

# 28. Cybercrime Newsletter

03.06.2022

## 1) Verkehrszuschuss der Deutschen Bahn? – Vorsicht vor diesem neuen WhatsApp-Kettenbrief

**Ein bei WhatsApp geteiltes Gewinnspiel verspricht einen angeblichen staatlichen Verkehrszuschuss in Höhe von 2.000 Euro. Vorsicht! Hinter dem Kettenbrief stecken Betrüger.**

Auf dem Chat-Dienst WhatsApp ist derzeit ein Kettenbrief in Umlauf, in dem ein angebliches Gewinnspiel der Deutschen Bahn geteilt wird. [Das berichtet das Verbraucherportal Biallo](#). Teilnehmer können angeblich einen staatlichen Verkehrszuschuss in Höhe von 2.000 [Euro](#) gewinnen. Aber: Weder die Bahn noch der Staat haben etwas mit dem gefährlichen Kettenbrief zu tun.

Was sollten Sie nicht machen? Auf den Link in der Nachricht klicken. Denn dann öffnet sich eine externe Website, die wie eine offizielle Seite der Deutschen Bahn aussieht. Dort sollen Nutzer vier Fragen beantworten und ein Päckchen mit dem Geldpaket finden.

Um den angeblichen Gewinn zu erhalten, soll die Nachricht entweder an fünf WhatsApp-Gruppen oder 20 Freunde geschickt werden. Außerdem sollen Nutzer ihre Adresse eingeben, um sich registrieren zu können.

### **Abofalle oder Banking-Trojaner**

Was passiert mit den eingegebenen Daten? Das ist in diesem Fall nicht ganz klar. Betrüger nutzen solche Adressdaten zum Beispiel, um sie an dubiose Firmen zu verkaufen, die dann mit Post, SMS oder Werbeanrufen nerven. Laut Biallo könnte es sich bei dem angeblichen Gewinnspiel auch um eine sogenannte Abofalle handeln. Dabei nutzen die Betrüger die Kreditkartendaten und Einstimmung der Nutzer aus, um eine monatliche Gebühr im zweistelligen Bereich abzubuchen.

Außerdem ist es möglich, dass das Smartphone beim Klick auf den Gewinnspiel-Link mit gefährlicher Schadsoftware infiziert wird. Dazu gehören auch sogenannte Banking-Trojaner, mit denen Kriminelle persönliche Bankdaten und Kreditkarteninformationen stehlen können.

**Unsere Tipps:** Klicken Sie nicht auf die Links in den Kettenbriefen. Sollten Sie es aus Versehen doch getan haben, dann beantworten Sie nicht die Fragen auf der Webseite und teilen Sie die Nachricht nicht mit Ihren WhatsApp-Kontakten. Und informieren Sie den Nutzer, von dem Sie den Kettenbrief erhalten haben, über den gefährlichen Inhalt und löschen Sie diesen im Anschluss.

Quelle: [https://www.t-online.de/digital/internet-sicherheit/sicherheit/id\\_100010496/whatsapp-kettenbrief-betrueger-locken-mit-verkehrszuschuss-fuers-9-euro-ticket.html](https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100010496/whatsapp-kettenbrief-betrueger-locken-mit-verkehrszuschuss-fuers-9-euro-ticket.html)

## 2) Phishing – Sparkasse warnt vor betrügerischen SMS

**Sparkassen-Kunden aufgepasst: Die Sparkasse warnt eindringlich vor einer neuen Phishing-Masche. Bei dieser versuchen Kriminelle mit betrügerischen Kurznachrichten, an die Finanzdaten ihrer Opfer zu gelangen.**

Cyberkriminelle versuchen immer wieder, an persönliche Daten zu gelangen. Sei es durch betrügerische E-Mails, mit Schadsoftware verseuchte Webseiten oder trügerische SMS-Nachrichten. So auch in diesem Fall, wie die [Sparkasse](#) offiziell auf dem Kurznachrichtendienst [Twitter](#) mitteilt.

Denn aktuell verbreiten Betrüger im Namen der Sparkasse gefälschte SMS, in denen sie die Nutzer dazu auffordern, auf ein neues TAN-Sicherheitsverfahren umzusteigen. In der Nachricht findet sich auch ein weiterführender Link, den Betroffene klicken sollen, um den entsprechenden Push-Tan-Dienst einzurichten.

Die Sparkasse stellt aber zweifelsfrei klar: Unter keinen Umständen auf den Link klicken und persönliche Daten eingeben. Hierbei handelt es sich um einen kriminellen Phishingversuch, bei dem Personendaten abgegriffen werden sollen.

### **So können Sie sich und Ihre Daten schützen**

Prinzipiell kann jeder Opfer eines Phishingversuchs werden. **Wichtig dabei ist immer:** Klicken Sie auf keine unbekanntem Links, schon gar nicht aus anonymer Quelle oder von unbekanntem Absendern. Dadurch vermeiden Sie bereits die größte Gefahrenquelle. Doch wie geht man am besten vor, wenn man eine dubiose Kurznachricht auf dem eigenen Handy vorfindet?

### **Falls Sie eine Phishing-SMS erhalten haben:**

- Klicken Sie auf keinen Fall auf den Link.
- Sollte Ihnen der Absender der Nachricht bekannt sein, kontaktieren Sie diesen und fragen nach, ob die Nachricht bewusst verschickt wurde.
- Sollten Sie den Absender nicht kennen, blockieren Sie diesen in Ihrem Kontaktbuch und löschen anschließend die vorliegende SMS.
- Für Android-Nutzer: Deaktivieren Sie den Download von Apps aus unbekanntem Quellen in den Einstellungen.
- Aktualisieren Sie Ihr Smartphone stets auf die aktuelle Betriebssoftware.

Ist man sich der Gefahr nicht direkt bewusst oder klickt versehentlich auf den Link, lassen sich immer noch ein paar Schritte im Nachhinein ergreifen, die man auf jeden Fall befolgen sollte, um den potenziellen Schaden zu minimieren.

### **Falls Sie eine Phishing-SMS erhalten und den Link bereits geklickt haben:**

- Trennen Sie das Mobiltelefon vom Netz, zum Beispiel durch Aktivierung des Flugmodus.
- Informieren Sie Ihren Mobilfunkprovider über die vorliegende Phishing-Gefahr hinsichtlich Ihrer persönlicher Daten.
- Prüfen Sie Ihr Bankkonto oder sonstige Zahlungsdienstleister auf unautorisierte Abbuchungen. Informieren Sie Ihre Bank über mögliche Fremdzugriffe.
- Erstellen Sie Anzeige bei einer örtlichen Polizeidienststelle. Hierfür ist es wichtig, dass Sie die Phishing-SMS nicht gelöscht haben und dort Ihr Smartphone zur Beweissicherung vorlegen.
- Setzen Sie Ihr Smartphone auf die Werkseinstellungen zurück, nachdem Sie Anzeige erstattet haben. Wichtige persönliche Daten wie Fotos, Dokumente oder Kontakte sollten vorher auf dem Computer oder in der Cloud gesichert werden. Das Zurücksetzen befreit Ihr Smartphone von jeglicher Schadsoftware, aber auch von allen anderen direkt

auf dem Handy gespeicherten Daten.

Quelle: [https://www.t-online.de/digital/internet-sicherheit/sicherheit/id\\_100010426/vorsicht-vor-phishing-sparkasse-warnt-vor-betruegerischen-nachrichten.html](https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100010426/vorsicht-vor-phishing-sparkasse-warnt-vor-betruegerischen-nachrichten.html)

### 3) Kartenstörung: Wer ist eigentlich schuld? Bafin untersucht

**Die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) untersucht die aktuellen Probleme mit der Kartenzahlung in Deutschland.**

**Update 31.5.:** Die massiven Probleme mit der Kartenzahlung (via Giro-/EC-Karte oder Kreditkarte) bei vielen Discountern und Ladengeschäften in Deutschland haben dazu geführt, dass die [Bundesanstalt für Finanzdienstleistungsaufsicht](#) (Bafin) die Störung untersucht. Das [berichtet](#) das Handelsblatt.

Dabei gehe es auch um die Frage, ob für den Ausfall nur der Kartenlesegeräte-Hersteller Verifone verantwortlich sei oder auch die Zahlungsdienstleister Concardis und Payone sowie die Banken eine Mitschuld tragen. "Die Ursache der Störung kann erst nach genauerer Analyse betrachtet werden", zitiert das Handelsblatt einen Bafin-Sprecher. Die Bundesbank wiederum wolle diese Panne "grundlegend aufarbeiten".

Zur Aufgabenteilung: Die in den Läden verwendeten ausgefallenen Geräte und auch die Software darauf stammen von dem US-Unternehmen Verifone. Die Netzbetreiber Concardis und Payone übernehmen aber die Zahlungsabwicklung.

Laut dem Forschungsinstitut des Handels (EHI) sollen bundesweit 90.000 bis 100.000 solcher Kartenterminals im Einsatz sein.

**Update Ende. Die Entwicklung sei 30.5.2022**

[Laut der Augsburger Allgemeinen Zeitung](#) soll bei Aldi Nord und Netto das Bezahlen mit Karte wieder möglich sein. Aldi Nord habe die betroffenen Geräte durch neue ersetzt. Dieser Umtausch sei laut Aldi Nord ohnehin geplant gewesen und sei nun vorgezogen worden. Aber freuen Sie sich nicht zu früh: In einigen Aldi-Nord-Filialen könne es trotzdem immer noch Probleme geben, weil der Austauschvorgang noch laufen würde. Am Eingang der Filialen stehe ein entsprechender Hinweis.

Am 30. Mai morgens hatte es noch geheißsen, dass die Störung bei der Kartenzahlung an Geräten vom Typ Verifone H5000 andauern würde. Zwar soll Verifone [laut Medienberichten](#) eine Software-Lösung bereitgestellt haben. Doch diese an die betroffenen Terminals auszuliefern, würde noch einige Tage dauern, weil an jedem Gerät ein manueller Eingriff erforderlich wäre. Das könne entweder der betroffene Händler oder aber ein Techniker machen. Die betroffenen Geräte müssten aber nicht ausgetauscht werden.

