

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

Schieb Report

Ausgabe 2023.48

Third Party Cookies: Was Sie über diese kleinen Datenkrümel wissen sollten



Cookies können durchaus nützlich sein, etwa beim Online-Shopping oder Besuch einer Webseite. Doch viele Cookies haben Einfluss auf unsere Privatsphäre, weil sie der Werbebranche helfen, uns auszukundschaften - das sind die sogenannten Third Party Cookies.

Third Party Cookies sind - bildlich gesprochen - kleine Datenkrümel, die von Drittanbietern auf einer Website gesetzt werden. Diese Cookies werden verwendet, um Informationen über Nutzer zu sammeln und für Werbung, Marketing und Tracking-Zwecke zu nutzen.

Einige Browser wie Chrome bieten Nutzern die Möglichkeit, Third Party Cookies zu blockieren und somit ihre Datenschutzrechte zu schützen. Es ist wichtig, sich über die Verwendung von Third Party Cookies und deren Auswirkungen auf die Domain und die Informationen der Nutzer bewusst zu sein.



Warum werden Third Party Cookies verwendet?

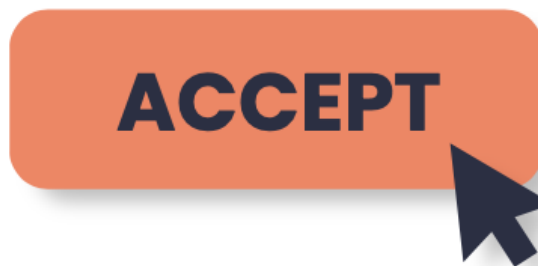
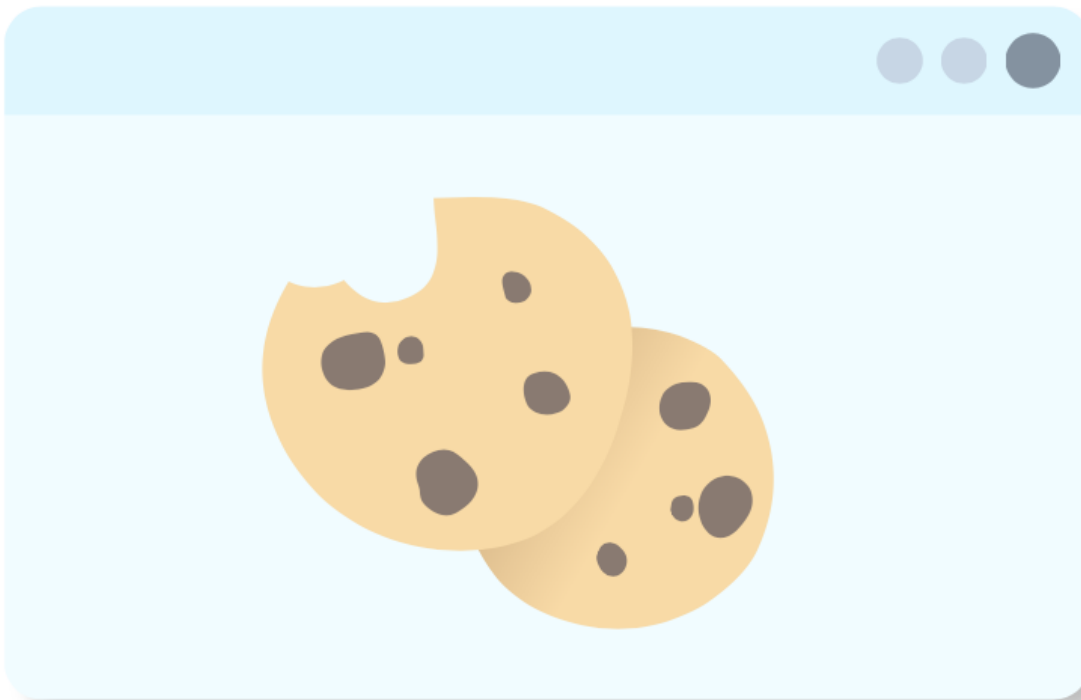
Third Party Cookies sind ein wichtiger Bestandteil des Online-Marketings und werden von Unternehmen genutzt, um Informationen über Nutzer zu sammeln.

Diese Daten können dann für gezielte Werbung und Analytics verwendet werden. Third Party Cookies werden oft von Drittanbietern wie Google Analytics auf Websites platziert, um das Verhalten der Nutzer aufzuzeichnen. Sie ermöglichen es den Betreibern, die Effektivität ihrer Website zu messen und zu verbessern.

Auch wenn einige Browser wie Chrome standardmäßig Third Party Cookies blockieren, gibt es immer noch viele Websites, die sie nutzen.

Datenschutzbedenken im Zusammenhang mit Third Party Cookies bestehen darin, dass persönliche Daten ohne Zustimmung gesammelt werden können.

Es ist wichtig für Nutzer und Unternehmen gleichermaßen sicherzustellen, dass sie verantwortungsbewusst mit diesen Daten umgehen und sich an die geltenden Regulierungen halten. Insgesamt bieten Third Party Cookies viele Vorteile für Nutzer und Unternehmen in Bezug auf personalisierte Werbung und verbesserte Website-Performance.



Überall werden ungeniert Daten eingesammelt

Datenschutzbedenken im Zusammenhang mit Third Party Cookies

Im Zusammenhang mit Third Party Cookies gibt es einige Datenschutzbedenken, die Nutzer und Unternehmen gleichermaßen betreffen. Durch das Sammeln von Daten durch Dritte kann das Tracking des Nutzerverhaltens auf verschiedenen Websites ermöglicht werden.

Dabei können Informationen wie besuchte Websites, Werbung und Marketing-Präferenzen gesammelt werden. Besonders Google Analytics als bekanntes Beispiel verwendet Third Party Cookies zur Erfassung von Nutzerdaten. Es ist wichtig zu wissen, dass diese Cookies nicht nur von der Website verwendet werden, auf der sie gesetzt wurden, sondern auch von anderen Websites in derselben Domain.

Viele Browser bieten inzwischen Optionen an, um Third Party Cookies zu blockieren oder einzuschränken - beispielsweise Google Chrome bietet hierfür verschiedene Einstellungsmöglichkeiten an. Es ist jedoch zu beachten, dass das Blockieren dieser Cookies auch Auswirkungen auf die Funktionalität einiger Websites haben kann.

Um sich vor den Nachteilen von Third Party Cookies zu schützen, sollten Nutzer stets bewusst mit ihren Cookie-Einstellungen umgehen und sich über die Datenerfassung durch Dritte informieren.

Die Vorteile von Third Party Cookies für Nutzer und Unternehmen

Third Party Cookies sind für Nutzer und Unternehmen gleichermaßen von Vorteil. Für Nutzer bieten diese kleinen Datenkrümel ein personalisiertes Erlebnis beim Surfen im Internet. So können beispielsweise Werbeanzeigen auf den Interessen und Suchanfragen des Nutzers basieren, was zu relevanteren Inhalten führt.

Auch Website-Betreiber profitieren von Third Party Cookies, da sie dadurch wertvolle Informationen über das Verhalten der Nutzer auf ihrer Domain sammeln können. Diese Daten werden oft für Analytics- und Marketing-Zwecke genutzt, um die Website zu verbessern oder gezielte Werbung auszuliefern.

Ein bekannter Anbieter von [Third Party Cookies](#) ist Google mit seinem Chrome-Browser, der es Website-Betreibern ermöglicht, Informationen über ihre Besucher zu sammeln. Doch trotz dieser Vorteile gibt es auch Bedenken bezüglich Datenschutz und Tracking durch Dritte.

Allerdings gibt es auch Möglichkeiten sich vor den Nachteilen von Third Party Cookies zu schützen, wie zum Beispiel das Blockieren von Third Party Cookies in den Browsereinstellungen oder das Verwenden alternativer Datenerfassungstechnologien ohne Third Party Cookies.

Letztendlich liegt es jedoch an jedem einzelnen Nutzer und Unternehmen verantwortungsvoll mit dieser Technologie umzugehen und sich an geltende Regulierungen und Gesetze zum Datenschutz zu halten.



Cookies werden auf der Festplatte, aber auch im Speicher von Mobilgeräten gespeichert (Symbolhaft)

Wie kann man sich vor den Nachteilen von Third Party Cookies schützen?

Third Party Cookies haben den Vorteil, dass sie für viele Unternehmen ein wichtiges Instrument im Marketing sind. Allerdings gibt es auch Nachteile, die nicht außer Acht gelassen werden sollten. Dazu gehören vor allem Datenschutzbedenken und das Tracking von Nutzern durch Third-Party-Cookies.

Um sich vor diesen Nachteilen zu schützen, gibt es verschiedene Möglichkeiten. Eine Option ist es, den eigenen Browser so einzustellen, dass keine Third-Party-Cookies zugelassen werden.

Hierfür bietet beispielsweise Google Chrome entsprechende Einstellungen an. Darüber hinaus können Nutzer auch Add-ons oder Plugins installieren, die das Sammeln von Daten durch Third-Party-Cookies verhindern. Eine weitere Möglichkeit ist es, gezielt Websites aufzusuchen, die auf den Einsatz von Third-Party-Cookies verzichten oder nur First-Party-Cookies verwenden. So kann man sicherstellen, dass keine ungewollten Informationen gesammelt werden und der Datenschutz gewahrt bleibt.



