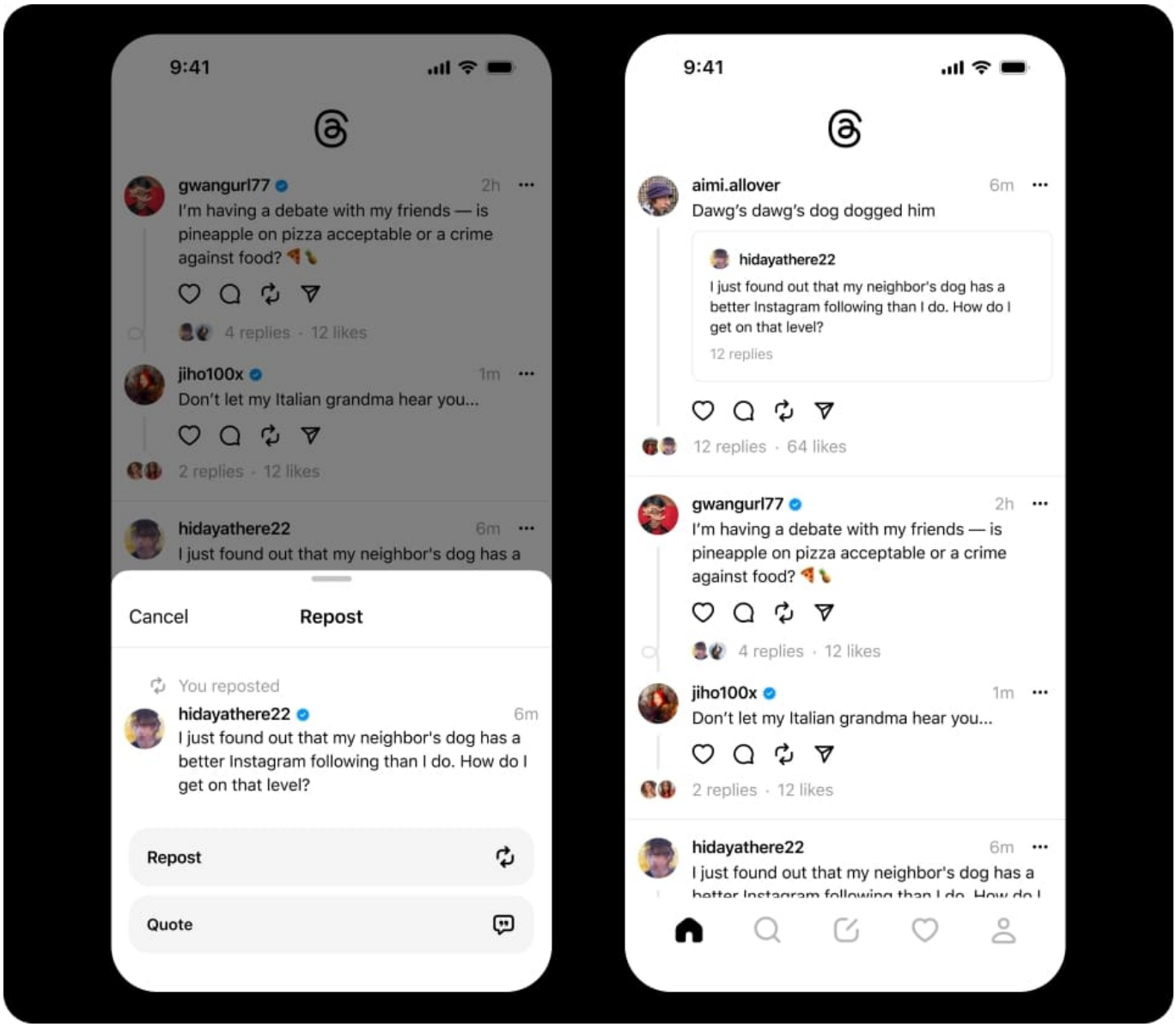
- Ihr könnt auch verschiedene Arten von Ausgabeformaten in die Anfrage integrieren. Wenn Ihr beispielsweise „Write an Instagram post about“ als ersten Teil der Anweisung benutzt, dann formuliert ChatSonic als Instagram-Beitrag, zu dem Ihr über **Copy Code** auch gleich den HTML-Code zum Einbetten herunterladen könnt.



Meta und der EU-Markt: Warum Threads hier nicht startet

Ein interessanter Vorgang: Ein Riese wie Meta startet einen global beachteten neuen Dienst - in 100 Ländern weltweit. Nur nicht in der EU. Weil hier Gesetze gelten, die Konsumenten schützen. Ist das nun gut - oder schadet das der Innovation?