Zudem soll entgegen ersten Berichten (siehe unten) nun doch kein Problem mit einem abgelaufenen Zertifikat vorliegen. Ein Hackerangriff werde von Hersteller Verifone als Grund für die Störung ebenfalls ausgeschlossen. Verifone schreibt [hier](#) folgendes:

*" Sehr geehrte Kunden und Partner, wir sind uns bewusst, dass es bei einem bestimmten Anteil der Verifone H5000 Terminals, die hauptsächlich in Deutschland eingesetzt werden, ein Problem mit der Nutzbarkeit für die Abwicklung von Kartenzahlungen gibt und durch diese Situation Unannehmlichkeiten entstanden sein könnten. Wir möchten betonen, dass das Problem nicht mit dem Ablauf eines Zertifikats oder einer Sicherheitslücke zusammenhängt und keine Sicherheitsbedrohung darstellt. Vielmehr handelt es sich um eine Software-Fehlfunktion in der H5000-Software. Die H5000 Terminal-Serie wird von Verifone seit Ende 2019 nicht verkauft und ausgeliefert, alle anderen verfügbaren und zukünftigen Verifone-*

*Terminalprodukte sind nicht betroffen. Eines der beobachteten H5000 Fehlerbilder ist, dass das Terminal „Betriebsbereit“ anzeigt, aber kontaktbehaftete Kreditkarten- und girocard-Transaktionen nicht verarbeitet werden. Die Verarbeitung von bestimmten kontaktlos-Transaktionen und Lastschrift-Transaktionen hingegen ist noch möglich. Es könnte daher nützlich sein, das Lastschriftverfahren temporär über den Netzbetrieb aktivieren zu lassen. Wir haben in den vergangenen Tagen mit höchster Priorität und unter intensiver Kooperation mit unseren Kunden und Partnern an der Behebung des Problems gearbeitet. Wir haben eine Update Lösung zur Behebung des Problems entwickelt. " Zitat Ende*

Geldautomaten sind von der Störung nicht betroffen.

## Hintergrund

Seit Dienstag (24.5.2022) kann bei einigen Discountern und Drogerieketten nicht per Giro- oder Kreditkarte bezahlt werden. Betroffen sind zum Beispiel Aldi Nord, Edeka und Rossmann; [aber zum Beispiel auch das Panzermuseum Munster](#). Diese Probleme bestehen auch heute noch.

## Das ist der Grund

Die Bezahlprobleme treten immer dann auf, wenn als Kartenzahlungsterminal das Modell H5000 des US-Herstellers Verifone verwendet wird. Laut [Spiegel Online](#) ist ein Zertifikatsfehler innerhalb bestimmter Versionen der von Verifone bereitgestellten Software der Grund für die Störung. Um dieses Problem zu lösen, müsse ein Software-Update aufgespielt werden, wie Hersteller Verifone [mitteilt](#). Hierzu sei aber ein manueller Eingriff an den Terminals erforderlich. Das würde einige Zeit benötigen. Bis das erfolgt sei, fallen die betroffenen Terminals von Verifone komplett für alle Zahlungsarten aus.

## [Geldkarte gestohlen: Das müssen Sie sofort tun!](#)

Solche H5000 Terminals, die noch funktionieren, sollten keinesfalls vom Strom getrennt und nicht ausgeschaltet werden. Die Geräte sollten auch nicht neu gestartet und die Netzwerkverbindung muss aufrechterhalten werden.

Der Finanzdienstleisters Concardis versucht das Problem zumindest teilweise dadurch zu entschärfen, dass er die Kartenzahlungsterminals austauscht.

Die Verifone H5000 Terminals werden hauptsächlich in Deutschland eingesetzt. [Laut Tagesschau](#) mache der entsprechende Typ jedoch nur einen geringen Anteil an allen in Deutschland eingesetzten Geräten aus.

## Das sollten Kunden wissen

Wichtig für Kunden, die an der Kasse nicht mit ihrer Giro- oder Kreditkarte bezahlen können: Ihre Karte ist in Ordnung und muss nicht ersetzt werden. Auch die POS-Netzbetreiber sind nicht für die Störung verantwortlich, wie der Bundesverband der electronic cash-Netzbetreiber [betont](#). Die Ursache für die Störung beim bargeldlosen Bezahlen liegt ausschließlich bei den Terminals von Verifone.

Aldi Süd, [Lidl](#) und die Rewe-Gruppe (Rewe, Penny, Toom Baumarkt) sollen von dem Problem nicht betroffen sein, wie der WDR [berichtet](#).

Quelle: [https://www.pcwelt.de/news/Kartenstoerung-Wer-ist-eigentlich-schuld-Bafin-untersucht-11239777.html?utm\\_source=best-of-pc-welt-manuell&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689557&pm\\_cat=%5B0%5D=Mobilfunk&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Kartenstoerung-Wer-ist-eigentlich-schuld-Bafin-untersucht-11239777.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3689557&pm_cat=%5B0%5D=Mobilfunk&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 4) DuckDuckGo-Browser enttäuscht Nutzer: Darum ist er nicht so anonym wie versprochen

**DuckDuckGo sieht sich als anonyme Alternative zu Google. Doch der hauseigene Browser macht für Microsoft-Tracking eine Ausnahme, was viele Nutzer schockiert. Wir erklären, was es damit auf sich hat.**

Google ist die Nummer 1 bei den Suchmaschinen, für viele geht es im Alltag gar nicht mehr ohne. Doch der Konzern dahinter steht wegen der Datensammelwut öfter mal in der Kritik.

Die Suchmaschine [DuckDuckGo](#), die es schon seit 2008 gibt, wollte dazu immer die anonyme Alternative sein und gar keine persönlichen Informationen über Nutzer abfragen.

Ein Sicherheitsexperte hat genauer hingeschaut und herausgefunden: Das stimmt so leider nicht ganz - zumindest was den Browser von DuckDuckGo betrifft.

### Microsoft-Tracking in DuckDuckGo? Was das für Sie bedeutet

Der Sicherheitsforscher Zach Edwards zeigte auf, dass DuckDuckGo für [Android](#) und [iOS](#) eben nicht komplett frei von Tracking seien. In dem mobilen Browser sind manche Tracker – etwa von Bing und LinkedIn, die zu Microsoft gehören – auf einer Whitelist und werden somit zugelassen.

Durch Bing wird der Suchindex zur Verfügung gestellt, den DuckDuckGo nutzt. Wie der Chef Gabriel Weinberg zugibt, seien die Verträge von Microsoft schlicht so streng aufgesetzt, dass deren Tracker nicht blockiert werden dürfen. Das betrifft allerdings nur die Apps, nicht die Suchmaschine, die Sie einfach im Browser aufrufen können.

Zwar verknüpft DuckDuckGo laut eigenen Angaben keine persönlichen Identifikationsmerkmale mit Ihren Suchanfragen, doch es kann eben sein, dass die [ausgespielte Microsoft-Werbung](#) Ihre IP-Adresse oder den User Agent trackt.

Allerdings beteuert DuckDuckGo, dass dabei kein Profil über Ihr Klickverhalten auf diesen Werbeanzeigen angelegt wird und dass diese Informationen nur zu buchhalterischen Zwecken gespeichert werden.

Man wolle in Zukunft mehr dafür tun, mit Microsoft verwandte Third-Party-Tracker zu blocken, so Gabriel Weinberg.

### Vertrauen verspielt? Die Alternativen zu DuckDuckGo

Microsoft sitzt bei den Verträgen schlicht am längeren Hebel und hat somit die eigenen Tracker erlauben können. Aus Sicht von CHIP können Sie DuckDuckGo durchaus weiter nutzen, sobald die Whitelist entsprechend angepasst wurde und ohne Werbetracker aus Redmond auskommt.

Falls Sie kein Vertrauen mehr in den Suchdienst haben, müssen Sie sich nicht ärgern. Zum Glück gibt es noch andere anonyme Suchmaschinen, die ebenfalls kostenlos sind:

- [Swisscows](#): Schweizer Suchmaschine mit eigenem Suchindex und kompletter Anonymität – auch für das Smartphone erhältlich.
- [Startpage](#): Suchen ohne Tracking, aber mit denselben Suchergebnissen wie bei Google – leider keine Apps zum Download verfügbar.

Probieren Sie diese einfach mal aus und schauen Sie, ob Sie im Alltag alle Antworten auf Ihre Fragen genau so schnell finden.

Quelle: [https://www.chip.de/news/DuckDuckGo-Browser-enttaeuscht-Nutzer-Darum-ist-er-nicht-so-anonym-wie-versprochen\\_184274214.html?utm\\_source=nl\\_chipd-dy&utm\\_medium=chip-newsletter&utm\\_campaign=30-05-2022%2B17%253A00%253A09&utm\\_content=nl\\_chipmob&utm\\_term=](https://www.chip.de/news/DuckDuckGo-Browser-enttaeuscht-Nutzer-Darum-ist-er-nicht-so-anonym-wie-versprochen_184274214.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=30-05-2022%2B17%253A00%253A09&utm_content=nl_chipmob&utm_term=)

## 5) Corona-Warn-App 2.23 verfügbar: Wichtige Neuerung an Bord

**Die Corona-Warn-App 2.23 ist erschienen und bringt eine Funktion, die jetzt für viele Nutzer wichtig ist. Die Details.**

Die Verantwortlichen der Corona-Warn-App (CWA) haben [wie angekündigt](#) ein [Update für ihre App veröffentlicht](#), mit dem Sie technisch abgelaufene Genesenen- und Impfungszertifikate leicht erneuern lassen können. Dieses Update trägt die Versionsnummer 2.23.