Alternativen zu Third Party Cookies: Möglichkeiten der Datenerfassung ohne diese Technologie

Immer mehr Nutzer sorgen sich um ihre Privatsphäre im Internet, besonders wenn es um das Thema Third Party Cookies geht. Daher suchen viele Unternehmen nach Alternativen, um Daten zu sammeln ohne diese Technologie zu verwenden. Eine Möglichkeit ist die Verwendung von First-Party-Cookies, die nur Informationen auf der eigenen Website speichern und somit nicht für Trackingzwecke verwendet werden können. A

uch Browser-Erweiterungen wie uBlock Origin oder Privacy Badger bieten Schutz vor Tracking durch Drittanbieter-Cookies. Zudem gibt es verschiedene Analytics-Tools, die ohne Third Party Cookies auskommen und dennoch wertvolle Informationen über Nutzer und deren Verhalten auf einer Website liefern können.

Google Analytics bietet beispielsweise eine Möglichkeit zur IP-Anonymisierung an, um den Datenschutz zu erhöhen. Auch Marketing-Maßnahmen wie E-Mail-Kampagnen oder Social Media Ads können genutzt werden, um gezielt Werbung an Zielgruppen zu richten, ohne dass dabei Third Party Cookies zum Einsatz kommen müssen.

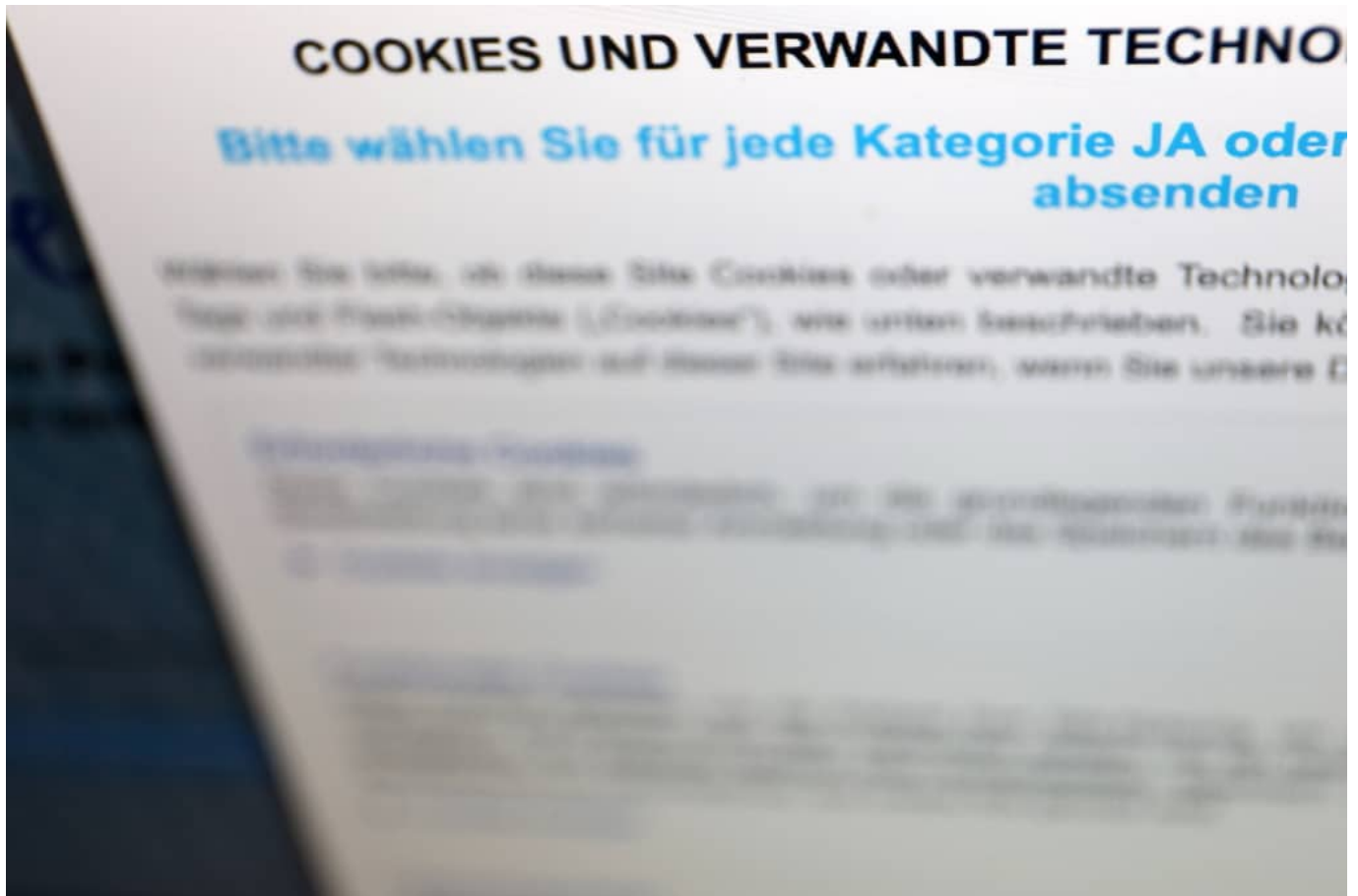
Es gibt also durchaus Möglichkeiten der Datenerfassung ohne Third Party Cookies – Unternehmen sollten diese Optionen in Betracht ziehen und verantwortungsvoll damit umgehen.

Die Rolle von Regulierungen und Gesetzen bei der Nutzung von Third Party Cookies

Die Nutzung von Third Party Cookies wird oft kontrovers diskutiert, insbesondere in Bezug auf den Datenschutz. Regulierungen und Gesetze spielen dabei eine wichtige Rolle, um die Nutzung dieser Technologie zu regulieren und sicherzustellen, dass Nutzerdaten nicht missbraucht werden.

Ein Beispiel hierfür ist die europäische Datenschutz-Grundverordnung (DSGVO), welche die Verwendung von Cookies einschränkt und Anforderungen an Transparenz und Zustimmung der Nutzer stellt. Auch Browser wie Google Chrome haben Maßnahmen ergriffen, um Tracking durch Dritte zu beschränken.

Unternehmen müssen daher sicherstellen, dass sie sich an diese Regulierungen halten und transparent über ihre Verwendung von Third Party Cookies informieren. Durch eine verantwortungsvolle Verwendung von Cookies können Unternehmen wertvolle Informationen sammeln, um das Marketing und die Werbung zielgerichteter zu gestalten, ohne dabei die Privatsphäre der Nutzer zu beeinträchtigen.



Best Practices für die Verwendung von Third Party Cookies in einer verantwortungsvollen Art und Weise

Eine verantwortungsvolle Verwendung von Third Party Cookies ist unerlässlich, um den Datenschutz der Nutzer zu gewährleisten.

Unternehmen sollten sich bewusst sein, welche Informationen über die Nutzer sie sammeln und wie sie diese verwenden. Zudem empfiehlt es sich, nur notwendige Daten zu erheben und eine klare Einwilligung einzuholen. Eine weitere Best Practice ist das regelmäßige Löschen von Cookies, insbesondere wenn sie nicht mehr benötigt werden.

Auch das Anonymisieren von Daten trägt dazu bei, dass die Privatsphäre der Nutzer gewahrt bleibt. Um das Tracking durch Third Party Cookies zu minimieren, können auch Browser-Add-Ons oder spezielle Einstellungen im Browser wie beispielsweise im Google Chrome genutzt werden.

Zusätzlich sollten Unternehmen sicherstellen, dass ihre Partner-Websites

ebenfalls verantwortungsvoll mit den Daten umgehen und keine sensiblen Informationen weitergeben oder missbrauchen. Durch die Einhaltung dieser Best Practices können Unternehmen das Vertrauen der Nutzer stärken und gleichzeitig ihre Marketing-Strategien optimieren.

Der richtige Umgang mit Third-Party-Cookies

Im Fazit lässt sich festhalten, dass der richtige Umgang mit Third-Party-Cookies entscheidend für den Datenschutz und die Privatsphäre von Nutzern ist. Unternehmen sollten transparent sein und Nutzer darüber informieren, welche Informationen durch Cookies gesammelt werden und zu welchem Zweck diese Verwendung finden.

Es empfiehlt sich außerdem, alternative Methoden zur Datenerfassung zu nutzen und nicht ausschließlich auf Third-Party-Cookies zu setzen. Browser wie Google Chrome bieten inzwischen auch Möglichkeiten, Cookies direkt zu blockieren oder nur für bestimmte Websites zuzulassen.

Eine verantwortungsvolle Nutzung von Third-Party-Cookies kann dazu beitragen, personalisierte Werbung und Marketingstrategien auf den Bedarf des Nutzers abzustimmen, ohne das Recht auf Datenschutz zu verletzen. Insgesamt gilt es bei der Verwendung von Third-Party-Cookies immer abzuwägen, welcher Mehrwert sie für Unternehmen und Nutzer bieten können und welche Risiken damit verbunden sind.



Was machen Third Party Cookies?

Third-Party-Cookies werden oft von Werbetreibenden auf Websites platziert, um das Nutzerverhalten zu verfolgen und personalisierte Anzeigen zu schalten. Diese Cookies werden von einer Domain platziert, die nicht die gleiche ist wie die Website, auf der der Nutzer sich befindet. Sie können verwendet werden, um Informationen über das Surfverhalten eines Nutzers auf verschiedenen Websites zu sammeln und ein detailliertes Profil zu erstellen.

