# 44. Cybercrime Newsletter

**30.10.2024**

## 1) Betrugs-Ticker - Neuer Android-Trojaner greift Bankdaten ab

**Betrüger sind einfallsreich, wenn es darum geht, Menschen um ihr Geld zu bringen. Wir zeigen Ihnen, welcher Maschen sich derzeit bedient wird.**

**Inhaltsverzeichnis:**



Kriminelle versuchen immer wieder, an sensible Daten von Konten und Kreditkarten sowie persönliche Informationen von Verbrauchern zu kommen. Dafür nutzen sie vorwiegend digitale Kanäle. Welche Maschen sie dabei verwenden, erfahren Sie hier.

### ++ Schadsoftware bei Android bedroht Bankdaten (22.10.2024) ++

Ein neuer Trojaner wird aktuell für Android-Nutzer gefährlich, wie Sicherheitsforscher berichten. Die Schadsoftware mit dem Namen Trickmo könne Sicherheitseinstellungen deaktivieren, Passwörter und PIN-Codes abgreifen und die Zwei-Faktor-Authentifizierung auf dem Smartphone umgehen. Dadurch könnten Betrüger zum Beispiel an Passwörter für das Online-Banking gelangen.

Das Programm sieht für Laien wie eine normale App aus und kann den Sperrbildschirm des Handys imitieren. Neben Bankdaten können auch E-Mails, Social-Media-Accounts und weitere vertrauliche Informationen betroffen sein.

Um die Installation von Schadsoftware auf dem Gerät zu verhindern, sollten Sie niemals auf Links in E-Mails oder SMS von verdächtigen Absendern klicken. Außerdem ist es ratsam, Apps nur aus dem offiziellen Google Play Store herunterzuladen.

**++ Behörde berichtet von Paypal-Betrugsmasche (8.10.2024) ++**

Wer zurzeit einen Anruf mit der belgischen Vorwahl +32 erhält, sollte vorsichtig sein. Dahinter könnte sich ein gefälschter Paypal-Anruf verstecken. Nimmt man das Gespräch an, berichtet am anderen Ende eine Stimme vom Band von einer ausgelösten, hohen Zahlung. Dann wird der Angerufene aufgefordert, zur Verhinderung der Zahlung die Taste 1 zu drücken.

Die Bundesnetzagentur warnt: "Es ist davon auszugehen, dass die Anrufe einen rechtsmissbräuchlichen Hintergrund haben. Die Bundesnetzagentur warnt insbesondere davor, Anrufern persönliche Daten mitzuteilen."

Laut der Behörde kommt es neben den Anrufen aus dem Ausland in einigen Fällen auch zu Anrufen unter Anzeige deutscher Mobilfunkrufnummern. "Beenden Sie den Anruf", rät die Bundesnetzagentur. "Ignorieren Sie außerdem die Aufforderung, eine Taste zu drücken und teilen Sie keinesfalls persönliche Daten mit. Erzählen Sie Familie, Freunden und Bekannten von dieser Masche, damit diese gewarnt sind."

**++ Targobank-Kunden im Visier von Betrügern (6.10.2024) ++**

Die Verbraucherzentrale warnt auf ihrer Webseite derzeit vor einer Betrugsmasche, die vor allem auf Kunden der Targobank abzielt. Laut dem "Phishing-Radar" der VZ haben die betrügerischen E-Mails die Betreffzeile: "Verifizieren Sie Ihre Telefonnummer für einen sicheren Kontozugang".

Über einen Link in der Nachricht soll man dann genau das tun können. Doch die Verbraucherzentrale warnt davor, diesen Link zu öffnen. Bereits an der "unseriösen Absenderadresse" und der "unpersönlichen Anrede" könne man erkennen, dass es sich bei der E-Mail um einen Phishing-Versuch handele. Wer diese Nachricht erhalten hat, sollte sie ins Spam-Postfach verschieben und nicht reagieren.

**++ Polizei warnt vor "Schockanrufen" (25.9.2024) ++**

Die Polizei in Thüringen warnt vor sogenannten "Schockanrufen" eines Betrügers, der sich als Polizist ausgibt. So seien die Beamten im Raum Apolda von mehreren Senioren auf Telefonbetrüger aufmerksam gemacht worden. Die Senioren berichteten, dass sich ein Mann am Telefon als Polizeibeamter ausgegeben und behauptetet habe, dass ein Familienmitglied in einen schweren Verkehrsunfall verwickelt war. Bei dem Unfall sei eine Person ums Leben gekommen und man benötigte nun zur Entlassung des Beschuldigten eine Kaution in Höhe mehrerer tausend Euro.

"Glücklicherweise ging keiner der Angerufenen dieser Aufforderung nach und informierte umgehend die Polizei", schreibt die Polizeiinspektion Apolda und warnt "eindringlich vor dieser Art von Anrufen", bei der Menschen durch schlechte Nachrichten und mit Panikmache unter Druck gesetzt werden. Ein Zeichen solcher "Schockanrufe" sei auch, dass der Anrufer versucht, den Angerufenen unter allen Umständen in der Leitung zu halten, damit keine Nachfrage bei Polizei, Verwandten oder Freunden möglich ist.

Gute Nachrichten in Sachen vereitelter Betrug kommen auch aus Nordrhein-Westfalen. Hier berichtet "Der Weseler Lokalkompass", dass in den vergangenen Tagen mehrere Senioren "Schockanrufe" bei der Polizei meldeten. Alle hätten die Betrugsmasche erkannt und das Richtige getan: aufgelegt.

**++ Kochtopfmasche: Seniorin um 110.000 Euro betrogen (24.9.) ++**

Betrüger haben eine Seniorin in Sachsen mit der sogenannten Kochtopfmasche um 110.000 Euro geprellt. In zwei weiteren Fällen übergaben Senioren den Betrügern jeweils 25.000 Euro, wie die Dresdner Polizei berichtet. Erst später bemerkten sie den Betrug und

verständigten die Polizei. Bei der sogenannten Kochtopfmasche geben sich die Täter gegenüber meist älteren Menschen am Telefon als Polizisten aus. Im Gespräch suggerieren sie den Senioren, dass eine Diebesbande in ihrem Wohnumfeld unterwegs sei, die mit einem speziellen Ortungsgerät namens CC 15 Geldscheine auch innerhalb von Häusern aufspüren könne und dann gezielt einbrechen würde.

Die angeblichen Polizisten raten daher, das Geld in einen Kochtopf zu stecken, wo es nicht geortet werden könne. Zugleich bieten sie an, dass ein Beamter in Zivil das Geld abholt und angeblich in Sicherheit bringt. Die echte Polizei rät indes, niemals Geld in fremde Hände zu geben und keine Fremden in die Wohnung zu lassen.

**++ Angstmacherei mit Abos von Disney+ (23.9.) ++**

Am Anfang der neuen Woche steht die Kundschaft des Streamingportals Disney+ im Phishing-Fokus. Der Betreff einer betrügerischen E-Mail, vor der die Verbraucherzentrale warnt, lautet "Bitte aktualisieren Sie Ihre Informationen". In der E-Mail wird darüber informiert, dass das Abonnement angeblich ausgesetzt wird. Grund dafür sei, dass die Bank die Belastung abgelehnt habe. Nun sollen die Rechnungsinformationen über einen Link aktualisiert werden – andernfalls könne der Kunde seine "Vorteile" verlieren.