**Hintergrund:** Die technische Gültigkeit von Impf- und Genesenenzertifikaten ist – unabhängig von der fachlichen Gültigkeit – auf 365 Tage begrenzt, wie die CWA-Macher erläutern. Deshalb erhalten jetzt ersten CWA-Nutzer den Hinweis, dass sie ihr Zertifikat erneuern sollen. Mit Version 2.23 können sie das direkt über die CWA machen.

### So erneuern Sie das Zertifikat

Die CWA informiert die Nutzerinnen und Nutzer vor Ablauf von Genesenen- und Impfungszertifikaten automatisch. Sie haben dann bis zu 90 Tage nach Ablauf der technischen Gültigkeit Zeit, das Zertifikat zu erneuern. Hierzu tippen Sie im Zertifikatsbereich der App auf den Hinweis "Zertifikat erneuern". Geben Sie dann Ihr Einverständnis – und schon ersetzt die App das Zertifikat automatisch. Das technisch abgelaufene Zertifikat verschiebt die App in den Papierkorb.

**Hinweise der CWA-Macher:** Genesenenzertifikate können immer technisch erneuert werden, wenn diese drohen abzulaufen. Bei Impfungszertifikaten müssen Nutzer nur das aktuell verwendete Zertifikat verlängern, da es ausreichend Informationen über den Impfschutz enthält. Bei Nutzern, die drei Impfungszertifikate in der CWA hinterlegt haben, wird als das Impfungszertifikat der Erst- und Zweitimpfung nicht ausgetauscht, sondern nur das Impfungszertifikat der Auffrischimpfung, sobald es droht abzulaufen.

Testzertifikate werden nicht erneuert, da sie fachlich ohnehin nicht so lange gültig sind.

**Wichtig:** Ein technisch abgelaufenes Zertifikat kann nur drei Mal erneuert werden. Sollten Nutzer ihr Zertifikat also auf mehreren Geräten in der CWA hinterlegt haben, können sie es nur auf drei Geräten erneuern. Sie haben allerdings die Möglichkeit, das neu ausgestellte Zertifikat als PDF-Datei zu exportieren, sodass Sie bei Bedarf den QR-Code des Zertifikats erneut einscannen können. [Mehr dazu lesen Sie hier.](#)

### So bekommen Sie das Update

Die Corona-Warn-App 2.23 wird schrittweise über 48 Stunden an alle Nutzer ausgerollt. iOS-Nutzer können sich die aktuelle App-Version ab sofort aus dem Store von [Apple](#) manuell herunterladen. Der [Google](#) Play Store bietet keine Möglichkeit, ein manuelles Update anzustoßen. Hier steht Nutzern die neue Version der Corona-Warn-App innerhalb der nächsten 48 Stunden zur Verfügung.

Quelle: [https://www.pcwelt.de/news/Corona-Warn-App-2.23-verfuegbar-Wichtige-Neuerung-an-Bord-11242212.html?utm\\_source=best-of-pc-welt-manuell&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689643&pm\\_cat=%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Corona-Warn-App-2.23-verfuegbar-Wichtige-Neuerung-an-Bord-11242212.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3689643&pm_cat=%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 6) Fieser Trick: So stehlen Hacker Whatsapp-Konten und so schützen Sie sich

**Hacker können fremde Whatsapp-Konten stehlen. Dafür ist ein Telefonanruf und eine bestimmte Technik nötig. So schützen Sie sich.**

Mit einem fiesem Trick können Hacker ein fremdes Whatsapp-Konto übernehmen und Zugriff auf dessen persönliche Nachrichten und Kontaktlisten bekommen. Das [berichtet](#) die US-IT-Sicherheitsnachrichtenseite Bleeping Computer unter Berufung auf einen [entsprechenden Beitrag von Rahul Sasi, CEO von CloudSEK, auf LinkedIn](#). Der Angreifer benötigt dafür nur wenige Minuten. Der Angreifer muss aber die Telefonnummer des Opfers kennen und zudem einige Social-Engineering-Tricks beherrschen.

### **Angreifer muss sein Opfer am Telefon überzeugen**

Denn der Angreifer muss das Opfer anrufen und mit seinem Anruf dazu bringen, eine Telefonnummer anzurufen, die mit einem sogenannten "Man Machine Interface Code" (MMI) beginnt. Diese Technik nutzen Mobilfunkprovider eigentlich für das Weiterleiten von Anrufen, wenn der Anschluss besetzt oder nicht erreichbar ist. Je nach Mobilfunknetzbetreiber kann ein MMI-Code aber auch alle Anrufe an ein Endgerät an eine andere Nummer weiterleiten. Derartige Codes beginnen immer mit "\*" oder mit "#" – beispielsweise \*\*67\* – und sind zehnstellig.

Der Sicherheitsforscher [erklärt](#), dass die 10-stellige Nummer, die das Opfer anrufen soll, dem Angreifer gehört und der vorangestellte MMI-Code den Mobilfunkanbieter anweist, alle Anrufe an die danach angegebene Telefonnummer weiterzuleiten. Das Opfer stimmt mit seinem Anruf an diese MMI-Nummer also der Weiterleitung aller seiner Anrufe an eine andere Nummer zu.

Damit kann der Angreifer nun für das Whatsapp-Konto die Registrierung und Verifizierung auf seinem eigenen Gerät starten. Inklusive Verifizierungscode, der dank MMI-Weiterleitung ja nun an das Handy des Hackers geschickt wird. Und schon ist das Whatsapp-Konto gekapert inklusive der Möglichkeit, dass der Hacker nun die 2-Faktor-Authentifizierung dafür einrichtet. Das bedeutet: Der eigentliche Besitzer des Whatsappkontos ist von seinem eigenen Whatsapp-Konto ausgesperrt.

### **Diese Hürden muss der Angreifer nehmen**

Bleeping Computer konnte diese Angriffsmethode zumindest bei den Providern Verizon und [Vodafone](#) nachstellen. Allerdings gibt es durchaus einige Hürden für die Angreifer. So muss der Mobilfunkprovider idealerweise MMI-Code verwenden, der alle Anrufe in allen Fällen weiterleitet und nicht nur in solchen Fällen, wenn das Telefon besetzt ist. Andernfalls müsste es der Angreifer schaffen, sein Opfer so lange am Telefon zu halten, bis der Whatsapp-Authentifizierungscode geschickt wurde und - da das Handy des Opfers ja durch den Anruf mit dem Hacker besetzt ist - dank MMI an das Handy des Hackers weitergeleitet wurde.

Zudem erhält der Besitzer des Whatsapp-Kontos Textnachrichten, die ihn darüber informieren, dass sein Whatsapp-Konto auf einem anderen Gerät registriert worden ist. Obendrein wird bei aktivierter Anrufweiterleitung ein diesbezüglicher Hinweis auf dem Smartphone des Opfers angezeigt.

### **So schützen Sie sich**

Es gibt aber einen einfachen Schutz gegen diese Angriffsmethode: Richten Sie für Whatsapp die Zwei-Faktor-Authentifizierung ein! Dann hat der Angreifer keine Chance.

Quelle: [https://www.pcwelt.de/news/Fieser-Trick-So-stehlen-Hacker-Whatsapp-Konten-und-so-schuetzen-Sie-sich-11241760.html?utm\\_source=security-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689624&pm\\_cat%5B0%5D=Mobifunk&pm\\_cat%5B1%5D=Apps&pm\\_cat%5B2%5D=Mobile+Security&pm\\_cat%5B3%5D=BYOD&pm\\_cat%5B4%5D=Cyberkriminalit%C3%A4t&pm\\_cat%5B5%5D=Security+allgemein&pm\\_cat%5B6%5D=Mobile+Device+Management&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Fieser-Trick-So-stehlen-Hacker-Whatsapp-Konten-und-so-schuetzen-Sie-sich-11241760.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3689624&pm_cat%5B0%5D=Mobifunk&pm_cat%5B1%5D=Apps&pm_cat%5B2%5D=Mobile+Security&pm_cat%5B3%5D=BYOD&pm_cat%5B4%5D=Cyberkriminalit%C3%A4t&pm_cat%5B5%5D=Security+allgemein&pm_cat%5B6%5D=Mobile+Device+Management&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 7) Die 10 gefährlichsten Telefonnummern für Telefonterror, aggressive Werbung etc.

**Das sind die zehn meistgenutzten Telefonnummern für Telefonterror, unerwünschte Werbung und mehr. Laut einer Zusammenstellung von Tellows.**

Das deutsche Unternehmen [Tellows bietet einen Anrufschutz für die Fritzbox an](#) , der vor Spamanrufen schützen sollen. Für sein Tool muss Tellows natürlich ständig neue verdächtige Telefonnummern erfassen. Kürzlich hat Tellows eine Zusammenstellung der zehn verdächtigsten "unerwünschten Rufnummern" [zusammengestellt](#) . Diese unrühmliche Top 10 sieht so aus:

- 015216117165 (tellows Score: 8, Anrufertyp: Telefonterror)
- 091188185811 (tellows Score: 7, Anrufertyp: Meinungsforschung)
- 017650642602 (tellows Score: 8, Anrufertyp: Telefonterror)
- 030439729066 (tellows Score: 8, Anrufertyp: Aggressive Werbung)
- 080380612 (tellows Score: 8, Anrufertyp: Telefonterror)
- 069870012292 (tellows Score: 8, Anrufertyp: Aggressive Werbung)
- 069870012291 (tellows Score: 8, Anrufertyp: Aggressive Werbung)
- 02317257820 (tellows Score: 8, Anrufertyp: Telefonterror)
- 0302514878 (tellows Score: 8, Anrufertyp: Gewinnspiel)
- 0333121503 (tellows Score: 8, Anrufertyp: Gewinnspiel)

Die oben aufgeführten Telefonnummern stammen zwar von April 2022, sie dürften aber auch jetzt noch genutzt werden, weil es sich überwiegend um Nummern handelt, die erst im April 2022 in Betrieb genommen wurden.