Diese Cookies sind oft mit Tracking-Technologien verbunden, die es Werbetreibenden ermöglichen, das Verhalten eines Nutzers über mehrere Websites hinweg zu verfolgen. Dies ermöglicht es ihnen, personalisierte Anzeigen basierend auf dem Surfverhalten des Nutzers anzuzeigen.

Third-Party-Cookies können auch verwendet werden, um eine Vielzahl von Daten über den Benutzer zu sammeln, einschließlich Standortdaten und Geräteinformationen. Diese Daten können dann für gezielte Werbung oder andere Marketingzwecke verwendet werden.

Obwohl Third-Party-Cookies oft dazu beitragen können, personalisierte Erfahrungen im Internet bereitzustellen, haben sie auch Bedenken hinsichtlich

Datenschutz und Sicherheit ausgelöst. Viele Browser blockieren mittlerweile standardmäßig Third-Party-Cookies oder bieten Optionen zum Blockieren oder Löschen dieser Cookies an.

Sind Third Party Cookies erlaubt?

Third-Party-Cookies sind Cookies, die von einer anderen Domain als der besuchten Website gesetzt werden. Ob diese erlaubt sind oder nicht, hängt von den Datenschutzrichtlinien der besuchten Website ab. In der Regel müssen Nutzer ihre Zustimmung zur Verwendung von Third-Party-Cookies geben. Die meisten Browser blockieren standardmäßig Third-Party-Cookies aus Datenschutzgründen. Einige Websites können jedoch möglicherweise nicht ordnungsgemäß funktionieren, wenn Third-Party-Cookies blockiert werden.

In Europa gibt es die EU-Datenschutzgrundverordnung (DSGVO), die vorschreibt, dass Websites ihre Besucher über die Verwendung von Cookies informieren und um deren Zustimmung bitten müssen. Dies gilt auch für Third-Party-Cookies. Es ist wichtig zu beachten, dass einige Unternehmen wie Google und Facebook aufgrund ihrer Geschäftsmodelle stark auf Third-Party-Cookies angewiesen sind.

Wenn diese Cookies blockiert werden, kann dies Auswirkungen auf das Tracking und die Personalisierung von Werbung haben. Insgesamt ist es Sache des Nutzers zu entscheiden, ob er Third-Party-Cookies erlauben möchte oder nicht. Es ist jedoch wichtig, sich über die damit verbundenen Risiken und Datenschutzrichtlinien im Klaren zu sein.

Warum werden Third Party Cookies abgeschafft?

[Third Party Cookies werden abgeschafft](#), weil sie ein ernsthaftes Problem für die Privatsphäre der Nutzer darstellen. Diese Cookies werden von Websites verwendet, um Daten über das Verhalten und die Interessen der Nutzer zu sammeln, ohne dass diese davon wissen oder zustimmen.

Das sogenannte Tracking ermöglicht es Drittanbietern, Werbung gezielt an bestimmte Nutzer auszurichten und personalisierte Profile zu erstellen. Dieses Vorgehen wird jedoch als eine Verletzung der Privatsphäre angesehen. Es gibt auch Bedenken hinsichtlich des Missbrauchs von Daten durch Dritte und den Schutz vor Cyberkriminalität. Aus diesem Grund haben viele Browserhersteller beschlossen, Third Party Cookies zu blockieren oder ganz abzuschaffen.

Eine weitere Ursache dafür ist die Regulierung durch die Datenschutzgesetze wie z.B. die Datenschutzgrundverordnung (DSGVO), welche den Schutz personenbezogener Daten stärkt und Unternehmen dazu verpflichtet, Transparenz über ihre Datensammlung und -verarbeitung zu schaffen.

Die Abschaffung von Third Party Cookies kann jedoch Auswirkungen auf das Online-Marketing haben, da es schwieriger wird, Zielgruppen gezielt anzusprechen. Unternehmen müssen sich daher auf alternative Lösungen wie First-Party-Cookies oder kontextuelles Targeting konzentrieren. Insgesamt ist die Abschaffung von Third Party Cookies ein wichtiger Schritt zur Wahrung der Privatsphäre im digitalen Zeitalter und zur Stärkung des Datenschutzes.

<https://www.youtube.com/watch?v=1KQ1kEWpfKY&t=237s>

MFA entmystifiziert: Alles, was du über die Multi Faktor Authentifizierung wissen musst



Wer seine Online-Konten optimal absichern will, ist gut beraten, auf "Multifaktor Authentifizierung" (MFA) zu setzen. Neben einem Passwort muss noch ein Code eingegeben werden, der in der Regel im Smartphone generiert wird.

Willst du wissen, was MFA ist und wie es funktioniert? Dann bist du hier genau richtig! In diesem Artikel erfährst du alles, was du über die Multi Faktor Authentifizierung wissen musst.



Was ist MFA und warum ist es wichtig?

MFA, oder Multi-Faktor-Authentifizierung ist ein wichtiger Schutzmechanismus für deine Konten und Daten. Durch die Verwendung von MFA wird ein zusätzlicher Schutzschritt hinzugefügt, der sicherstellt, dass nur autorisierte Personen auf dein Konto zugreifen können.

Das bedeutet, dass selbst wenn jemand dein Kennwort gestohlen hat, er immer noch einen weiteren Faktor überwinden muss, um in dein Konto einzudringen. Dies kann ein persönlicher Code sein oder auch biometrische Informationen wie Fingerabdrücke oder Gesichtserkennung.

Es ist wichtig zu verstehen, dass MFA kein Allheilmittel ist und nicht alle Sicherheitsprobleme lösen kann; es ist jedoch eine wichtige Ergänzung zur allgemeinen Sicherheitsstrategie für jeden Berufszweig und jede Branche. In den kommenden Absätzen werden wir uns genauer mit den verschiedenen Arten von MFA befassen sowie Tipps zur Einrichtung und Verwaltung geben.

Die verschiedenen Arten der Multi-Faktor-Authentifizierung (MFA)

Wenn wir über MFA sprechen, gibt es verschiedene Arten, die man nutzen kann. Die erste Art ist etwas, das du weißt - dein Passwort. Diese Methode allein ist jedoch nicht sicher genug und kann leicht gehackt werden. Deshalb gibt es weitere Methoden wie biometrische Authentifizierung, bei der dein Fingerabdruck oder deine Gesichtserkennung verwendet wird.

Eine andere Methode ist die Verwendung von Sicherheitstoken oder Smartcards, die dir einen eindeutigen Code generieren, den du eingeben musst, um dich zu authentifizieren. Bei der SMS-Authentifizierung erhältst du einen Code per SMS auf dein Telefon geschickt und gibst ihn dann ein.

All diese Methoden können kombiniert werden und ergeben zusammen eine starke MFA-Lösung für den Schutz deiner Daten und Konten vor unbefugtem Zugriff durch Hacker. Es ist wichtig zu wissen, dass jede dieser Methoden ihre eigenen Vor- und Nachteile hat und je nach Anwendungsfall unterschiedlich effektiv sein kann.

Durch das Wissen über die verschiedenen Arten von MFA können wir sicherstellen, dass wir unsere Online-Konten und sensible Daten effektiv schützen.



SMS als zweiter Faktor -- immer noch häufig möglich, aber nicht die beste Lösung

Vorteile der Nutzung von MFA

Hier kommt die Multi-Faktor-Authentifizierung (MFA) ins Spiel: Durch die zusätzliche Sicherheitsebene wird das Risiko von Hackerangriffen erheblich reduziert. Das bedeutet, dass Daten besser gesichert und Zugänge zu Online-Konten nicht durch Fremde genutzt werden können.

Zusammenfassend lässt sich sagen: Die Nutzung von MFA bietet viele Vorteile, nicht nur im Hinblick auf Datenschutz und IT-Sicherheit.