Auf den ersten Blick wirkt die Mail unauffällig, schreiben die Verbraucherschützer. Durch die unseriöse Absendeadresse wird jedoch deutlich, dass es sich um Phishing handelt. Lesen Sie hier alles dazu, was Phishing ist und wie man es erkennt. Klicken Sie auf keinen Fall auf den Link, sondern verschieben Sie die E-Mail unbeantwortet in den Spam-Ordner.

**++ Telefonbetrüger spielen Bundesbehörde (22.9.) ++**

Ein Mitarbeiter der Bundesdatenschutzbeauftragten ruft an und will helfen, verzocktes Geld zurückzuholen: Wenn Ihnen das seltsam vorkommt, liegen Sie mit Ihrem Gefühl genau richtig. Betrüger missbrauchen derzeit den Namen einer Bundesbehörde für Lockanrufe. Sie geben sich als Mitarbeitende der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aus und bieten vermeintlich ihre Hilfe an.

Konkret geht es um die angebliche Möglichkeit, bei Kryptobörsen investiertes, aber verlorenes Geld zurückzuholen.

Bei diesen Anfragen handele es sich aber um Betrug, stellt die Behörde in einer Mitteilung klar. Die Anrufe stammten nicht vom BfDI. Keinesfalls sollten Angerufene irgendwelchen Aufforderungen nachkommen oder Daten preisgeben.

Denn es gehe den Tätern darum, mit in den Telefonaten gewonnenen Informationen weitere Betrugsversuche zu unternehmen. Gleichzeitig müssten die Opfer der Phishing-Anrufe aber auch damit rechnen, für weitere Betrügereien erneut kontaktiert zu werden.

**++ Betrugsmasche mit angeblichem Millionenerbe (11.9.) ++**

Die unbekannte reiche Tante aus den USA ist gestorben – und plötzlich ist man unerwartet Millionär. Was wie ein unrealistisches Klischee klingt, ist derzeit Gegenstand einer altbekannten Betrugsmasche. Denn schon seit längerer Zeit gibt es Betrugsversuche mit gefälschten Briefen an Personen, die angeblich ein Millionenerbe aus dem Ausland bekommen sollen.

Der Polizei Bad Segeberg in Schleswig-Holstein ist nun eine Weiterentwicklung dieser Masche aufgefallen. Statt per Brief kamen solche Betrugsversuche in letzter Zeit häufig per E-Mail, wie die Polizei in einer Pressemitteilung erklärt. Oft versuchen die Kriminellen erst, an persönliche Daten der Opfer zu gelangen. Schließlich sollen diese dann Steuern für das Millionenerbe bezahlen.

Die Polizei rät davon ab, diese Schreiben zu beantworten. Im Zweifel sollte man Kontakt mit der Polizei aufnehmen.

**++ Stiftung Warentest warnt vor dubiosen Finanzportalen (7.9.) ++**

Die Stiftung Warentest warnt derzeit vor zwei Online-Finanzportalen – die Webseiten "zinsbox.com" und "Spar-global.com". Bei dem ersten Portal sollen Anleger angeblich gut verzinstes Festgeld von bis zu 4,30 Prozent inklusive Willkommensbonus erhalten. Laut Stiftung Warentest besteht allerdings "akute Abzockergefahr". Vermutlich ist die Webseite dazu da, um Adressdaten zu sammeln.

Auch bei "Spar-global.com" handelt es sich der Stiftung Warentest zufolge um Abzocker, die es ebenfalls auf Personen abgesehen haben, die Festgeld anlegen möchten. Dabei werden ein vermeintliches Festgeldangebot bei der Santander Bank mit 5,72 Prozent, einer Laufzeit von zwei Jahren und ein Willkommensbonus von 150 Euro angepriesen. Dahinter verbirgt sich aber schlichtweg eine Masche, um an das Geld von Interessierten zu kommen.

Die Stiftung Warentest rät dazu, bei solchen Webseiten immer erst das Impressum zu checken. Steht dort beispielsweise keine Firma oder fehlt die Rechtsform, handelt es sich mutmaßlich im Betrüger.

**++ Neue Betrugsmasche auf "Immoscout24" (30.8.) ++**

In vielen Städten ist die Wohnungssuche zu einer echten Herausforderung geworden. Dass Betrüger auf Internetportalen persönliche Daten abzocken wollen, erleichtert das Ganze nicht. Auf der Webseite "Immoscout24" kam es vor Kurzem zu einer Abzocke von 30.000 Euro, wie der Spiegel berichtet.

Über ein gefälschtes Inserat erschlichen sich die Betrüger die Bewerbungsunterlagen, darunter auch Gehaltsabrechnungen mit Bankdaten. Kurz darauf erhalten die Betrugsopfer Post von ihrer angeblichen Bank mit einer Aufforderung zur Verifizierung eines bestehenden Kontos per Postident-Verfahren. Wird dies bestätigt, wird dadurch unwissentlich ein Kredit im Wert von 30.000 Euro für fünf Jahre genehmigt.

"Immoscout24" wurde über die Betrugsmasche informiert und verweist laut Spiegel darauf, Bewerbungsunterlagen nur über die Plattform einzureichen und nicht per E-Mail zu verschicken.

Laut dem Lagebericht der IT-Sicherheit 2023 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Bedrohung im Cyberraum "so hoch wie nie zuvor". Gerade für Unternehmen sind die Folgen eines Cyberangriffs oft fatal. Aber auch Privatpersonen können nach einem erfolgreichen Angriff viel Geld verlieren und jede Menge Ärger bekommen.

**Tipp:** Vorsicht, Phishing!: Woran Sie Betrugs-Mails sofort erkennen

Hochmoderne Phishing-Attacke: KI-Betrug: Neue Gefahr für 2,5 Milliarden E-Mail-Konten

Smartphone Sicherheit: Phishing SMS Link geöffnet – was tun?

Quelle: https://www.t-online.de/digital/aktuelles/id_100494652/neue-android-schadsoftware-trojaner-trickmo-greift-bankdaten-ab.html

# 2) Cybertrading-Fraud oder Trading Scam --Fiese Internet-Betrugsmasche mit angeblicher Promi-Werbung

**Kriminelle bringen Privatanleger um Millionen. Angebliche todsichere Anlagetipps von Promis wie Helene Fischer, Markus Lanz oder Didi Hallervorden.**

Eine neue Masche im Internet bringt Anleger zum Teil um ihr gesamtes Erspartes. Betroffene müssen ihre Häuser verkaufen, Ehen gehen darüber in die Brüche, vereinzelt gibt es gar Suizide, warnt die Staatsanwaltschaft. Sie verbucht unter Cybertrading-Fraud Millionenschäden bei Privatleuten. Mitunter wird die Masche auch Trading Scam genannt.

Cybertrading-Fraud oder auch Trading Scam nennt die Polizei die noch recht neue, fiese Masche, mit der Kriminelle im Internet Privatanleger um ihr Erspartes bringen.