Tellows liefert zu jeder Nummer eine Einschätzung wie "Telefonterror" oder "Meinungsforschung" oder "Aggressive Werbung" oder auch "Gewinnspiel", wobei die Grenzen zwischen den einzelnen Kategorien natürlich fließend sind. Besonders die Telefonnummer "015216117165" nervte laut dieser Zusammenstellung, denn allein auf deren Konto gehen 25 Prozent aller Beschwerden über alle Nummern aus der Top 10. Liest man die [detaillierte Beschreibung von Tellows zu dieser Telefonnummer](#), dann erfährt man, dass offensichtlich ein Immobilienmakler "gezielt Rufnummern aus alten Anzeigen zu Immobilienverkäufen" anruft und Interesse an diesen Immobilien bekundet. Die Einschätzung von Tellows: "Einschätzung: sehr unseriös, nicht annehmen."

### **Rückwärtssuche: Fremde Telefonnummer schnell checken**

Sie können [hier bei Tellows rechts oben](#) eine Telefonnummer eingeben und auf deren Seriosität überprüfen lassen. Das sollten Sie bei jeder fremden Telefonnummer machen, bevor Sie diese zurückrufen.

## Anrufschutz von Tellows für die Fritzbox

Sie können mit dem [Tellows Anrufschutz für 19,99 Euro](#) unerwünschte und vielfach sogar betrügerische Anrufe direkt in der Fritzbox blockieren. Wir haben den Tellows Anrufschutz getestet, unseren Testbericht lesen Sie hier: [Tellows Anrufschutz für Fritz Box – Test, Howto & neue Funktionen](#).

[Fritzbox: Sperrliste gegen Spam-Anrufe erstellen](#)

### Tip: So schützen Sie sich vor betrügerischen Anrufen

Sie können nicht nur mit Tellows gefährliche Anrufe identifizieren. Sondern es gibt beispielsweise auch Apps für diesen Zweck. In dem Artikel [Call-ID Spoofing: So schützen Sie sich vor betrügerischen Anrufen](#) stellen wir diverse Schutzmethoden vor. Außerdem gibt es noch weitere Webseiten wie [wer-ruftan.de](#) oder [werruft.info](#), auf denen Sie verdächtige Telefonnummern überprüfen lassen können.

Quelle: [https://www.pcwelt.de/news/Die-10-gefaehrlichsten-Telefonnummern-fuer-Telefonterror-aggressive-Werbung-etc.-11241174.html?utm\\_source=security-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689604&pm\\_cat%5B0%5D=Netzwerk+Hardware&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Die-10-gefaehrlichsten-Telefonnummern-fuer-Telefonterror-aggressive-Werbung-etc.-11241174.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3689604&pm_cat%5B0%5D=Netzwerk+Hardware&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 8) OBI warnt vor Whatsapp-Abzocke mit Gasgrill-Gewinnspiel

**Über Whatsapp verbreitet sich die Nachricht, Obi verschenke 5.000 Gasgrills. Das stimmt nicht. Die Details.**

Erst Milka-Schokolade jetzt Gratis-Gasgrills von Obi: Zur Osterzeit machte [ein gefaktes Milka-Gewinnspiel auf Whatsapp die Runde](#), bei dem angeblich 5.000 mit Schokolade vollgestopfte Oster-Geschenkkörbe verlost wurden. Zeitnah zum Vatertag am 26. Mai 2022 (also diesen Donnerstag) gibt es jetzt eine ähnliche Abzocke.

Angeblich, so heißt es in der Whatsapp-Nachricht, die derzeit verbreitet wird, verlose der Baumarktkriese Obi insgesamt 5.000 Gasgrills. Vatertag und schönes Wetter (gut, danach sieht es derzeit nicht aus), da ist ein neuer, wertvoller Gasgrill natürlich willkommen. Allerdings: Es handelt sich um ein Fake-Gewinnspiel.

Auf [seiner Facebook-Seite weist Obi](#) nach diversen Nachfragen von Verbrauchern darauf hin, dass das angebliche "OBI Vatertags-Gewinnspiel" in keinem Zusammenhang mit dem Unternehmen stehe. Zusätzlich erklärt Obi: "Offizielle Gewinnspiele von OBI erkennt ihr daran, dass diese entweder von unseren offiziellen Social Media Kanälen gepostet werden und/oder der Teilnahmelink auf die obi.de oder in die heyOBI-App führt. Ihr erkennt unsere offiziellen Social Media Kanäle an dem blauen Verifizierungshaken."

### Auf keinen Fall Link in Whatsapp-Nachricht anklicken

Die über Whatsapp verbreitete Nachricht trägt unter anderem den Titel

"Obi 2022 Gewinnspiel zum Vatertag"

gefolgt vom Text

"5.000 kostenlose Gasgrills zu gewinnen".

Der zur Gewinnspielteilnahme angegebene Link führt zu einer WP20.RU-Seite, ähnlich wie im April auch beim angeblichen Milka-Gewinnspiel. Folgt der Nutzer dem Link, dann landet er auf einer Obi-ähnlichen Website und soll zunächst diverse Fragen beantworten und wird auch zum Teilen der Whatsapp-Nachricht mit seinen Kontakten aufgefordert, was dafür sorgt, dass immer mehr Whatsapp-Nutzer diese Nachricht erhalten.

## Whatsapp-Nachricht sofort löschen

Der Link in der Whatsapp-Nachricht über das angebliche Obi-Gewinnspiel sollte auf keinen Fall angeklickt werden. Es ist nicht auszuschließen, dass Betrüger über diesen Weg dann Malware auf dem verwendeten Gerät installieren. Außerdem sollten auch keinerlei persönlichen Daten auf der WP20.RU-Seite preisgegeben werden, denn diese könnten für künftige Angriffe missbraucht werden.

Die Whatsapp-Nachricht sollte auch auf keinem Fall an andere Whatsapp-Kontakte weitergeleitet werden, denn damit unterstützen Sie die Online-Betrüger bei ihrer Abzocke, wenn weniger erfahrene Nutzer hereinfluten. Am besten löschen Sie die Whatsapp-Nachricht sofort und informieren Sie den Absender, dass es sich um eine Abzocke handelt.

Quelle: [https://www.pcwelt.de/news/OBI-warnt-vor-Whatsapp-Abzocke-mit-Gasgrill-Gewinnspiel-11238499.html?utm\\_source=security-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689533&pm\\_cat%5B0%5D=Apps&pm\\_cat%5B1%5D=Social+Web&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/OBI-warnt-vor-Whatsapp-Abzocke-mit-Gasgrill-Gewinnspiel-11238499.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3689533&pm_cat%5B0%5D=Apps&pm_cat%5B1%5D=Social+Web&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## Anwenderinformationen:

### 1) Smartphone-Tipps – Wie Sie Akku-Killern auf die Schliche kommen

**Wenn sich die Smartphone-Batterie ungewöhnlich schnell entleert, kann das verschiedene Gründe haben. Wir erklären die häufigsten Ursachen für den Akkuschwund und was dagegen hilft.**

Smartphone-Akkus werden immer leistungsfähiger. Das müssen sie auch, denn die Ansprüche der Nutzer sind ebenfalls gestiegen. OLED-Displays, ausgefeilte Kameratechnik und schnellere Prozessoren eröffnen neue Anwendungsmöglichkeiten. Dadurch nimmt die Nutzungsdauer zu – und so der Stromverbrauch.

Trotzdem sollte es reichen, das Gerät nur einmal am Tag an die Steckdose anzuschließen. Aktuelle Top-Smartphones sind dazu oft mit ordentlicher Akku-Power ausgestattet. Dennoch stellen Nutzer immer wieder fest, dass das Handy nicht so lange durchhält, wie erwartet. Hier erfahren Sie die häufigsten Gründe für eine verkürzte Akkulaufzeit – und wie Sie das Problem beheben können.

#### **Schritt eins: Energie-Sündern auf die Schliche kommen**

So finden Sie auf einem [Android](#)-Gerät heraus, welche Anwendungen den Akku am meisten beanspruchen.

1. Öffnen Sie die **Einstellungen**.
2. Wählen Sie das Menü "**Akku**" aus.
3. Tippen Sie auf die drei Punkte oben rechts und dann auf "**Akkunutzung**". Hier werden die Apps nach ihrem Energieverbrauch aufgelistet.
4. Tippen Sie erneut auf die drei Punkte oben rechts, um sich die "**Vollständige Gerätenutzung anzeigen**" zu lassen.
5. Der Statistik lässt sich nun auch entnehmen, welche Systemanwendungen die meiste Energie verbrauchen. Das Display steht meistens ganz weit oben.

## Problemzone Display

Neue Display-Technologien sind der Hauptgrund, warum aktuelle Smartphones mehr Strom verbrauchen als ihre Vorgänger. Das Smartphone in den "**Dark Mode**", also den Dunkelmodus zu versetzen, wirkt sich oft positiv auf die Akkulaufzeit aus. Wer die Display-Helligkeit heruntersetzt oder die Funktion "**adaptive Helligkeit**" nutzt, kann ebenfalls Energie sparen.

Ein animierter Sperrbildschirm mag vielleicht hübsch aussehen, verbraucht aber unnötig viel Strom und sollte vermieden werden. Im Stromsparmmodus werden solche Funktionen als Erstes abgestellt.

## Funklöcher saugen heimlich den Akku leer

Um eine stabile Mobilfunkverbindung aufzubauen, muss sich das Smartphone pausenlos anstrengen – ganz besonders in Gegenden mit schlechter Netzabdeckung. Funklöcher sind quasi der natürliche Feind des Smartphone-Akkus. Denn je schwächer das Mobilfunksignal, desto härter muss das Gerät arbeiten, um die Verbindung nicht zu verlieren. Auch dicke Wände belasten den Smartphone-Akku meistens unbemerkt, indem sie den Empfang behindern.