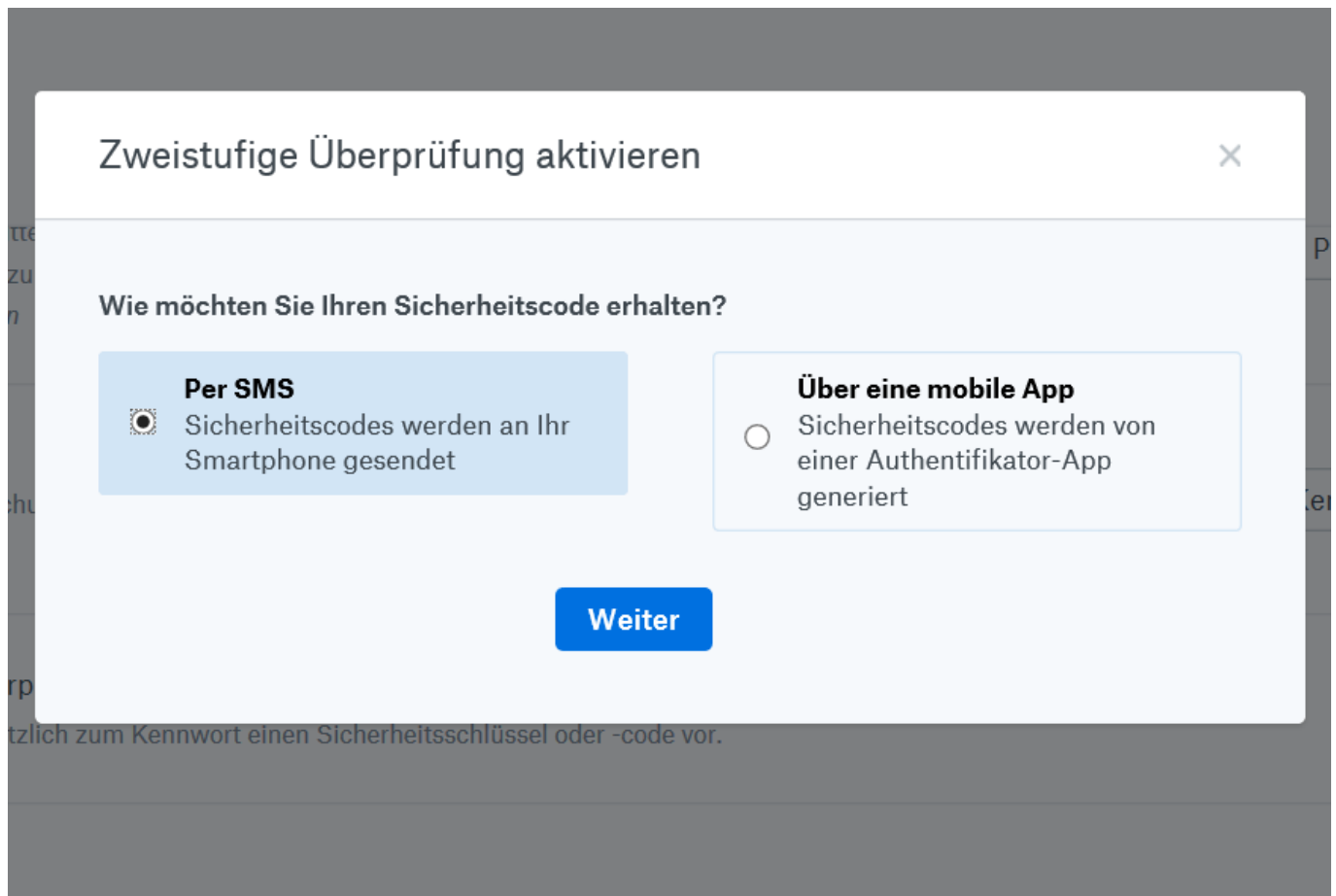


Wie funktioniert die MFA?

Die MFA, auch Multi-Faktor-Authentifizierung genannt, ist ein wichtiger Schutzmechanismus für die Sicherheit von Daten und Zugriffen auf Systeme.

Aber wie funktioniert die MFA eigentlich? Kurz gesagt handelt es sich dabei um ein Verfahren, bei dem mindestens zwei verschiedene Faktoren zur Authentifizierung verwendet werden. Diese können beispielsweise etwas sein, was man weiß (wie Passwörter oder PINs), aber auch etwas, was man besitzt (wie Smartcards oder USB-Token) oder etwas, das man ist (wie Fingerabdrücke oder Iris-Scans).

Die Kombination aus diesen verschiedenen Faktoren erhöht die Sicherheit im Vergleich zu einer einfachen Passwort-Authentifizierung erheblich.



Es gibt zahlreiche bekannte Anwendungen und Plattformen wie Microsoft Azure AD und Google Authenticator, welche die Integration von MFA unterstützen. Die Verwendung dieser Tools kann dazu beitragen, dass vertrauliche Informationen geschützt bleiben und somit ein zusätzliches Maß an Sicherheit gewährleistet wird.

Die Bedeutung und Wirksamkeit der Multi-Faktor-Authentifizierung

Wenn es um die Sicherheit von Daten geht, ist die Multi-Faktor-Authentifizierung (MFA) ein zentraler Bestandteil. In diesem Artikel haben wir gesehen, dass MFA eine äußerst effektive Methode ist, um unbefugte Zugriffe auf wichtige Informationen zu verhindern.

Die Kombination aus zwei oder mehr Faktoren wie Passwort und Biometrie bietet

einen zusätzlichen Schutz für sensible Daten. Besonders in Bereichen wie der Medizin, bei Juristen, Notaren, aber auch im sozialen Bereich und vielen anderen Bereichen, wo der Umgang mit sensiblen Daten zum Alltag gehört, ist MFA unerlässlich.

Verdächtige Verbindungen bei Bitdefender erkennen



Der Schutz eines PCs besteht nicht nur aus dem reinen Virenschutz, sondern auch darin, dass möglicherweise schädliche Verbindungen erkannt und möglichst vor dem erfolgreichen Aufbau blockiert werden. Wie aber damit umgehen?

Die Gefahr von Außen

Ihr könnt Euer Haus noch so gut mit Schlössern, Alarmanlagen und anderen Mechanismen schützen: Wenn jemand von Innen diese deaktiviert und den Einbrechern die Türen öffnet, dann seid ihr nahezu hilflos. Genau so könnt ihr euch Erweiterungen im Browser vorstellen: Einmal installiert erweitert diese den Funktionsumfang. Aber sie machen in vielen Fällen auch einen Weg aus dem Internet auf euren Rechner auf, über den Informationen, im schlimmsten Fall sogar Schadsoftware den Weg auf den Rechner finden. Gute Sicherheitssoftware überwacht auch diese Bedrohungen. [Bitdefender](#) beispielsweise meldet in einem

solchen Fall eine "Verdächtige Verbindung". Das ist erst einmal gut, denn dann ist diese blockiert und es konnte kein Schaden angerichtet werden. Die Ursache ist damit aber weiterhin nicht geklärt, geschweige denn abgestellt.

Alle Kritisch Warnung Informationen

Verdächtige Verbindung blockiert
vor 8 Minuten

Funktion: Online-Gefahrenabwehr

msedge.exe hat versucht, auf Grundlage eines abgelaufenen...
deff.nelreports.net aufzubauen. Wir haben die Verbindung bl...
müssen ihre Zertifikate über eine Zertifizierungsstelle erneuer...
Abgelaufene Sicherheitszertifikate stellen ein Risiko für Ihren...

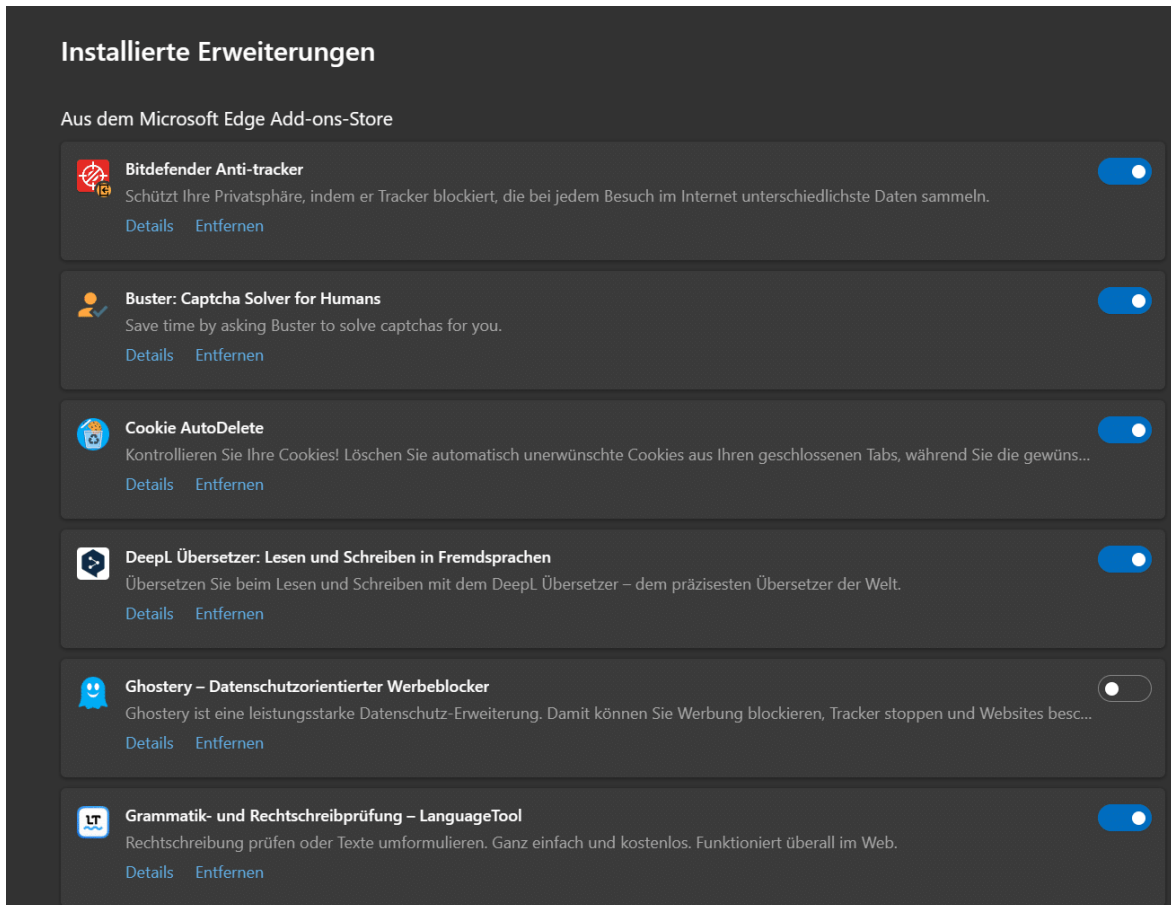
[Zu den Ausnahmen hinzufügen](#)

Erweiterungen kontrollieren

In den meisten Fällen handelt es sich bei der Ursache um eine [Browsererweiterung](#) in Edge (oder eurem jeweiligen Browser), die nicht ordnungsgemäß funktioniert. Wichtig dabei: Es muss sich nicht zwangsweise um eine Malware handeln, aber eine fehlerhafte Funktion öffnet ja gegebenenfalls Tür und Tor für eine echte Sicherheitslücke. Es macht also Sinn, die betroffene Erweiterung zu deinstallieren oder zumindest zu deaktivieren.