**Cybertrading-Fraud und Trading Scam: So läuft die Betrugsmasche ab**

Der Ablauf ist dabei laut Polizei immer der Gleiche: Kriminelle veröffentlichen auf Nachrichtenportalen oder Social-Mediaseiten Anzeigen, die wie redaktionelle Artikel von bild.de oder tagesschau.de aussehen

In den vermeintlichen Artikeln werden (nichtsahnende) Promis zitiert und mit Foto gezeigt. So sollen darin angeblich verraten, wie sie mit scheinbar todsicheren Geldanlagen vermeintlich ein Vermögen gemacht haben.
Über Links werden "Interessierte" daraufhin auf professionell wirkende Anlage-Plattformen weitergeleitet und ein Kontakt zu vermeintlichen Anlageberatern hergestellt.
Diese “Anlageberater” bauen teilweise über Wochen ein Vertrauensverhältnis zu ihren späteren Opfern auf. Die Betroffenen werden immer wieder ermutigt, in Raten in eine Kryptowährung wie Bitcoins oder andere Anlagen zu investieren. Die Kriminellen versprechen hohe Renditen.
Das Geld werde aber mitnichten angelegt, sondern verschwinde in den kriminellen Netzwerken.

**Betroffen sind auch Internet-erfahrene, überlegt handelnde Menschen**
Siegfried Berger ist so einer. Der Rentner wollte seinen Sohn bei dessen Hausbau unterstützen, hatte extra Geld beiseitegelegt: 34.000 Euro. Doch das Geld ist jetzt weg. Siegfried Berger, der seinen eigentlichen Namen nicht preisgeben will, ist fassungslos: "Das war für mich die größte Enttäuschung über mich selber, dass ich auf so eine Nummer reingefallen bin, weil: bis ich eine Entscheidung treffe, wird die zigmal abgewogen."

**Didi Hallervorden gibt scheinbar bei Markus Lanz tolle Geldanlage-Tipps**
Im Mai dieses Jahres stößt Siegfried Berger im Internet auf einen vermeintlichen Artikel über Dieter Hallervorden. Angeblich von Tagesschau.de. Dieter Hallervorden soll in der Talksendung von Markus Lanz über seine Geldanlagestrategie mit Online-Trading gesprochen haben.

Siegfried Berger: "Bei dem Artikel war alles absolut glaubwürdig, Die Zweifel sind erst viel später gekommen. Dieser Artikel und auch dieser Ablauf dieser ganzen Geschichte war extrem professionell gestaltet."

Ein Link in dem Artikel führt Siegfried Berger auf die Seite der vermeintlichen Finanzberatungsfirma "Inter Algo" mit Sitz in Wien, über die man Geld anlegen könne.

**Vermeintliche Anlageberater rufen mehrmals an, bauen Vertrauen auf**
Der Rentner gibt seinen Namen, E-Mail-Adresse und Telefonnummer an. Kurz darauf bekommt er eine Mail von einer angeblichen Kontomanagerin namens Anna Lau. Darin weist sie ihm einen Anlageberater zu – Martin Becker. Und behauptet:

"Sie brauchen Ihrem Expert Schritt für Schritt zu folgen und alles zu machen, was er Ihnen sagt, damit mit den besten Moeglichkeiten die höchsten Gewinne gemacht werden."

Von nun an ruft der vermeintliche Anlageberater fast täglich bei Siegfried Berger an. Zunächst soll Siegfried Berger 250 Euro überweisen, dann zweimal etwa 5.000 und noch zweimal etwa 10.000 Euro. Bereits nach kurzer Zeit zeigt sein Konto ihm hohe Gewinne an.

**Angeblich über 155.000 Euro Rendite**
Doch als der Rentner seine mittlerweile angeblich 190.000 Euro ausbezahlt bekommen möchte, gibt es Probleme. Er erhält ein Schreiben – von der Firma "Blockchain": Damit die Gewinne seiner Anlage in einer Kryptowährung in Euro ausgezahlt werden könnten, müsse Siegfried Berger vorher noch ein neues Konto eröffnen. Und noch mehr Geld zahlen.

Siegfried Berger: "Mir war von diesem Zeitpunkt an klar, dass meine eingezahlten Beträge weg sind." Er verständigt die Polizei und erfährt: Er ist auf eine Betrugsmasche hereingefallen, die sich in Expertenkreisen eben Cybertrading Fraud nennt: Bei dieser Betrugsmasche werden im Internet gezielt Werbeanzeigen als Artikel getarnt. Kriminelle kaufen dafür Werbeplätze bei Nachrichten-Seiten oder in sozialen Netzwerken.

**Promis wie Markus Lanz, Helene Fischer oder Til Schweiger geben angeblich super Anlage-Tipps**
Fast immer erzählen Promis wie etwa Markus Lanz, Helene Fischer oder Til Schweiger, mit welchem angeblich todsicheren Anlagetrick sie ein Vermögen gemacht haben.

André Wolf und seine Kollegen von dem gemeinnützigen Verein zur Aufklärung von Internetmissbrauch "Mimikama" beobachten Falschmeldungen und Betrug im Netz schon seit Jahren. Auch die aktuelle Betrugsmasche kennt er – die gab es in anderen Varianten schon öfter. André Wolf: „Wenn wir das anklicken, landen wir eben auf einer gefälschten Website. In diesem Fall gibt sie sich als die “Bild” aus und dort bekommen wir einen pseudo-redaktionellen Artikel – also, der tut so, als sei er ein echter Artikel.“

Diese Masche beschäftigt auch die Zentralstelle für Cyberkriminalität bei der Staatsanwaltschaft Bamberg.

**Zentralstelle Cybercrime der Polizei warnt vor dieser Masche**
Hier sind seit 2019 Anzeigen mit einem Gesamtschaden von 350 Millionen Euro bei Oberstaatsanwalt Nino Goldbeck eingegangen. Und das dürfte nur die Spitze des Eisbergs sein. Viele bringen den Betrug nicht zur Anzeige.

Nino Goldbeck, Oberstaatsanwalt bei der Zentralstelle Cybercrime Bayern: „Es gibt Fälle, da ist im siebenstelligen Bereich Geld verloren gegangen und leider müssen wir sehen, dass in vielen Fällen das ganze Familien kaputt macht, dass Ehen ganz erheblich unter diesen Verlusten leiden und in einigen wenigen Fällen waren tatsächlich auch schon Suizide am Ende zu beklagen.“

**Täter psychologisch geschult**
Die Täter sind psychologisch geschult, bauen in der Regel über Wochen und Monate per Telefon und Chatnachrichten Vertrauen zu ihren Opfern auf. Hinter dem Betrug steckt ein riesiges, wachsendes System, das europaweit agiert.

**Callcenter im Ausland**

Die Täter sitzen mit ihren Callcentern im Ausland: In Georgien, der Ukraine, Israel, Serbien oder Bulgarien. Im vergangenen Jahr gelang den Ermittlern ein Schlag in Georgien gegen eine von etlichen Tätergruppierungen.

Der Staatsanwalt war selbst dabei, er zeigt Fotos. Nino Goldbeck: „Es gibt die Hintermänner, es gibt die Managementebene und es gibt diejenigen Personen, die gewissermaßen an vorderster Front tätig sind und tagtäglich den Kundenkontakt halten. Und dort sind dann, aufgeteilt nach Sprachräumen, in unterschiedlichen Abteilungen Dutzende, teilweise Hunderte Personen tätig, die allesamt die jeweilige Sprache ihrer Kunden sprechen, häufig sehr gut. Und die machen von morgens bis abends nichts anderes als betrügen, als Lügengebilde aufbauen.“ Doch wer sind die Betrüger, die Siegfried Berger um viel Geld gebracht haben?