Grundsätzlich ist es deshalb besser, das Smartphone im Freien, statt im Gebäude zu nutzen. Auch die Wahl des Mobilfunkanbieters kann sich aufgrund der unterschiedlichen Netzqualität auf die Akkulaufzeit auswirken. Um den Akku zu schonen, kann das Smartphone zudem in Gegenden mit schlechtem Empfang in den Flugmodus versetzt werden. Dadurch werden die internen Antennen vorübergehend deaktiviert und hören auf, zu funkeln und nach Signalen zu suchen.

## Apps und Hintergrunddienste in die Schranken weisen

Auch Apps und unauffällige Hintergrundanwendungen können zu heimlichen Akku-Killern werden. Ein Blick in die Akkustatistik (siehe Anleitung oben) kann Übeltäter schnell entlarven. Dabei gibt es nicht selten Überraschungen: Teilweise nuckeln Apps am Akku, die man seit Tagen nicht geöffnet hat, und die unauffällig im Hintergrund weiter laufen. Manchmal führt auch ein missglücktes Update zu einem überhöhten Energieverbrauch. Spiele-, Video- und Streaming-Apps sind klassische Kandidaten für einen Spitzenplatz im Batterie-Ranking.

Wie Sie den Energieverbrauch einzelner Apps in den Griff bekommen, zeigen wir [in dieser Fotoshow am Beispiel von WhatsApp](#). Es kann zum Beispiel hilfreich sein, die Hintergrundnutzung von Apps einzuschränken. So geht's:

1. Öffnen Sie das Einstellungs-Menü "**Apps & Benachrichtigungen**".
2. Wählen Sie die App aus, die Sie einschränken wollen. Es werden die App-Informationen angezeigt.
3. Tippen Sie auf "**Erweitert**" und anschließend auf "**Akku**".
4. Unter "Akknutzung verwalten" können Sie jetzt die Hintergrundnutzung einschränken.

## Allgemeine Tipps

Smartphone-Akkus sind sensibel und können mit der Zeit stark an Leistung einbüßen. Das ist normal. Wer jedoch im Umgang mit dem Mobilgerät einige Grundregeln befolgt, kann die Lebensdauer der Batterie positiv beeinflussen. Dazu gehört beispielsweise, das Handy vor extremer Hitze oder Kälte zu bewahren und beim Aufladen Vorsicht walten zu lassen. [Mehr dazu lesen hier](#).

Um den Energieverbrauch zu senken, empfiehlt es sich, nicht mehr benötigte Apps zu deinstallieren. Dadurch wird einerseits Speicherplatz frei und gleichzeitig verhindert, dass die Programme im Hintergrund weiter Daten sammeln und an Dritte übermitteln. Wer mit

eingeschaltetem GPS-, WLAN- und Bluetooth spazieren geht, darf sich ebenfalls nicht über verkürzte Akkulaufzeiten wundern. Diese Funktionen sollten deaktiviert werden, wenn man sie nicht braucht.

Quelle: [https://www.t-online.de/digital/smartphone/id\\_86976234/smartphone-akku-staendig-leer-so-beheben-sie-das-problem.html](https://www.t-online.de/digital/smartphone/id_86976234/smartphone-akku-staendig-leer-so-beheben-sie-das-problem.html)

## 2) Ärger vermeiden – Abwesenheitsnotiz bei Outlook richtig einstellen

**Egal ob Urlaub oder Dienstreise: Eine automatische Abwesenheitsnotiz per E-Mail ist vor der Abreise ein Muss. Wir verraten Ihnen, wie Sie diese schnell und einfach bei Outlook 365 einstellen können.**

Der Sommerurlaub naht oder eine wichtige Geschäftsreise steht an? Oft sind Sie zu solchen Zeiten weder telefonisch noch per E-Mail zu erreichen. Ihre Kontakte können Sie dabei mit einer Abwesenheitsnotiz ganz einfach davon in Kenntnis setzen, wie lange Sie nicht erreichbar und wer alternative Ansprechpersonen sind. Die meisten Firmen setzen hier auf das [Microsoft Office Mail-Programm Outlook](#). Hier können Sie in wenigen Schritten eine automatische Abwesenheitsnotiz einstellen. Wir erklären Ihnen, wie das geht.

### Abwesenheitsnotiz bei Outlook richtig einstellen

Eine Abwesenheitsnotiz ist schnell und einfach mit nur wenig Klicks erstellt. Im Folgenden haben wir eine Schritt-für-Schritt-Anleitung für Outlook in der Version von Microsoft 365 für Sie zusammengestellt:

- Im ersten Schritt starten Sie das Mailprogramm Outlook auf Ihrem Rechner.
- Oben links finden Sie die Registerkarte "Datei", dort klicken Sie auf den Bereich "Informationen."
- Hier gehen Sie auf den Button "Automatisch antworten". Wenn "Automatisch antworten" nicht angezeigt wird, lässt sich das mithilfe des Auswahlpunktes "Regeln und Benachrichtigungen" einstellen.
- Achtung: Bei Outlook 2007 wählen Sie unter "Extras" den Abwesenheitsassistenten aus.
- Ein Fenster öffnet sich. Hier können Sie die Zeit einstellen, während der die automatische Abwesenheitsnotiz versendet wird.
- Darunter haben Sie die Möglichkeit, eine Abwesenheitsnotiz zu formulieren.
- Achtung: Hier gibt es zwei Felder. Eine Abwesenheitsnotiz geht an Adressaten innerhalb Ihrer Organisation und eine an Adressaten außerhalb Ihrer Organisation. Befüllen Sie beide Felder mit Ihrem Abwesenheitstext.
- Bestätigen Sie Ihre Auswahl mit "OK".

### So schreiben Sie eine gute und informative Abwesenheitsnotiz

Mit den folgenden Tipps gestalten Sie eine Abwesenheitsnotiz, die keine Fragen mehr offen lässt:

- Halten Sie die Notiz kurz und beschränken Sie sich auf die wesentlichen Informationen. Verzichten Sie auf Emojis oder Urlaubsbilder, das zeugt nicht von Professionalität.
- Schreiben Sie den Zeitraum Ihrer Abwesenheit in die Notiz und ab wann Sie wieder erreichbar sind.
- Nennen Sie mögliche Ansprechpartner mit Namen, Mailadresse und Telefonnummer, die während Ihrer Abwesenheit kontaktiert werden können.
- Bei internationalen Unternehmen empfehlen wir Ihnen, die Abwesenheitsnotiz auf Deutsch und Englisch zu verfassen.

## **Abwesenheitsnotiz bei Outlook: So deaktivieren Sie die automatische Benachrichtigung**

Das Deaktivieren der Abwesenheitsnotiz bei Outlook ist simpel. Wenn eine Abwesenheitsnotiz aktiviert ist, wird innerhalb des Mailprogramms ein Menüband mit dieser Information angezeigt. Hier klicken Sie einfach auf "Deaktivieren" und die Funktion der Abwesenheitsnotiz ist wieder ausgestellt. Wenn Sie einen festen Zeitraum definiert haben, in welchem die Abwesenheitsnotiz erscheinen soll, so läuft dieser automatisch mit dem definierten Enddatum ab.

**Ein Tipp:** Schalten Sie die Abwesenheitsnotiz etwas länger als Ihre eigentliche Abwesenheit. So vermeiden Sie, dass wichtige Anliegen kurz vor Urlaubsbeginn bei Ihnen auf dem Schreibtisch landen, zugleich haben Sie die Möglichkeit, nach dem Urlaub oder einer längeren Abwesenheit in Ruhe anzukommen. Selbstverständlich funktioniert das nur in Absprache mit den Kollegen und Kolleginnen.

Quelle: [https://www.t-online.de/digital/computer/software/windows/id\\_100009554/abwesenheitsnotiz-bei-outlook-richtig-einstellen.html](https://www.t-online.de/digital/computer/software/windows/id_100009554/abwesenheitsnotiz-bei-outlook-richtig-einstellen.html)

## **3) Chats löschen oder auslagern – Speicherfresser WhatsApp? So schaffen Sie Platz**

**Wer viel Fotos und Videos per WhatsApp austauscht, kann Speicherprobleme auf seinem Smartphone bekommen. Wir zeigen, wie Sie wieder Platz auf Ihrem Gerät schaffen.**

Mit Fotos und Videos können [WhatsApp](#)-Konversationen eine stattliche Größe erreichen. Sollte der Speicher auf dem Smartphone knapp werden, kann es deshalb hilfreich sein, WhatsApp-Chats zu löschen oder auszulagern.

### **[Speicherfresser WhatsApp? So schaffen Sie Platz](#)**

Um herauszufinden, welche Chats die größten Speicherfresser sind, geht man im Menü auf "Einstellungen/Speicher und Daten". Dort werden die Chats nach Größe sortiert aufgelistet.

### **Speicher freiräumen**

Mit einem Klick auf "Speicher verwalten" landen Sie nun im Menü, um den Speicher freizuräumen. WhatsApp zeigt dabei an, wie viel Speicher die App insgesamt belegt und listet die größten Speicherfresser als erstes auf. Zudem zeigt das Programm auch an, welche Chats am meisten Speicher belegen. Wenn Sie auf den entsprechenden Chat klicken, landen Sie im "Medien, Links und Doks"-Ordner, wo die Medien nach Größe sortiert sind.

Um entsprechende Medien zu löschen, tippen Sie mit dem Finger für einige Zeit drauf, bis das Medium markiert ist. So können Sie mehrere Videos oder Bilder auf einmal markieren. Klicken Sie dann auf das Mülleimer-Symbol, um die Datei zu löschen.

### **Chats exportieren**

Die Daten werden dabei von Ihrem Smartphone entfernt und sind nur wieder aufrufbar, wenn Sie ein Back-up angelegt haben – beispielsweise auf Google Drive. Wie Sie ein Back-up anlegen, [zeigen wir Ihnen in dieser Fotoshow](#).

Alternativ können Sie auch in Ihrer Fotogalerie den WhatsApp-Ordner aufrufen. Hier sind alle Video- und Fotodateien, die Sie per WhatsApp verschickt und erhalten haben, ebenfalls aufgelistet. Allerdings weniger übersichtlich als in WhatsApp selbst.