- Klickt in [Edge](#) in der Symbolleiste auf das kleine Symbol mit dem Puzzleteil. Dieses öffnet eine Übersicht über die installierten Erweiterungen.
- Da es sich meist um eine größere Zahl handelt, klickt unten auf Erweiterungen verwalten, um die komplette Liste der installierten Erweiterungen zu öffnen.

- Sucht die betroffene Erweiterung heraus. Klickt auf den Schalter rechts von ihrem Namen, um sie zu deaktivieren.
- Wenn ihr sie löschen wollt, dann klickt unter deren Namen und dem Erklärungstext auf **Entfernen**.



Um welche Erweiterung handelt es sich?

Manchmal ist es nicht so eindeutig, welche Erweiterung den Fehler der Sicherheitssoftware verursacht. In einem solchen Fall hilft wie so oft eine Suche im Internet. Gebt den Namen des Prozesses aus der Meldung der Sicherheitssoftware ein und lest euch die Tipps dazu durch. Alternativ könne ihr auch in der Übersicht der installierten Erweiterungen oben das Suchfeld nutzen.

Ab Dezember: Google löscht unbenutzte Konten



Wer sein Google-Konto seit mehr als zwei Jahren nicht mehr aktiv genutzt hat, könnte Zugriff auf sein Konto verlieren: Google startet im Dezember eine große Löschaktion. Offiziell aus Sicherheitsgründen. Über die Hintergründe und was zu beachten ist.

Google bietet zahlreiche Online-Dienste an, für die man immer auch ein Google-Konto braucht oder aus Komfortgründen eins einrichten kann: Google-Suchdienst, Youtube, Google Mail, Android, Google Maps, Google Docs, Google Fotos – und viele andere. Ein Google-Konto reicht, um all die Dienste zu verwenden und zu individualisieren.

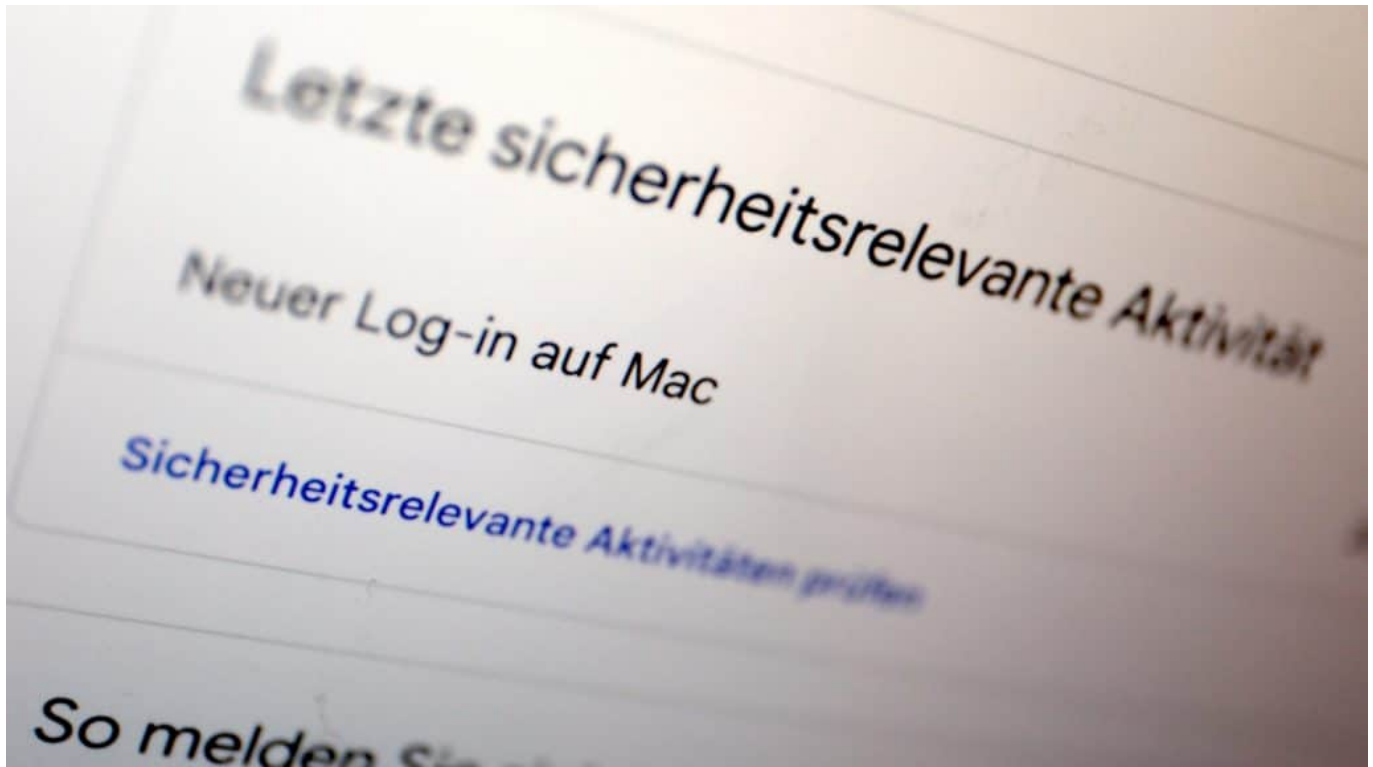


Es gibt Dutzende Google-Dienste, in denen Google-Konten nötig sind

Ungenutzte Konten: Ab Dezember wird gelöscht

Das Unternehmen [hat neue Regeln angekündigt](#), ab Anfang Dezember länger ungenutzte Google-Konten zu löschen. Betroffen sind alle Konten, in die sich seit 24 Monaten niemand mehr eingeloggt hat. Davon ausgenommen sind laut den neuen Nutzungsbedingungen Unternehmenskonten (für die Gebühren anfallen) sowie Konten von Schulen, die mit Google-Diensten arbeiten.

Viele Nutzer sind durch die Ankündigung verunsichert, denn nicht wenige haben im Laufe der Zeit mehrere Konten angelegt und wissen nicht, ob sie möglicherweise betroffen sind. Es lohnt sich, das zu überprüfen, denn niemand möchte die möglicherweise unzähligen Fotos verlieren, die vor langer Zeit mal bei Google Fotos hochgeladen und seitdem nicht mehr abgerufen wurden. Oder Dokumente in Google Docs, die mal archiviert, aber schon länger nicht mehr abgerufen worden sind.



Bei Bedarf den letzten Login überprüfen

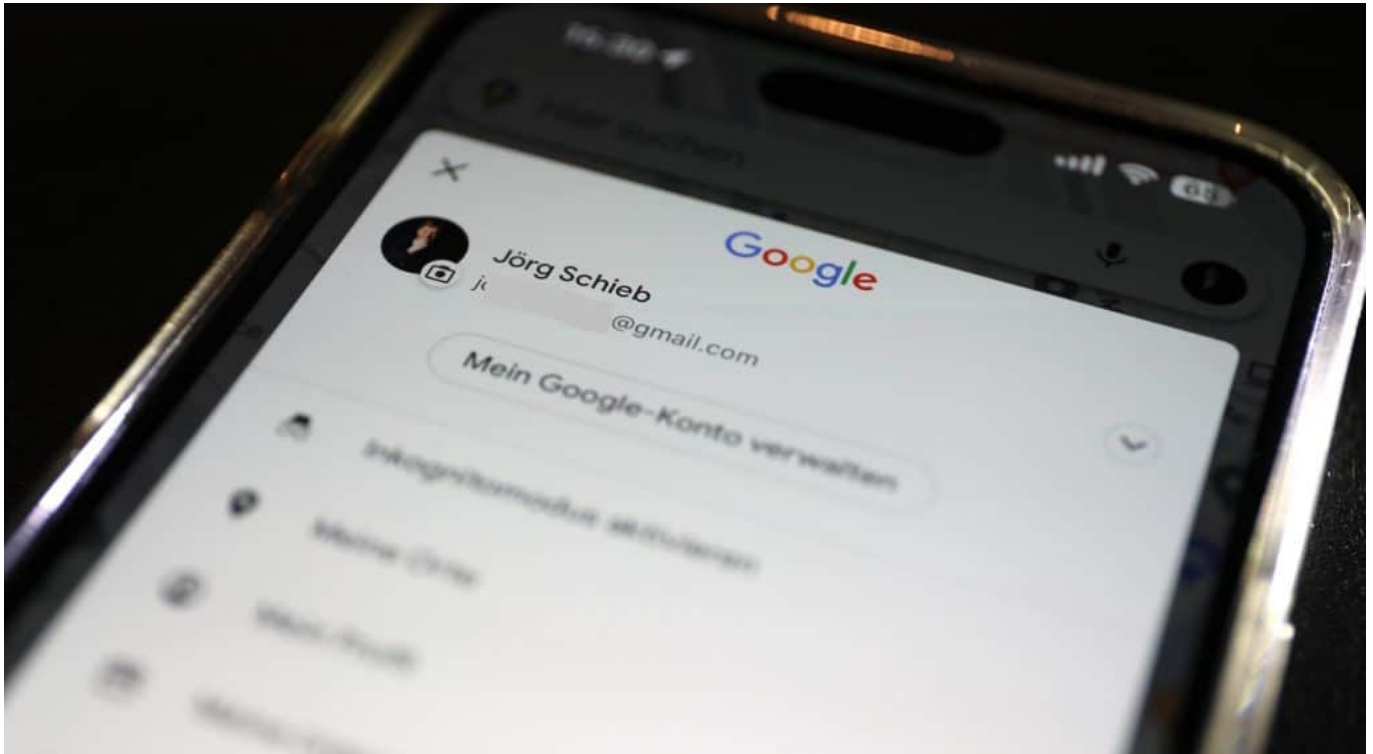
Google warnt betroffene Nutzer rechtzeitig

Wichtig: Falls tatsächlich eine Löschung droht, kündigt Google das mit einer E-Mail rechtzeitig an. Was man allerdings auch nur mitbekommen kann, wenn man die entsprechenden E-Mails abrufen – bei einer selten genutzten Gmail-Adresse ist das möglicherweise nicht der Fall.