**Gibt es die Firma wirklich?**
Ein Schreiben der Redaktion an Anna Lau, die damals das Konto für Siegfried Berger eingerichtet hat, bleibt unbeantwortet. Im österreichischen Firmenregister ist keine Firma mit dem Namen Inter-Algo registriert.

Und bei der angegebenen Adresse in Wien ist weder das Unternehmen Inter-Algo noch eine Anna Lau zu finden. Der angebliche Firmensitz – ein Fake. Und was sagen die Prominenten, mit deren Namen die Betrüger ihre Opfer ködern?

**Didi Hallervorden entsetzt über Betrug unter seinem Namen**
Marktcheck trifft Didi Hallervorden in seinem Theater in Berlin. Der betrügerische Artikel, auf den Siegfried Berger hereingefallen ist, handelte von ihm.

Didi Hallervorden ist entsetzt, dass sein Name für solche Betrugsmaschen missbraucht wurde: "Ich bin ja durch Sie drauf aufmerksam gemacht worden. Da stimmt ja hinten und vorne gar nichts. So dämlich wäre ich ja niemals, mich im Fernsehen hinzusetzen mit einem Hemd – was übrigens längst im Müll gelandet ist. Das ist von vorne bis hinten alles getrickst. Und die armen Leute, die darauf reingefallen sind und das Geld ist ja futsch! Es ist eine solche Arglist, mit der diese Leute vorgehen und dermaßen Menschen-verachtendes Verhalten ich bin entsetzt."Aber wie erkennt man, dass es sich um einen gefälschten Artikel handelt?

**Wie kann man sich schützen?**
André Wolf von Mimikama rät, auf die URL des Onlineartikels zu achten. Da steht häufig ein anderer Name als der des angeblichen Mediums wie etwa Tageschau oder Spiegel. Andre Wolf: „Der beste Tipp ist immer noch: ich nehme so eine Schlagzeile, tippe sie in eine Suchmaschine und schaue, ob diese Schlagzeile irgendwo im Netz gefunden werden kann. Das machen wir einfach mal: Ich öffne eine Suchmaschine meiner Wahl, kopiere die Schlagzeile oder tippe Sie dort einfach ein und das war es. Und jetzt sehe ich: diese Schlagzeile ist nirgendwo zu finden. Was heißt das? Was angeblich passiert ist, stimmt nicht.“

Für Siegfried Berger kommen diese Tipps zu spät. Sein Geld ist weg. Irgendwo im Ausland versickert. Er wird künftig wachsamer sein beim Surfen und hofft, dass nun wenigstens andere durch seine Geschichte gewarnt sind.

**Anmerkung der Redaktion:** Unter dem u.g. Link sind weitere Infos abrufbar

Quelle: https://www.swr.de/verbraucher/ard-marktcheck/anlagebetrug-mit-prominenten-100.html

# 3) Fiese Masche: Hacker geben sich als IT-Support aus und kapern Ihren PC

**Ein neuer Sicherheitsbericht zeigt eine gefährliche Masche der Hackergruppe Black Basta auf. Sie verschaffen sich Zugriff, indem sie sich als Tech-Support ausgeben.**

Sicherheitsforscher der Firma Reliaquest haben eine neue Masche aufgedeckt, mit der sich Hacker Zugriff auf Unternehmensrechner verschaffen. Die Phishing-Kampagne nutzt eine fiese Social-Engineering-Taktik, bei der die Opfer über Microsoft Teams kontaktiert und im Glauben gehalten werden, mit einem IT-Support zu sprechen.

Laut des Berichts operiert die Ransomware-Gruppe Black Basta, die seit 2022 zu den bekanntesten Hackergruppen aufgestiegen ist, mit diesem System. Zuvor stützte sich die Gruppe auf klassisches E-Mail-Phishing, doch im Oktober wurden vermehrt Angriffe mit der neuen, verbesserten Methode festgestellt.

### So funktioniert der Hack-Versuch

Sowohl beim E-Mail-Phishing als auch bei der Variante mit Teams fordern die Hacker bestimmte Nutzer dazu auf, ein Ticket mit ihrem Helpdesk zu erstellen, um ein vorgetäuschtes IT-Problem zu lösen. Anstatt auf die erstellte Mail zu antworten, kommunizieren die Angreifer aber über Microsoft Teams, um das Ganze direkter und glaubhafter wirken zu lassen.

Dabei wird meist ein Gespräch erstellt, das den Betreff “OneOnOne” beinhaltet. Nutzer werden dann dazu aufgefordert, einen QR-Code zu scannen, um eine Remote-Software zur Problemlösung herunterzuladen. Dahinter steckt aber ein Ransomware-Tool, das die komplette Übernahme des genutzten PCs ermöglicht.

Dabei scheinen die Gespräche mit dem angeblichen Helpdesk-Mitarbeiter glaubhaft genug zu sein, um eine ernsthafte Bedrohung für Unternehmen darzustellen. Die Phishing-Kampagne soll sich mit “alarmierender Intensität” ausgebreitet haben. Die Hackergruppe soll dabei die anvisierten Firmen mit tausenden E-Mails “zuspammen”, bis eine davon letztlich Erfolg hat.

Vorsicht vor diesen sieben neuen Hackertricks: So schützen Sie sich

### Das können Sie tun

Achten Sie bei der Nutzung von Microsoft Teams darauf, dass Sie nur mit Personen innerhalb Ihres Unternehmens kommunizieren oder genau wissen, welche Person über extern Kontakt mit Ihnen aufnehmen kann. Die Hacker nutzen meistens Mail-Adressen, die auf “onmicrosoft.com” enden, um Vertrauen zu wecken.

Gehen Sie nicht direkt davon aus, dass Sie mit einem IT-Support schreiben, wenn dieser Sie nicht auf den offiziellen Kanälen kontaktiert oder per Mail auf Ihre Anfrage antwortet. Zudem

sollten Sie darauf achten, in welcher Zeitzone sich Ihr Gesprächspartner befindet. Die Angriffe sollen vor allem aus Russland erfolgen.

Bei weiteren Unsicherheiten kontaktieren Sie am besten Ihren IT-Beauftragten oder installieren, wenn möglich, eine effektive Antiviren-Software zum Schutz Ihres Rechners.

Quelle: https://www.pcwelt.de/article/2502537/fiese-masche-hacker-geben-sich-als-it-support-aus-und-kapern-ihren-pc.html

# 4) Sicherheitsforscher haben funktionsfähige macOS-Malware entdeckt

**Malware-Entwickler haben funktionsfähige Ransomware erstellt, die auf macOS abzielt. Im Umlauf ist sie aber offenbar nicht.**

Offenbar haben Cyberkriminelle bemerkt, dass sie die Taktiken, die sie auf anderen Plattformen fahren, auch auf Apple-Systeme anwenden können. Sicherheitsforscher der Firma Trend Micro haben macOS-Malware entdeckt, die in der Lage ist, Dateien zu sperren und Daten zu exfiltrieren. Bisher gab es Ransomware, die auf macOS abzielt, bestenfalls als Proof of Concept, schlechtestenfalls tat sie nicht, was sie sollte.