Wenn Sie hier Dateien löschen, landen Sie je nach Betriebssystem aber erst im Mülleimer, ehe sie das System nach einer bestimmten Zeit entfernt.

Quelle: [https://www.t-online.de/digital/handy/id\\_85845506/whatsapp-verbraucht-zu-viel-speicher-so-schaffen-sie-platz.html](https://www.t-online.de/digital/handy/id_85845506/whatsapp-verbraucht-zu-viel-speicher-so-schaffen-sie-platz.html)

## 4) Ab 28.5.: Das wird für Online-Shopper besser – mehr Transparenz

**Der 28. Mai 2022 ist ein wichtiger Tag für alle, die gerne im Internet einkaufen. Das ändert sich beim Online-Shopping.**

Verbraucherschützer aus [Rheinland-Pfalz](#) und [Brandenburg](#) weisen auf wichtige Verbesserungen für Verbraucher hin, die ab 28. Mai 2022 im Internet einkaufen oder online Verträge schließen.

### Verkaufsplattformen

Denn "Internetseiten, auf denen Waren gekauft oder Verträge geschlossen werden, müssen ihre Kundschaft ab 28. Mai 2022 umfassender informieren". Das Angebot und dessen Preise müssen transparenter dargestellt werden. Verkaufsplattformen wie Amazon oder [Ebay](#) müssen künftig angeben, ob ein Unternehmen oder eine Privatperson etwas verkauft. Das ist deshalb wichtig, weil es bei einem Verkauf von privat kein Widerrufsrecht und im Regelfall keine Gewährleistung gibt.

### Buchungs- und Vergleichsportale

Buchungs- und Vergleichsportale wie [Check24](#) oder [Idealo](#) wiederum müssen aufzeigen, ob sie bestimmte Aufgaben für die auf ihren Portalen gelisteten Anbieter übernehmen. Damit soll der Nutzer sofort erkennen können, wer bei Problemen und Fragen der richtige Ansprechpartner ist. Vergleichsportale müssen außerdem mit einer Liste kenntlich machen, welche Unternehmen sie in ihr Ranking einbeziehen, damit der Nutzer erkennen kann, ob überhaupt alle Anbieter erfasst werden. Zudem müssen die Vergleichsportale erklären, welche Hauptparameter bei der Erstellung berücksichtigt werden und wie stark diese auf das Gesamtergebnis Einfluss nehmen.

### Schwankende Preise dank Algorithmus

Wichtig für die Preisfindung: "Alle Online-Shops und Online-Marktplätze sind verpflichtet anzugeben, wenn Preise unter Verwendung personenbezogener Daten oder Merkmale durch einen Algorithmus personalisiert werden". Eine Ausnahme gibt es nur, wenn die Preise zwar im Laufe der Zeit schwanken, diese veränderlichen Preise aber für alle Kunden im gleichen Maße gelten.

### Ticket-Weiterverkauf

Webseiten, auf denen Tickets weiterverkauft werden, müssen den ursprünglichen Ticketpreis zusätzlich zu dem von ihnen verlangten Preis angeben. Damit sollen Wucherpreise bei Eintrittskarten sofort erkennbar werden.

### Artikelbewertungen

Zu Artikelbewertungen müssen Anbieter ab dem 28.5.2022 [erläutern](#) , "ob und wie sie sicherstellen, dass die Bewertungen von Verbrauchern stammen, die die beurteilten Produkte wirklich genutzt oder erworben haben".

## Ausnahmen

Ausgenommen von den neuen Informationspflichten für den Online-Handel sind Verträge über Finanzdienstleistungen wie Kredite, Versicherungen und die Altersversorgung von Einzelpersonen.

### Tipps:

[Das gilt neu für Internet, Telefonie, Anbieterwechsel, Neu- und Altverträge](#)

[Ab 1.3.: Kürzere Kündigungsfristen für neue Verträge](#)

[Mobilfunk & Internet: Ihre neuen Rechte als Verbraucher](#)

Quelle: [https://www.pcwelt.de/news/Ab-28.5.-Das-wird-fuer-Online-Shopper-besser-mehr-Transparenz-11235305.html?utm\\_source=security-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689447&pm\\_cat=%5B0%5D=Web+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Ab-28.5.-Das-wird-fuer-Online-Shopper-besser-mehr-Transparenz-11235305.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3689447&pm_cat=%5B0%5D=Web+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 5) 9-Euro-Ticket in iPhone-Wallet übertragen: Mit diesem Trick klappt's

**Mit diesem Trick können Sie das 9-Euro-Ticket in Ihre Apple Wallet übertragen und anzeigen lassen.**

Wenn Sie diesen Artikel hier lesen, haben Sie wahrscheinlich bereits das beliebte 9-Euro-Ticket gekauft und fragen sich nun: Gibt es eine Möglichkeit, das Ticket in die [Apple](#) Wallet zu übertragen? Tatsächlich gibt es die, es folgt aber ein großes "aber". Es kommt nämlich ganz darauf an, wo und vor allem wie Sie das Ticket gekauft haben:

1. Ticket als ausgedrucktes Exemplar
2. Online-Ticket über die DB-Navigator-App
3. Online-Ticket über regionale Anbieter

### **Nicht übertragbar: Diese 9-Euro-Tickets funktionieren nicht**

Wenn Sie das Ticket in physischer Form vorliegen haben, da Sie es etwa über ein Reisezentrum gekauft haben, können Sie es leider nicht in die [Apple](#) Wallet hinzufügen. Dies funktioniert ebenfalls (noch) nicht mit einem über die DB-Navigator-App gekauften Ticket. Die Deutsche Bahn hat bisher nicht bekannt gegeben, ob sie an einer Möglichkeit arbeitet, dass das günstige 9-Euro-Ticket genauso zur [Apple](#) Wallet hinzugefügt werden kann wie Tickets für IC oder ICE. Da Sie aber auch keine DB-Monatstickets auf Ihrem [iPhone](#) in der digitalen Brieftasche hinterlegen können, ist die Wahrscheinlichkeit doch recht gering.

**Lesetipp :** [Achtung: 9-Euro-Ticket gilt doch nicht in allen Nahverkehrszügen](#)

### **Übertragbar: So zeigen Sie das 9-Euro-Ticket in der Apple Wallet an**

Je nachdem, wo Sie in Deutschland wohnen, können Sie die 9-Euro-Tickets über die App der entsprechenden regionalen Verkehrsbetriebe kaufen. Sie haben dadurch keine Nachteile, die Tickets lassen sich genauso leicht wie am Schalter oder der DB-Navigator-App kaufen, Sie können sogar eine Rechnung anfordern.

Der Vorteil liegt jedoch klar auf der Hand: In manchen Apps von regionalen Verkehrsbetrieben können Sie Tickets in Ihre Apple Wallet übertragen, wie in der BVG-App der Berliner Verkehrsbetriebe. Wenn Sie das Ticket bereits vor dem 01. Juni erworben haben, werden Sie noch warten müssen, bis Sie das Ticket in Ihre Wallet-App werden importieren können. Sollten Sie zudem bereits ein 9-Euro-Ticket gekauft haben, müssen Sie bis Juli oder August warten,

bis Sie ein neues Ticket für den nächsten Monat erwerben können – eine Stornierung oder ein Umtausch ist nicht möglich.

**Hinweis:** Ob die App Ihres bevorzugten regionalen Verkehrsbetriebs tatsächlich Apple Wallet unterstützt, können Sie ganz leicht überprüfen: Suchen Sie im App Store nach der entsprechenden App, scrollen Sie weiter nach unten und schauen Sie nach dem Hinweis, ob die App auch wirklich Apple Wallet unterstützt.

Quelle: [https://www.macwelt.de/news/9-Euro-Ticket-in-iPhone-Wallet-uebertragen-Mit-diesem-Trick-klappt-s-11240727.html?utm\\_source=macwelt-daily-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3689576&pm\\_cat%5B0%5D=Apple&pm\\_cat%5B1%5D=iOS&pm\\_cat%5B2%5D=Mobile+Client&pm\\_cat%5B3%5D=Mobile+Plattformen&pm\\_cat%5B4%5D=Mobilfunk&pm\\_cat%5B5%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.macwelt.de/news/9-Euro-Ticket-in-iPhone-Wallet-uebertragen-Mit-diesem-Trick-klappt-s-11240727.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3689576&pm_cat%5B0%5D=Apple&pm_cat%5B1%5D=iOS&pm_cat%5B2%5D=Mobile+Client&pm_cat%5B3%5D=Mobile+Plattformen&pm_cat%5B4%5D=Mobilfunk&pm_cat%5B5%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 6) Gekauft bei Apple: Apps und Medien zurückgeben

**Im Onlinehandel ist es weithin üblich, bei Problemen oder Nichtgefallen bestellte Waren – meist auf Kosten des Verkäufers – binnen vierzehn Tagen zurückgeben zu können. Im Onlinehandel ist es weithin üblich, bei Problemen oder Nichtgefallen bestellte Waren – meist auf Kosten des Verkäufers – binnen vierzehn Tagen zurückgeben zu können. Aber wie sieht es bei digitalen Inhalten aus? Im Folgenden erfahren Sie, ob und auf welche Weise Sie bei Apple erworbene Apps, E-Books, Filme oder Musikdateien zurückgeben können.**

Seit der Corona-Pandemie boomt der Onlinehandel noch mehr als zuvor, und damit steigt auch die Zahl der Retouren. Den Onlinehändlern entstehen dadurch Kosten in erheblichen Ausmaßen, die sie größtenteils selbst tragen müssen. Zudem werden manche niedrigpreisige Waren deswegen entsorgt, was der Umwelt nicht gerade zuträglich ist. Amazon, aber auch andere Onlinehändler wie [Otto](#), sind, was Rückgaben anbelangt, überwiegend sehr kulant. Sobald sie allerdings feststellen, dass ein Kunde viele Bestellungen wieder zurückgehen lässt, werden Sie hellhörig und können die von ihnen freiwillig gewährten Rückgabemöglichkeiten, über das Fernabsatzgesetz hinaus, erheblich einschränken oder drohen gar mit Sperrung des Benutzerkontos.