Es lohnt sich daher, sich in allen relevanten Google-Konten vor Anfang Dezember einmal aktiv einzuloggen. Oft ist das jedoch gar nicht nötig. Wer zum Beispiel bei Google Maps ein Konto eingerichtet hat, aktiviert bei jedem Start der Anwendung automatisch einen Login.

Dasselbe gilt für eine Suche auf Youtube, wenn man eingeloggt ist – oder die Verwendung eines Mobilgeräts mit Android. Das Laden einer App im Google Play Store reicht ebenfalls schon aus, um ein Konto als aktiv zu kennzeichnen.

Wer seine Google-Konten regelmäßig benutzt, muss sich keine Gedanken machen. Wer vor langer Zeit mal ein Konto eingerichtet hat und es noch braucht, der ist gut beraten, die Zugangsdaten herauszusuchen und sich mal einzuloggen.



Löschaktion soll Sicherheit dienen

Das Unternehmen gibt mehrere Gründe für die Löschaktion und die neuen Nutzungsbedingungen an. Zum einen lassen sich so wertvolle Ressourcen sparen. Denn gespeicherte Dokumente, Fotos oder Videos, die niemand mehr benötigt, binden wertvollen und teuren Speicherplatz. Das zu beenden spart nicht nur Geld, sondern auch Energie.

Der wohl aber wichtigste Grund betrifft die Sicherheit: Viele Betrüger nutzen einmal eingerichtete Google-Konten für Betrug, Phishing, Spam und Hackangriffe. Sie loggen sich aber nie in diese Konten ein. Wenn Google auf diese Weise betrügerisch verwendete Google-Konten deaktivieren kann, ist das gut für die Allgemeinheit.

Dasselbe gilt für von Privatanutzern angelegte Konten, die aber nicht mehr benutzt werden. Oft sind diese schlecht abgesichert: einfaches Passwort und ohne Zwei-Faktor-Authentifizierung. Das wiederum können sich Cyberbetrüger zunutze machen. Sie kapern solche schlecht geschützten Konten und missbrauchen sie für Identitätsdiebstahl oder andere kriminelle Aktivitäten. Auch das soll durch die Löschaktion eingedämmt und verhindert werden.

Google-Suche nicht von Löschaktion betroffen

Wer kein Google-Konto eingerichtet hat und Googles Suchmaschine und andere Dienste wie Youtube ohne Anmeldung nutzt – was problemlos möglich ist –, hat durch die angekündigte Löschaktion keinerlei Nachteile und ist nicht betroffen. Die Dienste lassen sich weiter problemlos verwenden.

Einrichten eines neuen Routers ohne Stress



Ob Defekt, Modellwechsel oder ein anderer Grund, ein neuer Router für den Zugang zum Internet muss irgendwann eingerichtet werden. Ihr habt kein Gerät mit Netzwerkkabel? Kein Problem, das geht auch ohne!

Das leidige Thema Netzwerkkabel

Euer WLAN wollt und müsst ihr einrichten. Im Router. Der aber ja noch nicht per WLAN erreichbar ist, weil das ja nicht konfiguriert ist. Solche oder ähnliche Gedanken gehen den meisten Anwendern durch den Kopf. Und da die meisten Geräte mittlerweile auf einen kabelgebundenen Netzwerkanschluss (LAN, RJ45) verzichten, scheint das schwer lösbar zu sein. Dummerweise sind wenig Dokumentationen in der Verpackung. Und ohne Internetverbindung im Internet danach zu suchen (oder den kleinen Bildschirm des Smartphones zu benutzen) ist keine echte Option. Aber dreht doch mal euren Router um!




Vorkonfiguriertes WLAN

Diese Herausforderung ist den Herstellern natürlich auch nicht fremd. Im Auslieferungszustand bieten die meisten Router ein einfaches WLAN, dessen Zugangsdaten auf dem Typenaufkleber des Routers zu finden sind:

- Der Name des Routers ist meist auch der Name des [WLANs](#), beispielsweise **FritzBox 7590 AX**.
- Der WLAN-Passcode, den ihr bei der Verbindung eingeben müsst, steht als Kombination von Ziffern auf dem Aufkleber.
- Um euch mit der Konfigurationsoberfläche des Routers zu verbinden, gebt bei Fritz!Boxen im Browser **fritz.box** ein, bei anderen Herstellern die IP-Adresse, die auf dem Typenaufkleber steht (beispielsweise 192.168.70.1).
- Das Passwort, das ihr für die Weboberfläche eingeben müsst, findet ihr auch auf dem Typenaufkleber.

WPA-Verschlüsselung

Hier legen Sie fest, wie das WLAN-Funknetz gesichert wird.

WPA-Verschlüsselung (größte Sicherheit) 

WPA-Modus

WPA2 (CCMP) ▼

unverschlüsselt (nicht empfohlen, ungeschützt)

WLAN-Netzwerkschlüssel

Legen Sie einen WLAN-Netzwerkschlüssel fest. Dieser dient als Kennwort, um Netzwerkschlüssel muss mindestens 8, darf aber höchstens 63 Zeichen lang s

Zugangsdaten direkt ändern!

So schön es ist, dass alle benötigten Informationen auf dem [Router](#) stehen, so gefährlich ist das auch: Jeder, der den Router im Zugriff hat, könnte sich damit anmelden und eure [Internetverbindung](#) übernehmen. Aus dem Grund sollte der erste Schritt sein, diese Standardinformationen zu ändern:

- Klickt oben rechts in der Weboberfläche auf die drei Punkte, dann auf **Kennwort ändern**, um das Kennwort zur Weboberfläche selbst zu ändern. Verwendet dazu ein gutes Passwort!
- Unter **Einstellungen > WLAN > Sicherheit** gebt unter WLAN-Netzwerkschlüssel einen neuen WLAN-Schlüssel ein. Den braucht jedes Gerät, um ins WLAN zu kommen.
- Keine Sorge: Die WLAN-Verbindung wird getrennt. Das ist korrekt, denn der Netzwerkschlüssel stimmt ja nicht mehr. Verbindet euch einfach neu mit dem WLAN!

CoPilot in Windows 11 23H2 aktivieren



Microsoft ist mit der Beteiligung an OpenAI ganz weit vorne bei der Integration von Künstlicher Intelligenz (KI) in die eigenen Produkte. Das hat jetzt auch im neuesten Windows 11-Update Auswirkungen.