## Imposter: Malware ändert das Desktop-Wallpaper zu LockBit 2.0

Nach erfolgter Verschlüsselung der Dateien auf dem System gab sich die Malware per geändertem Desktop-Banner als LockBit-Ransomware aus. Offenbar stammte die Schadsoftware jedoch nicht von der bekannten Ransomware-Gruppe, auch wenn einer der erfolgreicheren unter den vorangegangenen Versuchen, Ransomware für macOS zu entwickeln, tatsächlich von LockBit stammte. Das Wallpaper zeigte die Aufschrift LockBit 2.0, die Schadsoftware der Gruppierung liegt allerdings schon seit Längerem in Version 3.0 vor und die Entwickler wurden gefasst. Hinter dem jetzt entdeckten Sample scheint ein anderer Akteur zu stecken, der nur den Namen der bekannteren Gruppierung nutzt.

Geschrieben ist die Ransomware laut der Forscher in der von Google entwickelten Programmiersprache Go. Sie wird als x86_64-Binärdatei verteilt, was bedeutet, dass sie nur auf Macs mit Intel-Prozessor läuft – oder auf Apple Silicon Macs, auf denen die Rosetta Emulation Software installiert ist.

**"macOS.NotLockBit"**

Forscher der Firma Sentinel, die das Thema auf ihrem Blog aufgreifen, schlagen den Namen macOS.NotLockBit für die Schadsoftware vor. Sie haben zusätzlich zu den bereits von anderen Forschern identifzierten eine Reihe weiterer sogenannter Mach-O-Dateien gefunden. Mach-O ist ein spezielles Dateiformat für Programme, Objektcode und dynamische Bibliotheken, das in macOS verwendet wird. In einem Blogpost haben sie sogenannte Indicators of Compromise (IoC) untersucht. Anhand solcher Hinweise lässt sich im Allgemeinen überprüfen, ob eigene Systeme befallen sein könnten.

Die NotLockBit-Malware scheint sich derzeit noch in der Entwicklung zu befinden und in freier Wildbahn wurde sie bisher nicht gesichtet. Der AWS-Account des Entwicklers wurde gesperrt, nach Einschätzung der Verfasser des Sentinel-Blogposts ist es angesichts der Entwicklungsarbeit, die bisher in die Malware geflossen ist, eher wahrscheinlich, dass mittelfristig noch etwas aus dieser Richtung kommen könnte.

Quelle: https://www.heise.de/news/Sicherheitsforscher-haben-funktionsfaehige-macOS-Malware-entdeckt-9993566.html?wt_mc=rss.red.ho.ho.rdf.beitrag.beitrag

# 5) News – Nicht rangehen: Gefährlicher Anruf aus Österreich will Ihre Bankdaten stehlen

**Aktuell melden Nutzer vermehrt Scam-Anrufe aus Österreich. Es geht um angebliche Gewinnspiele, Abos oder die Abfrage von Bankdaten. So handeln Sie richtig.**

Immer wieder kommt es zu vermehrten Anrufen aus dem Ausland, die mit betrügerischer Absicht deutsche Nutzer kontaktieren wollen. Aktuell gibt es vermehrte Meldungen über Anrufe aus Österreich, vor allem unter der Nummer **+4367764423153**. Das steckt hinter den Anrufen.

### Betrugsversuch

Mehrere Nutzer meldeten die österreichische Nummer als Betrugsversuch, Kostenfalle oder Telefonterror. Allein im letzten Monat sollen laut tellows über 7000 Anrufe durch die Unbekannten eingegangen sein, die sich am Telefon als Abo-Service oder Lotterie-Anbieter ausgeben.

Teilweise rufen sie mehrmals am Tag oder in kurzen Abständen hintereinander an, oft auch mit wechselnden Nummern. In jedem Fall wird am Telefon nach Ihren Bankdaten verlangt, um ein dubioses Abo abzuschließen oder auch einen angeblichen Gewinn einzufordern.

In manchen Fällen verlangen die Telefon-Betrüger auch Geld für die Löschung der Nutzerdaten oder geben sich als Verbraucherschützer aus. Auch Ping-Anrufe, bei denen direkt wieder aufgelegt wird, wurden von Betroffenen dokumentiert.

### Das sollten Sie tun

Wie immer gilt, auf jegliche Angebote am Telefon nicht einzugehen. Ihre Bankdaten sollten Sie keinesfalls weitergeben und auch nicht zurückrufen, falls Sie mehrmals angerufen wurden und nicht erreichbar waren.

Am besten ist, Sie sperren die Nummer direkt und prüfen weitere Anrufe mithilfe einer kurzen Google-Suche. Geben Sie außerdem Ihre Telefonnummer nicht weiter, wenn Sie die Absichten der Person oder Firma nicht kennen. Sonst landet sie eventuell in weiteren Telefonlisten, die für weitere Scam-Anrufe genutzt werden können.

Quelle: https://www.pcwelt.de/article/2496846/gefaehrlicher-anruf-aus-oesterreich-verlangt-nach-ihren-bankdaten-4367764423153.html?utm_date=20241029135711&utm_campaign=Security&utm_content=slotno5-title-Nicht%20rangehen%3A%20Gef%C3%A4hrlicher%20Anruf%20aus%20%C3%96sterreich%20will%20Ihre%20Bankdaten%20stehlen&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 6) Warnung vor Cyberkriminellen – Betrüger auf Airbnb: Diese Masche bringt Sie um Ihr Geld

**Aktuell treiben Betrüger auf Airbnb ihr Unwesen. User werden angewiesen, Zahlungen für Ferienunterkünfte außerhalb der Plattform zu leisten. Die Folgen können schwer wiegen.**

Nicht jeder möchte in seinem Urlaub ins Hotel. Wer eher auf Individualtourismus setzt, mietet sich lieber eine Ferienwohnung – über einschlägige Portale wie Airbnb.

Doch wer derzeit eine Unterkunft über diese Plattform buchen möchte, sollte vorsichtig sein. Denn wie die Internetsicherheitsplattform Watchlist Internet mitteilt, treiben dort gerade

Betrüger ihr Unwesen.

Wenn man sich ein Ferienhaus oder eine -wohnung bei Airbnb bucht, tut man dies normalerweise direkt auf der Webseite oder in der App – inklusive Bezahlung. Werden Sie vor Ihrer Buchung darauf hingewiesen, stattdessen die Unterkunft per E-Mail zu buchen, sollten bei Ihnen die Alarmglocken schrillen.

Laut Watchlist Internet versuchen Kriminelle, ihre Opfer von der Webseite zu locken und ihnen dann das Geld für die Ferienwohnung zu stehlen. Die Experten der Sicherheitsplattform gehen davon aus, dass die Betrüger in tatsächlich existierende Airbnb-Konten eindringen und diese für ihre Zwecke missbrauchen.

### Betrüger locken Opfer auf gefälschte Webseite

Wer der Aufforderung der Cyberkriminellen nachkommt und die "Vermieter" per E-Mail kontaktiert, bekommt auch eine Antwort. In der (auf Englisch verfassten) Nachricht heißt es dann, dass die angefragte Unterkunft noch verfügbar sei. Allerdings habe der angebliche Gastgeber Probleme mit dem Airbnb-Kalender. Deswegen wird man gebeten, die Ferienwohnung über Booking.com zu buchen.