### Kann ich digitale Inhalte zurückgeben?

Bei digitalen Inhalten, die Sie per Download auf Ihrem Computer, Tablet oder Smartphone erwerben, sieht es etwas anders aus. In diesem Fall war bis 2014 überhaupt keine Rückgabe möglich. Mittlerweile gilt auch hier das gesetzliche Widerrufsrecht von 14 Tagen nach Kauf – unter Umständen mit gewissen Einschränkungen, über die der Käufer vor dem Vertragsabschluss in Kenntnis gesetzt werden muss. Überdies ermöglicht Ihnen [Apple](#) digitale Inhalte auch nach diesem Zeitpunkt zurückgeben zu können. Bitte beachten Sie dazu die folgenden Hinweise. Übrigens gilt auch hier: Wer zu viele Apps und digitale Inhalte zurückgibt, dem wird eine Rückgabe auf Kulanz unter Umständen eingeschränkt oder komplett gestrichen.

Ihre bei [Apple](#) erworbenen digitalen Inhalte können binnen vierzehn Tagen ohne Angabe von Gründen zurückgegeben werden. Dies gilt auch für In-App-Käufe, jedoch nicht für Abonnements. Ist der Erwerb länger als vierzehn Tage her, müssen Sie es triftig begründen, warum Sie eine App, einen Film, einen Musiktitel, ein ganzes Album oder auch ein E-Book nicht mehr haben wollen. Nach 90 Tagen erlischt dann jegliche Möglichkeit, bei [Apple](#) erworbene digitale Inhalte zurückzugeben.

## Wann erhalte ich mein Geld zurück?

Wird Ihrer Rückgabe stattgegeben, kann es einige Zeit dauern, bis Sie das Geld zurückerhalten. Dies hängt unter anderem davon ab, ob eine Prüfung durch Apple erforderlich ist, was bis zu sieben Tage in Anspruch nehmen kann. Haben Sie die App oder die anderen digitalen Inhalte mit iTunes-Guthaben erworben, wird der Kaufbetrag meist binnen 48 Stunden gutgeschrieben. Bei der Bezahlung durch Lastschrift kann dies allerdings bis zu 30 Tage in Anspruch nehmen und bei Begleichung über Ihren Mobilfunkvertrag ist es möglich, dass Sie sogar bis zu 60 Tage warten müssen.

Möchten Sie Apps, Filme oder Musiktitel und Musikalben zurückzugeben, folgen Sie unserer Anleitung. Die Vorgehensweise ist immer die gleiche, egal um was für digitale Inhalte es sich handelt. Ob Sie hierzu einen Mac, ein **iPhone** oder **iPad** verwenden, macht ebenfalls keinen Unterschied, da die Rückgaben über die entsprechende Webseite von Apple abgewickelt werden.

1. Um eine App zurückzugeben, suchen Sie zunächst die dazugehörige Rechnung von Apple. Diese befindet sich meistens in Ihrem iCloud-Postfach oder im Postfach eines anderen E-Mail-Kontos, je nachdem, welches Sie für Ihre Apple-ID angegeben haben.
2. Auf der Rechnung klicken Sie unten auf den Eintrag „Ein Problem melden“ und melden sich dann über die Apple-ID an, mit der Sie den Kauf getätigt haben.
3. Alternativ können Sie auch gleich die Webseite „ <https://reportaproblem.apple.com> “ aufrufen und sich dann mit der entsprechenden Apple-ID anmelden. Unter Umständen müssen Sie sich wegen der bei Apple üblichen Zwei-Faktor-Authentifizierung mit einem neunstelligen Code identifizieren.
4. Anschließend wählen Sie die entsprechende App oder den anderen digitalen Inhalt aus, den Sie zurückgeben möchten. Klicken Sie dann rechts des Kaufdatums auf die Rechnungsnummer.
5. Als Nächstes klicken Sie auf den Eintrag „Beleg anzeigen“. Im Beleg finden Sie den Eintrag „Problem melden“. Klicken Sie auch auf diesen.
6. Im ersten Aufklappmenü „Wie können wir dir helfen“ wählen Sie zuerst „Eine Rückerstattung beantragen“ aus und klicken auf „Weiter“.
7. Im zweiten Aufklappmenü „Erzähl uns mehr“ wählen Sie die entsprechende Antwort, wie „Ich wollte das nicht kaufen“ oder „Widerrufsrecht“. Ihr Widerrufsrecht können Sie aber nur binnen vierzehn Tagen nach dem Kauf in Anspruch nehmen.
8. Über einen Mausklick auf „Weiter“ versenden Sie Anfrage auf Rückerstattung. Wie oben erwähnt, kann Ihr Antrag auf Rückerstattung auch längere in Anspruch nehmen. Er wird in jedem Fall über die Bezahlmethode gutgeschrieben, die Sie dafür verwendet haben.

## Abos kündigen

Apps, die Sie per Abo erworben haben, können Sie leider nicht ohne Weiteres zurückgeben. In diesem Fall müssen Sie das Abo fristgerecht kündigen. Hierzu gehen Sie auf die folgende Weise vor:

1. Öffnen Sie den App Store und klicken Sie auf Ihre Apple-ID (am Mac links unten).
2. Klicken Sie dort auf „Accounteinstellungen“ und wählen Sie unten in der Kategorie „Verwalten“ rechts neben „Abos“ auf den gleichnamigen Eintrag.
3. Um ein Abo zu kündigen, klicken Sie auf „Bearbeiten“ und dann auf die Schaltfläche „Abo kündigen“.

4. Bitte beachten Sie etwaige Kündigungsfristen. Die Abos können Sie gegebenenfalls nach der Kündigung weiter nutzen – so lange, bis der entsprechende Abonnementzeitraum abgelaufen ist.

**Anmerkung der Redaktion:** Weitere Infos können unter dem u.g. Link abgerufen werden.

Quelle: [https://www.macwelt.de/news/Gekauft-bei-Apple-Apps-und-Medien-zurueckgeben-8307463.html?utm\\_source=macwelt-daily-automatisch&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3040184&pm\\_cat=%5B0%5D=Apple&pm\\_cat%5B1%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.macwelt.de/news/Gekauft-bei-Apple-Apps-und-Medien-zurueckgeben-8307463.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3040184&pm_cat=%5B0%5D=Apple&pm_cat%5B1%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 7) Dekra sucht Auto-Besitzer für Werkstatt-Tests – Inspektionskosten werden erstattet

**Die Dekra sucht für Werkstatt-Tests Auto-Besitzer. Teilnehmende Auto-Besitzer bekommen in der Regel einen Großteil der Inspektionskosten erstattet.**

Im Rahmen ihrer regelmäßigen Werkstatt-Tests sucht die Dekra Automobil GmbH Testkunden. Im Auftrag von Fahrzeugherstellern oder Autohäusern überprüft die Dekra mithilfe dieser Fahrzeugbesitzer die Qualitätsstandards von Werkstätten.

### **Inspektionskosten teilweise erstattet**

Der Kunde wünscht sich von seiner Werkstatt im Prinzip das gleiche wie der Autohersteller von seinem Vertrags-Autohaus: erstklassigen Service und beste Qualität. Um das zu gewährleisten, beauftragen Hersteller, aber zunehmend auch Autohäuser selbst, Prüf-Unternehmen wie die Dekra mit Werkstatt-Tests. Dazu wird ein Kundenfahrzeug präpariert: kleine Mängel sollten im Rahmen der fälligen Inspektion behoben werden.

Nach dem Test prüfen die Dekra-Experten das Auto noch einmal und bauen, wenn nötig, die Veränderungen wieder zurück. **Für den zeitlichen Aufwand bekommt der Testkunde in der Regel einen Großteil der Inspektionskosten erstattet.**

### **Hier registrieren**

Wer sich dafür interessiert, mit seinem Fahrzeug an einem solchen Test teilzunehmen, kann sich entweder online unter [www.inspektion-kostenlos.de](http://www.inspektion-kostenlos.de) als Testkunde registrieren oder unter der Telefonnummer 07117861-1919 direkt im Dekra Service Center anrufen. Auf der genannten Webseite gibt es auch ein Erklärvideo mit allen Informationen, wie ein solcher Werkstatt-Test aus Kundensicht abläuft.

Die Werkstatt-Tests werden jeweils nach Marken und teilweise auch nach Regionen geplant. Sobald ein entsprechender Test ansteht, werden registrierte Kunden mit passenden Fahrzeugen kontaktiert. Sie können dann endgültig entscheiden, ob sie teilnehmen wollen.

Aktuell sucht die Dekra beispielsweise Fahrzeuge der Marken VW (Pkw und Nutzfahrzeuge), BMW / MINI, Volvo, Opel, Škoda, Fiat und Mazda für Werkstatt-Tests. Grundsätzlich kommen aber Fahrzeuge aller Marken infrage.

Quelle: [https://www.pcwelt.de/news/Dekra-sucht-Auto-Besitzer-fuer-Werkstatt-Tests-Kosten-erstattet-9550558.html?utm\\_source=best-of-pc-welt-manuell&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3111330&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/news/Dekra-sucht-Auto-Besitzer-fuer-Werkstatt-Tests-Kosten-erstattet-9550558.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3111330&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 8) Whatsapp: So sehen Sie, wer Sie blockiert

**Ob ein Kontakt Sie auf Whatsapp blockiert, können Sie recht schnell herausfinden. Wir zeigen Ihnen, wie das geht.**

Aus Gründen der Privatsphäre teilt Whatsapp Ihnen nicht mit, wenn jemand Sie blockiert. Und doch gibt es Möglichkeiten, es herauszufinden. Es gibt nämlich einige Hinweise, die Ihnen Aufschluss darüber bringen, wer Sie bei Whatsapp blockt.