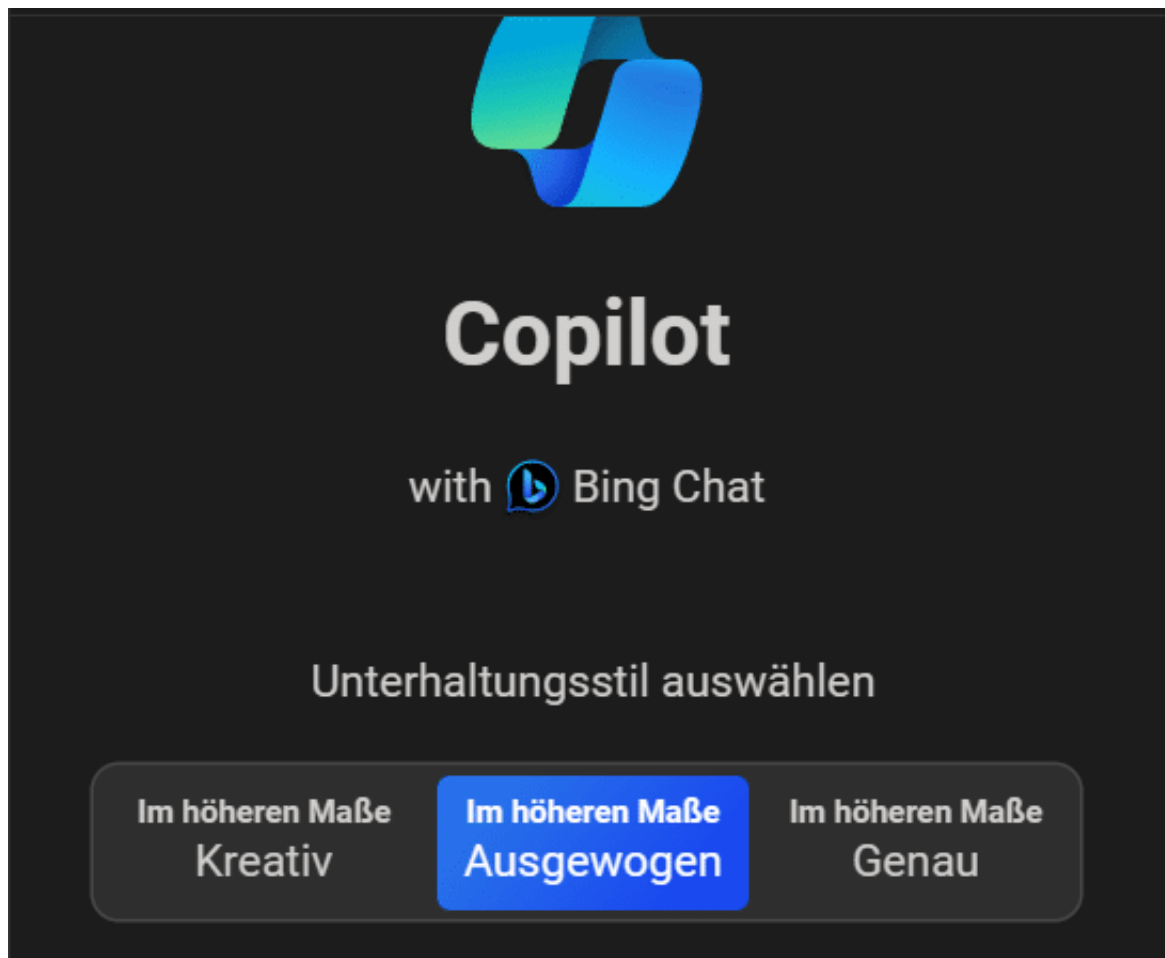
CoPilot - Consumer- und Firmenversion

[KI](#) ist weit mehr als nur ChatGPT, das wisst ihr schon länger, wenn ihr regelmäßig auch [schieb.de](https://www.schieb.de) vorbeischaut. Viele Hersteller integrieren KI in ihre Produkte und bieten damit weit mehr als "nur" einen Chatbot. Bei Microsoft sind die Funktionen unter CoPilot zusammengefasst. Der Name soll andeuten, dass die KI-Funktionen unterstützen sollen bei der Erfüllung der Navigation durch Programme und das Betriebssystem. Hier gilt es aber zu unterscheiden:

[CoPilot](#) wird in den meisten Fällen mit der Integration in die Office-Produkte und Microsoft 365 gleichgesetzt und ist auch für die "normalen" Kunden Anfang November 2023 verfügbar geworden. Allerdings ist ein "normaler Kunde" in dieser Definition ein Microsoft 365-Kunde mit mindestens einem E3-Plan. E steht hier für

Enterprise. Diese Funktionen bekommt der private Endanwender (noch) nicht zur Verfügung gestellt.

Allerdings gibt es mit dem 23H2-Update von Windows 11 eine Vielzahl von KI-Erweiterungen für Windows, die zwar nicht so weitreichend sein mögen, aber in der täglichen Anwendung helfen und einen guten Ausblick geben.



CoPilot in Windows 11 aktivieren

Die Idee von CoPilot in Windows 11 ist die Ablösung der über die Jahre immer weiter reduzierten Funktionalität der hauseigenen Sprachassistentin Cortana. Auch diese konnte schon Fragen beantworten, Dinge auf dem PC suchen und einfache Routinen ausführen. Auch CoPilot soll mit einer Tastenkombination gestartet werden: **Windows + C** ruft in Edge CoPilot auf. Aber noch nicht für alle Benutzer!

In der Startphase des [23H2-Updates](#) hat Microsoft den Zugang limitiert und schaltet diesen nur Stück für Stück frei. Es sei denn, Ihr kennt unseren Hack:

- Drückt auf der Tastatur Windows + R.
- Gebt als auszuführenden Befehl `microsoft-edge://?ux=copilot&tcp=1&source=taskbar` ein.
- Drückt die Eingabetaste, dann kann startet Edge einmal mit der Konfigurationsoberfläche.
- Über **Windows + C** könnt ihr diese dann jederzeit erreichen.

wer ist der liebenswürdigste Charakter in Harry Potter?

- ✓ Suche nach der richtigen Aktion
- ✓ Generieren einer Antwort aus dem Web
- ✓ Suchen nach: **liebenswürdigste Charakter in Harry Potter**
- ✓ Antworten für Sie werden generiert...

Der liebenswürdigste Charakter in Harry Potter ist eine subjektive Frage

1 von 30 •

Power up! Wie du mit nur einem Kabel deine Maus und Tastatur auflädst – ganz ohne Stress



Das kempt jeder: Maus und Tastatur sind fast leer und wir müssen wieder einmal zwei verschiedene Kabel suchen, um sie aufzuladen. Aber wusstest du, dass du mit nur einem Kabel deine Geräte aufladen kannst?

Das ist nicht nur einfach und stressfrei, sondern auch super praktisch. In diesem Blogbeitrag erfährst du, wie du deine Maus und Tastatur mit nur einem Kabel auflädst und so Zeit und Nerven sparst. Außerdem geben wir dir Tipps, wie du auch andere Geräte wie dein Handy oder Tablet schnell und einfach aufladen kannst.

Egal ob du einen Vertrag oder Prepaid hast, mit oder ohne SIM-Karte, online oder direkt vor Ort - Aufladung war noch nie so einfach. Lies weiter und lass dich inspirieren!



Aufladen von Maus und Tastatur - der neue Trend für stressfreies Arbeiten

Hast du auch genug von ständig leeren Batterien in deiner Maus und Tastatur? Dann haben wir eine gute Nachricht für dich: Der neue Trend des kabellosen Aufladens macht es möglich, deine Geräte stressfrei aufzuladen.

Kein lästiges Wechseln der Batterien mehr oder das Anschließen eines Kabels – einfach drahtlos aufladen. In diesem Artikel erfährst du alles über die verschiedenen Möglichkeiten zum Aufladen deiner Geräte sowie Tipps zur optimalen Nutzung und Verlängerung der Akkulaufzeit. Auch die Sicherheit beim kabellosen Aufladen wird thematisiert.

Mit unserer Schritt-für-Schritt-Anleitung kannst du ganz einfach den drahtlosen Ladevorgang einrichten und schon bald ohne lästige Kabel arbeiten.

Wir zeigen dir auch, welche Mäuse und Tastaturen sich kabellos aufladen lassen und wie die Zukunft des Ladens mit Qi-Technologie aussieht. Also lass dich inspirieren und genieße ab sofort das bequeme Aufladen deiner Maus und Tastatur – schnell, einfach und ohne Stress!



Vorteile des kabellosen Aufladens für deine Maus und Tastatur

Kabellose Aufladung für deine Maus und Tastatur kann dein Leben einfacher machen, indem du schnell und einfach aufladen kannst, ohne dich um Kabelsalat oder unordentliche Arbeitsbereiche sorgen zu müssen. Die Möglichkeiten zum kabellosen Aufladen deiner Geräte sind heutzutage vielfältiger denn je, mit der Qi-Technologie als der neuesten Methode zur drahtlosen Aufladung.

Diese Technologie ermöglicht es dir, mehrere Geräte gleichzeitig aufzuladen und eine direkte Verbindung zwischen deinen Geräten herzustellen. Darüber hinaus ist die Einrichtung des kabellosen Ladevorgangs sehr einfach und erfordert nur wenige Schritte.

Es gibt auch Tipps zur optimalen Nutzung deiner kabellos aufgeladenen Geräte sowie Sicherheitshinweise beim kabellosen Aufladen zu beachten. Mit all diesen Vorteilen wird das Arbeiten mit deiner Maus und Tastatur stressfreier sein als je zuvor!

Die verschiedenen Möglichkeiten zum Aufladen deiner

Geräte

Es gibt heute viele verschiedene Möglichkeiten, deine Geräte aufzuladen. Dabei ist es wichtig zu beachten, welche Art von Gerät du hast und welche Art von Lademöglichkeiten zur Verfügung stehen.

Einige der gängigsten Methoden sind das Aufladen über ein Kabel oder drahtloses Laden mit Qi-Technologie. Wenn du ein Samsung Galaxy hast, kannst du dein Handy direkt über die App aufladen und auch dein Online-Guthaben schnell und einfach aufladen.

Wenn du Hilfe benötigst oder Fragen hast, gibt es viele Kontaktmöglichkeiten wie den Kundenservice oder Hilfeforen im Internet. Bei Prepaid-Karten ist es wichtig zu prüfen, ob sie kompatibel sind und ob ein Code benötigt wird, um das Guthaben aufzuladen.

Bei einem Vertrag hingegen erfolgt die Aufladung in der Regel automatisch durch Abbuchung vom Bankkonto oder per Rechnung. Wichtig bei allen Arten der Aufladung ist jedoch immer die Beachtung von Sicherheitshinweisen sowie Tipps zur Verlängerung der Akkulaufzeit deiner Maus und Tastatur für eine optimale Nutzungserfahrung ohne Stress beim Arbeiten.