Die Betrüger geben sich als bemühte Vermieter aus, die ihren Opfern auch gleich einen Buchungslink zu Booking.com zuschicken. Folgt man diesem Link, gelangt man zu einer Webseite, die tatsächlich wie die von Booking.com aussieht – es aber nicht ist. Die bekannte Seite wurde von den Kriminellen schlichtweg kopiert. Erkennen kann man das an URLs wie "booking.stays-3876566623.live[…]".

Abgesehen davon wirkt die gefälschte Webseite aber doch recht überzeugend. Entscheidet man sich dazu, seine Ferienwohnung dort zu buchen, geht das nur per direkter Banküberweisung. Doch wer den geforderten Betrag überweist, wird diesen vermutlich nicht wiedersehen – die Falle der Betrüger ist zugeschnappt.

### Was tun, wenn man in die Falle getappt ist?

Seien Sie daher besonders vorsichtig, wenn Sie über Airbnb buchen wollen, den Vermieter aber per E-Mail kontaktieren sollen. Kontrollieren Sie die URL der Webseite, wenn Sie einen Link erhalten, wie Watchlist Internet rät.

Ist das Geld erst einmal weg, ist es schwierig, es wiederzubekommen. Bemerken Sie den Betrug schnell, können Sie Ihre Bank kontaktieren und darum bitten, die Überweisung zu stoppen. Wie das geht, lesen Sie hier.

Leider funktioniert so etwas in den seltensten Fällen. Sie können sich auch an Airbnb wenden und den Fall schildern – vielleicht lassen sie Milde walten und erstatten Ihnen das Geld. Außerdem sollten Sie den Betrug melden – bei Airbnb und auch bei der Polizei.

Quelle: https://www.t-online.de/digital/aktuelles/id_100510274/airbnb-diese-betrugsmasche-kann-sie-viel-geld-kosten.html

## 7) Ecovacs-Amoklauf: Hacker lassen Saugroboter eskalieren

**Hacker haben Saugroboter ins Visier genommen und lassen sie rassistische Beleidigungen und Schimpfwörter aussprechen.**

Hacker haben die in China hergestellten Staubsaugerroboter Ecovacs Deebot X2 angegriffen und eine bekannte Sicherheitslücke ausgenutzt, um die volle Kontrolle über die Geräte zu erlangen.

Mehrere verdutzte Besitzer berichteten, dass sich ihre Staubsaugerroboter unberechenbar verhielten und anstößige Aussagen von sich gaben. Anwalt Daniel Swenson aus Minnesota berichtete ABC News von seinen Erfahrungen. Swenson sah gerade fern, als sein Deebot X2 anfing, seltsame Geräusche zu erzeugen.

Als Swenson die App des Staubsaugers überprüfte, stellte er fest, dass jemand auf die Live-Kameraübertragung als auch auf die Fernbedienungsfunktionen zugegriffen hatte. Wie ihm das gelang, ist nicht bekannt. Trotz seiner Versuche, das Gerät durch Zurücksetzen des Passworts und Neustart den Hackern zu entreißen, eskalierte die Situation. Der Staubsauger setzte sich selbstständig wieder in Bewegung, und aus seinen Lautsprechern ertönte eine menschliche Stimme, die rassistische Obszönitäten schrie.

### Mehrere Geräte betroffen

Der Angriff auf Swensons Gerät ereignete sich am 24. Mai 2024, zeitgleich mit einem ähnlichen Vorfall in Los Angeles, bei dem ein anderer Deebot X2 Berichten zufolge einen Hund verfolgte, während das Gerät über seine Lautsprecher beleidigende Kommentare von sich gab. Fünf Tage später ereignete sich ein vergleichbarer Vorfall in El Paso.

Die Ursache für diese Eingriffe scheint eine kritische Sicherheitslücke im Deebot X2s zu sein, die es nicht autorisierten Benutzern ermöglicht, die erforderliche vierstellige Sicherheits-PIN zu umgehen und so die volle Kontrolle über das Gerät zu erlangen. Dieser Fehler wurde erstmals im Dezember 2023 entdeckt.

Als Reaktion auf diese Vorfälle entwickelt Ecovacs, der Hersteller des Deebot X2s, einen Sicherheitspatch, um die Schwachstellen zu schließen. Laut Informationen von Gizmodo soll dieses Update im November 2024 veröffentlicht werden. Eine offizielle Bestätigung von Ecovacs bezüglich des Patches gibt es nicht.

Quelle:https://www.golem.de/news/ecovacs-amoklauf-hacker-lassen-saugroboter-eskalieren-2410-189771.html?utm_source=flipboard&utm_content=KarinHeise%2Fmagazine%2FMeine%0AAuswahl

# 8) Tausende betroffen: Ermittlungen gegen DSL-Anbieter gestartet

**15.000 Kunden sollen es sein, die in die Fänge eines DSL- und Telefonanbieters gerieten. Dessen Methoden dürften zumindest als zweifelhaft bezeichnet werden. Jetzt wurden Ermittlungen eingeleitet. Verbraucherschützer prüfen indes eine Sammelklage.**

Die Methode ist offenbar immer dieselbe: In einem Brief wirbt die Firma für einen DSL– und Telefon-Anschluss, der günstiger ist als der aktuelle Telekom-Anschluss der Kunden, die den Brief bekommen. Diese unterschreiben den Vertrag, weil sie denken, dass das Schreiben von ihrem Anbieter käme. Mit der Unterschrift beauftragen sie jedoch keinen Tarifwechsel, sondern einen Anbieterwechsel. Erst einige Tage später, wenn die Deutsche Telekom ihren Kunden mitteilt, ihr liege ein Wechselwunsch vor, wird den Kunden oftmals klar: Sie haben keinen Tarifwechsel veranlasst, sondern einen neuen Vertrag abgeschlossen: mit der 1N Telecom GmbH. Über den Anbieter berichteten wir bereits im vergangenen Jahr.

### 1N Telecom fordert bei Stornierung 419,88 Euro

Das Problem: Möchte der Kunde den Vertrag rückgängig machen, scheitert er. Übereinstimmenden Kundenberichten zufolge ist das Unternehmen telefonisch nicht zu erreichen. Selbst an der angegebenen Firmenanschrift ist niemand anzutreffen, wie TV-Reporter des SWR Marktcheck herausfanden. Die Verbraucherzentralen haben seit dem

Jahr 2023 mehr als 11.000 Beschwerden über den Telekommunikationsanbieter erhalten.

Vor allem ältere Menschen seien nach Angaben der Verbraucherzentrale betroffen. Wiederholt berichten Betroffene, dass sie erst nach Ablauf der 14-tägigen Widerrufsfrist bemerkt haben, dass sie nicht auf Post der Deutschen Telekom reagiert haben, sondern einen Vertrag mit einem anderen Anbieter eingegangen sind. Verhindern sie anschließend die Portierung ihrer Telefonnummer, kündigt 1N Telecom und fordert Schadensersatz in Höhe von 419,88 Euro. Das Geld lässt die Firma demnach auch von einer Inkassofirma eintreiben, berichten die Verbraucherschützer. Der vzbv hält die Regelung zur Vertragslaufzeit in den Verträgen für unwirksam und deswegen die Schadensersatzforderung für unberechtigt. Die Bundesnetzagentur hat nach Angaben der ARD Tagesschau im vergangenen Jahr 15.000 Wechselvorgänge gestoppt.