Twitter hat schon immer seine Herausforderungen gehabt, aber seit der Übernahme durch Elon Musk hat sich der Kurznachrichtendienst so stark verändert, dass viele Nutzer nach Alternativen suchen. Von gesperrten Accounts über strikte Monetarisierung bis hin zu technischen Problemen - die Liste der Veränderungen ist lang und hat viele Nutzer verunsichert.



Threads: Die neue Hoffnung

In diesem Kontext hat sich ein neuer Konkurrent mit großem Potenzial hervorgetan: Threads. Dieser Kurznachrichtendienst wurde von Instagram, einem Tochterunternehmen von Meta, entwickelt und am 6. Juli 2023 gestartet - allerdings nicht in der EU.

Bereits im März 2023, nur vier Monate nachdem Musk den Kauf von Twitter abschließen musste, gab es erste Berichte darüber, dass Meta an einer eigenen Konkurrenz zu Twitter arbeitet. Im Mai tauchten dann erste geleakte Screenshots im Netz auf.

Der beeindruckende Start von Threads

Meta ist bereits der größte Social-Media-Konzern der Welt. Mit Facebook, Whatsapp und Instagram kommt das Unternehmen von Mark Zuckerberg zusammen auf rund sieben Milliarden Accounts. Im Vergleich dazu kam Twitter im Jahr 2022 auf ein weltweites Publikum von 368 Millionen.

Was Threads im Vergleich zu anderen Plattformen wie Mastodon oder Bluesky einen enormen Startvorteil beschert, ist die bestehende Nutzerbasis von Instagram. Mehr als eine Milliarde Konten können sich sofort einloggen, ohne einen neuen Account anlegen zu müssen. Selbst ohne europäische Nutzer brauchte Threads nur sieben Stunden, um den Meilenstein von 10 Millionen Nutzern zu erreichen. Nach einem Tag waren es bereits 30 Millionen.

Facebook hat einen neuen Dienst namens Threads eingeführt

Der europäische Markt: Eine verpasste Chance?

Trotz des beeindruckenden Starts stellt sich die Frage, warum Meta auf den europäischen Millionenmarkt verzichtet. Die Antwort auf diese Frage ist nicht ganz einfach und erfordert ein tieferes Verständnis der rechtlichen und technischen Herausforderungen, die mit einem solchen Schritt verbunden sind.

Der Digital Markets Act: Ein Stolperstein für Meta

Ein wichtiger Faktor, der Meta davon abhält, Threads in der EU zu starten, ist der Digital Markets Act (DMA). Dieses Gesetz wurde von der Europäischen Union eingeführt, um den Wettbewerb im digitalen Markt zu fördern und zu regulieren. Es zielt darauf ab, die Dominanz von großen Tech-Unternehmen zu begrenzen und kleineren Unternehmen mehr Chancen zu geben.

Der DMA stellt strenge Anforderungen an sogenannte "Gatekeeper"-Unternehmen, also Unternehmen, die eine dominante Position im Markt einnehmen und den Zugang zu bestimmten Diensten oder Produkten kontrollieren. Meta, mit seinen Milliarden von Nutzern und einer Vielzahl von Plattformen, fällt definitiv in diese Kategorie.

Unter dem DMA müssen Gatekeeper-Unternehmen eine Reihe von Verpflichtungen erfüllen, darunter die Gewährleistung der Interoperabilität ihrer Dienste, das Verbot von exklusiven Vorinstallationen und das Verbot von Maßnahmen, die den Wettbewerb behindern könnten. Diese Anforderungen könnten für Meta eine Herausforderung darstellen, insbesondere wenn es darum geht, Threads in der EU zu starten.

Zum Beispiel könnte die Anforderung der Interoperabilität bedeuten, dass Meta Threads so gestalten muss, dass es mit anderen Kurznachrichtendiensten kompatibel ist. Dies könnte zusätzliche technische Herausforderungen und Kosten verursachen. Darüber hinaus könnte das Verbot von exklusiven Vorinstallationen bedeuten, dass Meta Threads nicht automatisch auf den Geräten seiner Nutzer installieren kann, was die Verbreitung der App erschweren könnte.