Mit Qi lassen sich viele Geräte drahtlos aufladen; auch Maus und Tastatur

Kabelloses Laden mit Qi-Technologie – die Zukunft des Ladens

In der Welt der kabellosen Technologie gibt es eine neue Möglichkeit, deine Maus und Tastatur aufzuladen: Qi-Technologie. Diese innovative Methode ermöglicht es dir, deine Geräte ohne Kabel direkt zu laden. Die Zukunft des Ladens ist somit viel einfacher und stressfreier geworden.

Mit dieser Technologie bist du nicht mehr auf ein Kabel angewiesen und kannst deine Geräte schnell und bequem aufladen. Um sicherzustellen, dass dein Gerät mit der Qi-Technologie kompatibel ist, solltest du jedoch vorher prüfen, ob das entsprechende Modell diese Funktion unterstützt.

Wenn dies der Fall ist, kannst du Schritt für Schritt vorgehen und das drahtlose Laden einrichten. Zusätzlich gibt es einige Tipps zur optimalen Nutzung deiner

kabellos aufgeladenen Geräte sowie Sicherheitshinweise beim Aufladen zu beachten.

Insgesamt bietet die Qi-Technologie eine großartige Möglichkeit für alle Nutzer von Maus und Tastatur, um ihr Arbeitsleben stressfrei zu gestalten.



Kompatibilität prüfen: Welche Mäuse und Tastaturen lassen sich kabellos aufladen?

Wenn du dich für das kabellose Aufladen deiner Maus und Tastatur entscheidest, ist es wichtig zu wissen, ob deine Geräte dafür überhaupt kompatibel sind. Glücklicherweise gibt es mittlerweile viele Mäuse und Tastaturen auf dem Markt, die sich drahtlos aufladen lassen.

Einige der bekanntesten Marken wie Logitech und Microsoft bieten bereits Modelle mit Qi-Technologie an. Auch Apple hat mit der Magic Mouse 2 und dem Magic Keyboard eine drahtlose Ladefunktion integriert.

Wenn du dir unsicher bist, ob deine Geräte für das kabellose Aufladen geeignet sind, kannst du in der Bedienungsanleitung nachschauen oder direkt beim Hersteller nachfragen. Es lohnt sich auf jeden Fall, diese Möglichkeit des

Aufladens zu prüfen – denn es ist nicht nur bequem und einfach, sondern auch schnell und sicher.

Mit einem kompatiblen Ladepad oder einer Ladestation kannst du deine Maus und Tastatur jederzeit aufladen, ohne dass ein Kabel im Weg ist oder Steckdosen in der Nähe sein müssen.

Schritt-für-Schritt-Anleitung zum Einrichten des drahtlosen Ladevorgangs

Im sechsten Schritt unserer Anleitung zeigen wir dir, wie du den drahtlosen Ladevorgang für deine Maus und Tastatur einrichtest. Zunächst solltest du sicherstellen, dass deine Geräte mit der Qi-Technologie kompatibel sind.

Ist dies der Fall, kannst du direkt mit dem Einrichtungsprozess beginnen. Als erstes musst du das Ladekabel an die Stromversorgung anschließen und das andere Ende in die Ladestation deiner Maus oder Tastatur stecken. Danach legst du einfach dein Gerät auf die Ladestation und der Aufladungsvorgang startet automatisch.

Beachte dabei, dass eine direkte Berührung zwischen dem Gerät und der Ladestation notwendig ist. Auch wenn es schnell und einfach ist, kann es sein, dass bei manchen Geräten noch ein Code eingegeben werden muss oder eine App heruntergeladen werden muss, um die Aufladung zu ermöglichen.

Prüfe daher vorab immer die Bedienungsanleitung deiner Maus oder Tastatur oder kontaktiere den Hersteller für Hilfe. Mit dieser Methode des kabellosen Aufladens bist du in Zukunft unabhängig von lästigen Kabeln und kannst dich voll auf deine Arbeit konzentrieren – ganz ohne Stress!

Tipps zur optimalen Nutzung der kabellos aufgeladenen Geräte

Nachdem du deine Maus und Tastatur drahtlos aufgeladen hast, möchtest du sicherstellen, dass du das Beste aus dieser neuen Technologie herausholst. Hier sind einige Tipps zur optimalen Nutzung deiner kabellos aufgeladenen Geräte:

1. Verwende eine Qi-Ladestation

Wenn du ein iPhone oder ein Android-Gerät der Galaxy-Serie besitzt, kannst du es einfach auf einer Qi-Ladestation aufladen. Diese Ladestation ist mit den meisten kabellos aufladbaren Mäusen und Tastaturen kompatibel.

2. Halte die Geräte in Reichweite

Die Reichweite von kabellos geladenen Geräten ist begrenzt. Achte darauf, dass sich deine Maus und Tastatur innerhalb der Reichweite des Ladevorgangs befinden, um eine optimale Aufladung zu gewährleisten.

3. Überprüfe die Akkulaufzeit

Auch wenn kabellose Geräte bequem sind, sollten sie regelmäßig überprüft werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Überwache die Akkulaufzeit deiner Maus und Tastatur regelmäßig und lade sie bei Bedarf auf.

4. Beachte die Sicherheitshinweise

Wie bei jeder anderen Technologie gibt es auch beim kabellosen Laden Sicherheitsrisiken zu beachten. Vergewissere dich immer, dass sowohl die Ladestation als auch das Gerät sicher verwendet werden.

5. Nutze Apps für schnelleres Aufladen

Es gibt viele Apps auf dem Markt, mit denen du dein Smartphone oder Tablet schneller aufladen kannst als mit einem normalen Ladegerät. Einige dieser Apps funktionieren auch mit kabellosen Ladestationen.

6. Verbinde dich direkt mit dem Internet

Wenn du Probleme beim Aufladen deiner Geräte hast, wende dich direkt an den Hersteller oder besuche ihre Website für Hilfe und Unterstützung. Mit diesen Tipps kannst du sicherstellen, dass du das Beste aus deinen kabellos aufgeladenen Geräten herausholst und stressfrei arbeiten kannst!

Sicherheitshinweise beim kabellosen Aufladen beachten

Beim kabellosen Aufladen deiner Maus und Tastatur gibt es einige wichtige

Sicherheitshinweise zu beachten. Zum einen solltest du nur zertifizierte Ladegeräte verwenden, um sicherzustellen, dass die Geräte ordnungsgemäß geladen werden und nicht beschädigt werden.

Zudem sollte das Ladekabel nicht beschädigt oder abgenutzt sein, da dies zu Kurzschlüssen führen kann. Auch solltest du darauf achten, dass keine Flüssigkeiten in die Ladebuchsen gelangen können, um Schäden durch Kurzschlüsse oder Korrosion zu vermeiden.

Weiterhin ist es wichtig, das kabellose Laden während Gewittern oder in der Nähe von Wasserquellen zu vermeiden. Hier besteht ein erhöhtes Risiko für Stromschläge oder Kurzschlüsse.

Auch solltest du deine aufgeladenen Geräte nicht unbeaufsichtigt lassen und sie aus der Reichweite von Kindern halten. Wenn du diese Sicherheitsmaßnahmen beachtest, kannst du dein Arbeitsumfeld sicher gestalten und das stressfreie Aufladen deiner Maus und Tastatur genießen.



Tipps zur Verlängerung der Akkulaufzeit vo Maus und Tastatur

Wenn du deine Maus und Tastatur kabellos auflädst, hast du viele Vorteile

gegenüber dem herkömmlichen Aufladen mit Kabeln. Es ist nicht nur bequemer und stressfreier, sondern auch einfacher und schneller. Trotzdem solltest du einige Tipps beachten, um die Akkulaufzeit deiner Geräte zu verlängern.

Zum Beispiel solltest du darauf achten, dass dein Computer oder Laptop immer auf dem neuesten Stand ist und alle Updates installiert sind. Dadurch kann der Energieverbrauch optimiert werden. Auch das Ausschalten von Hintergrundprogrammen und -prozessen kann helfen, den Akku zu schonen.

Eine weitere Möglichkeit ist die Reduzierung der Helligkeit deines Bildschirms oder die Verwendung eines Energiesparmodus für deine Maus und Tastatur. So kannst du sicherstellen, dass deine Geräte so lange wie möglich durchhalten, bevor sie wieder aufgeladen werden müssen.

Stressfrei arbeiten dank dem bequemen Aufladen von Maus und Tastatur

Nachdem du nun alle Schritte durchgeführt hast und deine Maus und Tastatur drahtlos aufladen kannst, wirst du merken, wie viel einfacher und stressfreier dein Arbeitsalltag wird. Du musst nicht mehr ständig auf das Aufladen deiner Geräte achten oder dir Gedanken machen, ob du genug Ladekabel dabei hast. Mit der kabellosen Aufladung bist du jederzeit flexibel und unabhängig.

Auch wenn es momentan noch verschiedene Möglichkeiten gibt, um deine Geräte drahtlos aufzuladen, ist die Zukunft eindeutig: Qi-Technologie wird sich immer weiter durchsetzen und bald zum Standard werden. Es lohnt sich also, bereits jetzt in diese Technologie zu investieren, um auch in Zukunft stressfrei arbeiten zu können.

Beachte jedoch immer die Kompatibilität deiner Geräte und folge den Sicherheitshinweisen beim kabellosen Aufladen. Mit diesen Tipps zur Verlängerung der Akkulaufzeit deiner Maus und Tastatur sowie einer optimalen Nutzung kabellos aufgeladener Geräte steht einem effektiven Arbeitsalltag nichts mehr im Weg – einfach direkt loslegen!