### Verbraucherschützer prüfen Sammelklage

Der vzbv hatte den Anbieter nach eigenen Angaben bereits abgemahnt. 1N Telecom weigerte sich aber, eine Unterlassungserklärung abzugeben, berichten die Verbraucherschützer. Deswegen hat der vzbv Unterlassungsklage beim OLG Düsseldorf eingereicht. Auch die Verbraucherzentralen Baden-Württemberg und Sachsen-Anhalt gehen gegen das Unternehmen vor. Und: Nach Angaben der Tagesschau ermittelt jetzt auch die Staatsanwaltschaft.

Der vzbv bittet Betroffene, sich an einer kurzen Umfrage unter www.sammelklagen.de/verfahren/1n-telecom zu beteiligen. Die Umfrageergebnisse nutzt der vzbv, um eine Sammelklage gegen 1N Telecom zu prüfen. Mit einer Sammelklage können im Erfolgsfall Rückzahlungen für Betroffene gerichtlich erwirkt werden, so die Verbraucherschützer.

Quelle: https://www.inside-digital.de/news/tausende-betroffen-ermittlungen-gegen-dsl-anbieter

# 9) Produktsuche im Internet – Geraten Kunden über Google-Werbung an Fakeshops?

**Hinter etwa 20 Prozent der Anzeigen bei den Google-Suchergebnissen („Google Ads“) könnten Fakeshops stecken. Unternimmt der Konzern genug dagegen?**

Drei Kühlschränke für knapp 200 Euro? Wer im Internet nach einem Produkt sucht, landet schnell bei attraktiven Angeboten von Onlineshops. Vor allem bei Google werden solche **gesponsorten Produktanzeigen** weit oben in den Suchergebnissen angezeigt: Besonders günstige Angebote, die genau zum Gesuchten passen. Doch hinter den prominent platzierten Suchergebnissen stecken nicht immer seriöse Angebote und Webseiten, wie eine Marktcheck-Recherche zeigt.

Die Abzocke **betrügerischer Fakeshops** im Netz ist dabei nichts Neues. Neu ist allerdings, dass Betreiber solcher Seiten die Suchmaschine Google offenbar als Köder nutzen. Wer Links zu seinen Produkten bei Google prominent platzieren will, muss dafür bezahlen – die Rede ist dabei von gesponsorten Suchergebnissen. Und genau das nutzen Betrüger nun mutmaßlich aus, um Kunden in die Falle zu locken.

### Fakeshop-Betreiber schalten Anzeigen bei Google Shopping

Gregor Ambros aus Cottbus hat das Vorgehen von Fakeshop-Betreibern im Internet beobachtet. Er selbst sei Opfer von betrügerischem Handeln im Netz geworden, sagt er. Er betreibt zwei Online-Shops mit Produkten aus dem Spreewald. Doch sein Impressum und die Adresse seiner Firma tauchten vor Kurzem noch auf einer weiteren Seite im Netz auf:

Dem vermeintlichen Online-Shop werners24.de, der inzwischen gar nicht mehr existiert. Betrüger hätten die Adressangaben von seiner Seite Gourmeo 24 einfach für ihre Fakeseiten verwendet, sagt Gregor Ambros gegenüber Marktcheck.

Er glaubt, dass die Betrüger **bei Google Werbeanzeigen kaufen**, um ihre Opfer in die Falle zu locken. "So, wie wir das gesehen haben, haben die massiv Anzeigen bei Google Shopping geschaltet und aktiv Produkte beworben, um sichtbarer zu werden." Üblicherweise würde ein Webshop, der neu aufgesetzt wird, ansonsten gar nicht so weit vorne bei den Suchergebnissen auftauchen. "Vermutlich war das das Ziel: Dass dort aktiv Werbung betrieben wird, um Leute auf die Seite zu bekommen."

### Ein Insider vermutet, dass Google mit den Fakeshops viel Geld verdient

Auch Branchenkenner beobachten dieses Vorgehen. Im Gespräch mit Marktcheck berichtet einer von ihnen, dass er regelmäßig Fakeshops hinter Werbeanzeigen aufspüre und diese an Google melde. Aus Angst vor den Fake-Shop-Betreibern will er anonym bleiben. Nach seiner Erfahrung reagiere der Tech-Konzern auf die Meldungen oft **wochenlang** nicht, erzählt er. In der Zeit könnten zahlreiche Kunden weiterhin zu Betrugsopfern werden.

Er schätzt, dass im Jahr 2023 über 300 000 Menschen hierzulande Opfer von Fakeshops wurden – und der Schaden bei rund 100 Millionen Euro liegt. "Man kann ganz klar sagen, Google macht viel zu wenig", findet er. In seinen Augen verspiele der Konzern damit das Vertrauen der Verbraucher. Warum Google oft so lange nichts mache – diese Frage stelle er sich häufig: "Meine einzige Erklärung ist, dass sie damit **Geld verdienen** - und das fahrlässig in Kauf nehmen. Und vielleicht ist es ist ihnen egal."

### Kartellrechtsexperte sieht den Internetgiganten in der Pflicht

Macht der Suchmaschinen-Gigant Google es Betrügern wirklich so einfach? Während der Recherche macht Marktcheck eine **Stichprobe** und lässt den Branchenkenner nach Hochdruckreinigern suchen. Dabei soll sich zeigen, ob auch gesponserte Produkte von Fakeshops angezeigt werden. Und tatsächlich: Auf 35 Werbeplätzen findet der Branchenkenner schon innerhalb kurzer Zeit acht Fakeshops – eine Quote von 25 Prozent bei dieser Stichprobe.

Der Insider erhebt **schwere Vorwürfe** gegen Google: Er schätzt, dass der Internetgigant rund 20 Millionen Euro allein mit Werbeanzeigen von Fakeshops einnehmen könnte. „Also Google verdient massiv an den Betrug mit, das ist der Skandal.“

Rechtsanwalt Professor Thomas Höppner war an vielen Kartellrechtsverfahren gegen Google beteiligt, auch vor dem EuGH. Er kennt sich aus mit den Geschäftspraktiken des Konzerns. Geht es um bezahlte Anzeigen, die auf die Seiten von Fakeshops führen, sieht er Google durchaus in der Pflicht. Man könne durchaus erwarten, dass der Konzern genau prüfe, wessen Anzeigen auf der ersten Ergebnis-Seite angezeigt würden, sagt Professor Thomas Höppner: „Dass man also mit dieser prominenten Position, die man einzelnen Shops vergibt und mit der man Geld verdient, gleichzeitig auch die Verantwortung bekommt, genau hinzusehen und diejenigen auszusieben, bei den Endkunden definitiv nicht landen sollen.“

### Google selbst verweist auf seine strengen Richtlinien

Was sagt der Konzern selbst dazu? Wie kann es sein, dass auch gemeldete Fakeshops unter den gesponserten Produkten oftmals erst nach Wochen entfernt werden? Marktcheck konfrontiert Google mit den Ergebnissen der Recherche.