### **Nachricht wird nicht zugestellt – nur ein Haken**

Schicken Sie eine Nachricht an einen Whatsapp-Kontakt und es erscheint nur ein Häkchen unter der Nachricht, dann ist dies ein erster Hinweis. Denn kommt eine Nachricht ganz regulär beim Empfänger an, erscheinen normalerweise zwei Häkchen: Das erste Häkchen bedeutet, dass die Nachricht auf den Servern bei Whatsapp gelandet ist. Das zweite Häkchen erscheint, wenn die Nachricht erfolgreich beim Empfänger angekommen ist.

Fehlt der zweite Haken, kann dies bereits ein Indiz sein, dass der Empfänger keine Nachrichten mehr von Ihnen bekommen möchte. Das Indiz kann aber erst durch die nächsten Punkte bekräftigt werden. Denn es kann auch daran liegen, dass es aktuell ein technisches Problem seitens Whatsapp gibt oder, noch wahrscheinlicher, der Empfänger das Handy derzeit ausgeschaltet, es in den Flugmodus gestellt oder einfach keinen Internetempfang hat.

### **Das Profilbild fehlt plötzlich**

Befindet sich auf einmal an der Stelle des Profilbildes nur noch ein grauer Platzhalter und Sie können den Whatsapp-Status der Person nicht mehr sehen, dann wurden Sie wahrscheinlich blockiert. Fehlt nur das Profilbild, kann es auch daran liegen, dass Ihr Kontakt sein Bild entfernt hat.

### **Sehr sicheres Indiz: Neue Whatsapp-Gruppe erstellen**

Erstellen Sie eine neue Whatsapp-Gruppe und fügen Sie unter anderem den Kontakt hinzu, von dem Sie vermuten, blockiert zu werden. Schauen Sie sich anschließend die Teilnehmer der Gruppe genau an. Taucht hier der Kontakt nicht auf, hat dieser Sie blockiert. Daher ist diese Methode sehr sicher, um festzustellen, ob Sie geblockt werden.

Interessant ist aber: Sind Sie bereits mit dem Blockierer in einer bestehenden Gruppe, dann können Sie diesen in der Gruppe noch immer markieren und anschreiben. Allerdings sehen diese Nachricht natürlich auch die anderen Gruppenmitglieder.

### **Whatsapp-Anrufe nicht mehr erfolgreich**

Bei Whatsapp können Sie Video- und Sprachanrufe über eine Internetverbindung führen. Wenn Sie blockiert sind, dann sind Anrufe nicht mehr erfolgreich, heißt: Der Empfänger sieht diese nicht und kann sie entsprechend nicht annehmen. Sie hören allerdings die Anruftöne, der Anruf bricht nicht sofort ab. Das kann auf jeden Fall verwirren.

### **"Zuletzt Online" prüfen**

Hat ein Kontakt Sie blockiert, dann können Sie nicht mehr sehen, wann dieser zuletzt online war. Hier ist allerdings Vorsicht geboten: Denn auch, wenn ein Kontakt die entsprechende Einstellung unter "Datenschutz" deaktiviert hat, können sie diese Info nicht einsehen.

**Hinweis:** Die meisten Punkte treffen auch dann zu, wenn eine Person ihren Whatsapp-Account gelöscht hat.

## So können Sie selbst einen Kontakt blockieren

Um selbst jemanden zu blockieren, tippen Sie auf den Chat mit der Person und dann auf ihren Namen. Scrollen Sie nach ganz unten und tippen Sie dort auf "Blockieren" und bestätigen Sie dies anschließend. Um zu sehen, wen Sie alles blockieren, navigieren Sie in die WhatsApp-Einstellungen und tippen Sie dort auf "Account – Datenschutz". Hier finden Sie den Punkt "Blockierte Kontakte". Tippen Sie den Kontakt an, können Sie ihn wieder "freigeben".

Alle Nachrichten, die der Kontakt während der Blockierung an Sie geschickt hat, können Sie nicht sehen. Und andersherum sieht der Blockierer nicht, was Sie ihm während der blockierten Zeit geschrieben haben.

## Weitere spannende Whatsapp-Themen

- [So nutzen Sie WhatsApp auf PC, iPad und Android-Tablet](#)
- [WhatsApp-Status heimlich ansehen](#)
- [Gelöschte WhatsApp-Nachrichten trotzdem lesen](#)
- [WhatsApp mit Festnetznummer nutzen](#)
- [WhatsApp für Notizen verwenden](#)
- [WhatsApp-Profilbilder von anderen Kontakten abspeichern](#)

Quelle: [https://www.pcwelt.de/ratgeber/WhatsApp-blockiert-wer-hat-mich-geblockt-11007222.html?utm\\_source=best-of-pc-welt-manuell&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3665594&pm\\_cat=%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/ratgeber/WhatsApp-blockiert-wer-hat-mich-geblockt-11007222.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3665594&pm_cat=%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)

## 9) Geldkarte gestohlen: Das müssen Sie sofort tun!

**Ihre Girocard (EC-Karte) oder Kreditkarte ist weg? So reagieren Sie richtig, um finanziellen Schaden zu vermeiden. Plus: Restrisiko ausschließen.**

Der erste Sommerurlaub nach Corona steht vor der Tür. Wenn Ihnen im Urlaub die Girocard (früher als EC-Karte bezeichnet) oder die Kreditkarte gestohlen werden, oder diese wichtigen Karten sonst wie verloren gehen, dann müssen Sie schnell handeln, um finanziellen Schaden zu vermeiden. Sibylle Miller-Trach, Finanzjuristin der Verbraucherzentrale Bayern, [hat Tipps dazu zusammengestellt](#), wie Sie nach dem Verlust von Girocard oder Kreditkarte reagieren sollten.

Karte sperren lassen: Bei Verlust oder Diebstahl sollte die Karte sofort unter der Rufnummer 116 116 gesperrt werden. Wer aus dem Ausland anruft, muss die deutsche Vorwahl 0049 vorwählen oder kann die Nummer 0049 30 4050 4050 nutzen. Für die Kartensperrung benötigen Verbraucher die IBAN-Nummer ihres Kontos beziehungsweise die Kartenummer der Kreditkarte.

**[Hier hat die Volksbank alle Sperrnummern zusammengestellt.](#)**

**Aufgepasst:** Trotz erfolgter Kartensperre können Diebe kontaktlos noch für einige Stunden mit der gestohlenen Karte bezahlen. Wie das möglich ist und wie Sie dieses Restrisiko unterbinden, lesen Sie in dem Beitrag ["Trotz Kartensperre: Diebe zahlen mit gestohlener Karte – so verhindern Sie das."](#)

**Nummern vorher notieren:** Hilfreich ist es, vorbeugend einen Notfallzettel mit den Telefonnummern zum Sperren und der Kartenummer/IBAN zu erstellen und diesen an einem sicheren Ort aufzubewahren.

Mit der Kartensperrung können Dritte nicht mehr über das Konto verfügen.

**Anzeige erstatten:** Wurde die Karte gestohlen, sollten Verbraucher zudem bei der Polizei vor Ort Anzeige erstatten.

**Meldung an Kuno:** Urlauber in Deutschland können den Kartenverlust außerdem über die [Polizei bei Kuno](#) melden. Kuno ist eine Kooperation zwischen Polizei und Einzelhandel, die Kartenmissbrauch vermeiden soll. Nutzt ein Betrüger eine bei Kuno gemeldete Karte, wird der Verkäufer an der Kasse über die Kartensperrung informiert. Der Kriminelle kann dann im Geschäft mit Karte und Unterschrift nicht mehr bezahlen (Lastschriftverfahren). Auch hier lesen Sie mehr in [Trotz Kartensperre: Diebe zahlen mit gestohlener Karte – so verhindern Sie das.](#)"

**Geld aus Ersatzquellen beschaffen:** Sollten Urlauber im Ausland tatsächlich einmal ohne ausreichendes Bargeld und ohne Zahlungskarten dastehen, haben sie die Möglichkeit, Zahlungsdienste wie Western Union, Azimo, Paypal oder Money Gram zu nutzen. Über diese Dienstleister können Angehörige Geld schicken.

**Apple Play oder Google Pay als alternative Bezahlmöglichkeiten:** Sofern Sie nicht auch noch Ihr Smartphone verloren haben, können Sie gegebenenfalls auf einem [iPhone](#) über [Apple Pay](#) und auf einem Android-Smartphone über [Google Pay](#) bezahlen. Dazu müssen Sie diese Bezahlverfahren aber in aller Ruhe rechtzeitig vor dem Aufbruch in den Urlaub einrichten. Voraussetzung ist, dass Ihre Bank diese Bezahlverfahren unterstützt. Außerdem können Sie nur bei teilnehmenden Partnerunternehmen mit diesen Bezahlverfahren tatsächlich bezahlen.

Quelle: [https://www.pcwelt.de/ratgeber/Geldkarte-gestohlen-Das-muessen-Sie-sofort-tun-10604181.html?utm\\_source=best-of-pc-welt-manuell&utm\\_medium=email&utm\\_campaign=newsletter&ext\\_id=3620034&pm\\_cat%5B0%5D=Mobile+OS&pm\\_cat%5B1%5D=Mobile+Client&pm\\_cat%5B2%5D=Mobile+Plattformen&pm\\_cat%5B3%5D=Mobilfunk&pm\\_cat%5B4%5D=Apps&pm\\_cat%5B5%5D=Google&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4](https://www.pcwelt.de/ratgeber/Geldkarte-gestohlen-Das-muessen-Sie-sofort-tun-10604181.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3620034&pm_cat%5B0%5D=Mobile+OS&pm_cat%5B1%5D=Mobile+Client&pm_cat%5B2%5D=Mobile+Plattformen&pm_cat%5B3%5D=Mobilfunk&pm_cat%5B4%5D=Apps&pm_cat%5B5%5D=Google&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4)