In der EU behindern strenge Regeln die Einführung von Threads

Fazit: Ein schwieriger Weg nach Europa

Insgesamt stellt der Digital Markets Act eine erhebliche Hürde für Meta dar, wenn es darum geht, Threads in der EU zu starten. Während das Unternehmen sicherlich die Ressourcen hat, um diese Herausforderungen zu bewältigen, könnte es entscheiden, dass die Kosten und der Aufwand einfach zu hoch sind.

Es bleibt abzuwarten, ob Meta in der Zukunft einen Weg finden wird, Threads in der EU zu starten. Bis dahin müssen europäische Nutzer auf andere Alternativen zurückgreifen oder auf Umwegen versuchen, Zugang zu Threads zu bekommen.

Windows 11: Notfall Restart durchführen

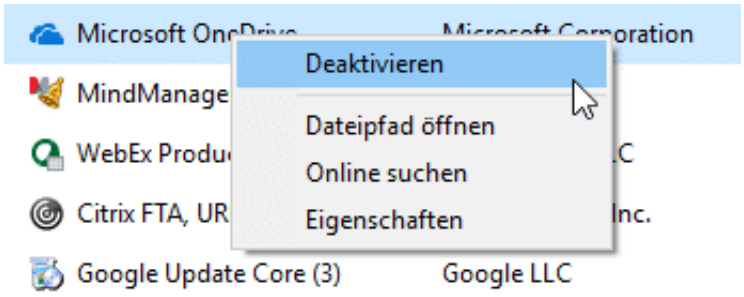
Windows 11 ist im Normalfall sehr stabil, aber es gibt immer mal Situationen, in denen es sich nicht so verhält, wie es soll. Es bietet aber auch einige versteckte Optionen, mit denen Ihr schonend neustarten könnt!

Ausschalten als letzte Lösung!

Wenn Ihr schnell weiterarbeiten wollt, Euer PC oder ein Programm nicht mehr reagiert, dann liegt es intuitiv nah, den PC auszuschalten. Das solltet Ihr aber möglichst nicht tun, denn damit nehmt Ihr jedem laufenden Programm jede Möglichkeit, ordentlich beendet zu werden und alle Daten zu speichern. Probiert vorher folgendes:

- Versucht, eventuell blockierende oder CPU-fressende Dienste über den Task Manager zu beenden. Auch das ist nicht risikolos, trifft aber pro

Dienst immer nur ain Programm und nicht alle laufenden.
- Wenn das Problem häufiger auftritt, dann solltet Ihr überlegen, die betroffenen Dienste aus dem Autostart auszuschließen.
- Versucht den PC normal runterzufahren.



Herunterfahren des PCs

Um den PC herunterzufahren, habt Ihr in Windows diverse Möglichkeiten:

- Klickt auf die Start-Schaltfläche, dann auf den Power Button.
- Öffnet den Task-Manager durch gleichzeitiges Drücken von **Alt** + **Strg** + **Entf** und dann auf den Power Button.
- Wechselt durch **Alt** + **D** auf den Desktop, dann wählt **Herunterfahren**.

Beim Herunterfahren des Rechners beendet Windows geordnet alle Dienste und Programme. Bei letzteren überprüft jedes Programm, ob alle Daten gespeichert sind. Wenn nicht, bekommt Ihr einen Hinweistext. Ohne Reaktion darauf blockiert das jeweilige Programm das Herunterfahren. Das vermeidet Datenverluste. Wenn keine der Optionen zum Herunterfahren funktioniert, dann habt Ihr noch einen weiteren Pfeil im Köcher, bevor Ihr Euren PC ausschaltet. Der ist wenig bekannt.

Geheime Restart-Option

Die normalen Neustart-Optionen funktionieren meist, aber nicht immer. Vor allem, wenn irgendwelche Windows-Module oder Dienste einander blockieren, werdet Ihr umsonst auf den Restart warten. Windows hat hier aber einen geheimen Restart-Modus versteckt:

- Öffnet den Task-Manager durch gleichzeitiges Drücken von **Alt** + **Strg** + **Entf** aber klickt noch nicht auf den Power Button.
- Stattdessen drückt auf der Tastatur die **Strg-Taste** und haltet sie gedrückt.

Erst dann klickt mit der Maus auf den Power-Button.

- Windows zeigt Euch auf dem kompletten Bildschirm eine Meldung an, dass es einen Notfall-Neustart durchführen kann, das Risiko hier aber Datenverlust ist. Ein Klick auf **OK** führt diesen Neustart durch. Der Unterschied zum Ausschalten ist hier, dass Windows nacheinander alle Möglichkeiten ausprobiert, jedes Programm ordentlich zu beenden und damit Datenverluste zu vermeiden.