Das Unternehmen schreibt: „Der Schutz unserer Nutzer*innen hat für uns oberste Priorität. Wir haben strenge **Anzeigenrichtlinien**, die festlegen, welche Arten von Anzeigen und

Werbetreibenden wir auf unseren Plattformen zulassen. Wir setzen unsere Richtlinien rigoros durch, und wenn wir Anzeigen finden, die dagegen verstoßen, entfernen wir sie. (...)"

Auf die Frage nach den geschätzten Werbe-Einnahmen durch Werbeanzeigen zu Fakeshops von rund 20 Millionen geht Google allerdings nicht ein. Und auch die Frage, warum gemeldete Fakeshops häufig erst nach einiger Zeit aus den gesponserten Suchergebnissen verschwinden, bleibt offen.

### Tipp: Erkennen, ob ein Shop im Internet seriös ist – oder Betrug

Fakeshop im Netz locken Kundinnen und Kunden häufig mit besonders günstigen Angeboten auf ihre Seite – und mit professionellem Erscheinungsbild. Laut Verbraucherzentrale sind viele dubiose oder betrügerische Seiten oft Kopien von Websites oder Shops, die es wirklich gibt. Auch AGBs – also Allgemeine Geschäftsbedingungen – oder das Impressum können kopiert sein.

**Folgende Kriterien können erste Anzeichen für Betrug sein:**

- Eine bekannte Internetadresse wurde leicht abgewandelt – zum Beispiel endet die Domain auf „.info“ statt auf „.de“
- Beim Bestellvorgang des Internetshops wird am Ende nur noch Vorkasse (Überweisung) akzeptiert
- Auf bekannten Bewertungsportalen, in Sozialen Medien oder Foren gibt es keine Bewertungen – auf der eigenen Internetseite des Shops dagegen nur positive
- Der Name der Seite passt nicht zu den angebotenen Produkten
- Ist kein Impressum vorhanden, sollte das skeptisch machen. Im Impressum müssen unter anderem eine Adresse und Email-Adresse angegeben sein, die überprüft werden können. Auch eventuelle Handelsregisternummern kann man überprüfen
- Wird eine Bestellung durchgeführt, erhält man keine (korrekte) Bestellbestätigung
- Angegebene Bankverbindungen sind ungewöhnlich, liegen z.B. im Ausland

Die Verbraucherzentralen bieten eine Seite an, über die Internetadressen überprüft werden können: Hier geht es zum Fakeshop-Finder.

### Hintergrund: Problem betrifft auch Plattformen wie Facebook oder Instagram

Auch über Werbeanzeigen bei anderen großen Internetkonzernen geraten Userinnen und User übrigens auf betrügerische Internetseiten. Unter den Anzeigen bei Facebook Instagram oder Tiktok etwa finden sich ebenfalls Links zu unseriösen oder falschen Shops, Abo-Fallen oder dubiosen Investment-Angeboten.

Auf der österreichischen Seite onlinesicherheit.at, betrieben vom Kanzleramt Österreich und dem A-SIT Zentrum für sichere Informationstechnologie Austria, wird davor gewarnt – und darauf hingewiesen, dass das Problem weit verbreitet sei. Auch hier wird die Frage aufgeworfen, warum die Plattformbetreiber so wenig gegen unseriöse Anzeigen unternehmen. „Der Grund dafür ist einfach: Das Anzeigengeschäft rentiert sich“, heißt es als Antwort auf der Ratgeberseite des Zentrums für sichere Informationstechnologie Austria. Schwere Vorwürfe, die da gegen Plattformanbieter wie Facebook, Instagram und Tiktok erhoben werden.

Zwar gebe es demnach seitens der Betreiber großer sozialer Medien halbherzige Versuche, die Flut von unseriösen Anzeigen mittels Algorithmen und Meldemechanismen einzudämmen, doch dies geschehe nur mit geringem Erfolg. „Selbst die von Nutzerinnen und Nutzern gemeldeten Anzeigen bleiben in vielen Fällen online – obwohl die Plattformen rechtlich verantwortlich für betrügerische Inhalte werden, sobald sie von ihnen Kenntnis erhalten.“

**Tipp: Was tun, wenn man auf einen Fakeshop hereingefallen ist?**

Haben Sie etwas bestellt, aber keine Bestellbestätigung erhalten? Kommt die Ware nicht bei Ihnen an? Oder sind Ihnen einfach Zweifel gekommen? Viele Menschen werden Opfer von Fakeshops. Das Bundesinstitut für Sicherheit in der Informationstechnik (BSI) und die Verbraucherzentrale haben zentrale Ratschläge erarbeitet, was in diesem Fall zu tun ist:

- Wenn möglich, sollte man die Zahlung stoppen – deshalb so schnell wie möglich die eigene Bank kontaktieren. Überweisungen lassen sich in der Regel nicht zurückrufen, beim Lastschriftverfahren allerdings kann die Zahlung noch bis zu acht Wochen später zurückerstattet werden.
- Alle Belege sammeln und sichern – also zum Beispiel mögliche eMails, Screenshots von den Internetseiten des Fakeshops.
- Bei Verdacht auf Betrug sollte Strafanzeige bei der Polizei erstattet werden. Das geht auch Online bei den Onlinewachen der Polizeien der Bundesländer. Die Polizei kann nur dann strafrechtlich gegen die Betreiber von Fakeshops vorgehen, wenn eine Anzeige von einer oder einem Geschädigten vorliegt.

**Inzwischen gibt es auch Möglichkeiten, Fakeshops und Betrugsfälle online zu melden:**

- Über die Informationsplattform Watchlist Internet können unseriöse Webseiten und neue Fake-Shops gemeldet werden.
- Auch auf der Seite HinweisHelden.com werden Betrugsfälle gesammelt. Diese Meldungen werden dann an die zuständigen Plattformen und Website-Hosts weitergegeben.

Quelle: https://www.swr.de/verbraucher/ard-marktcheck/fakeshops-in-google-ads-100.html

# 10) Spam-Liste für September – Diese Telefonnummern sollten Sie unbedingt blockieren

**Betrüger locken am Telefon mit hohen Geldsummen und angeblichen Gewinnspielen. Wer sichergehen will, sollte diese Nummern sofort blockieren.**

Telefonbetrüger versuchen derzeit wieder verstärkt, mit angeblichen Gewinnspielen zu locken. Wie die Firma "Clever Dialer" mitteilt, meldeten sich zahlreiche Betroffene, denen von unbekannten Anrufern horrende Geldsummen versprochen wurden. Die Masche der Trickbetrüger wird dabei immer dreister. So stellten einige Betrüger sogar eine vermeintliche Bargeldlieferung bis an die Haustür in Aussicht.

Die App von Clever Dialer ("cleverdialer.app") hilft dabei, lästige und betrügerische Anrufe zu erkennen und abzuwehren. Jeden Monat veröffentlicht t-online die fünf am häufigsten gemeldeten Spam-Nummern, damit Sie sich als Nutzer sich besser schützen können.

**Die dreisten Maschen der Betrüger**

An der Spitze der Liste steht eine deutsche Handynummer, die bereits über 500-mal von anderen Nutzern blockiert wurde. Ein Betroffener berichtet zum Beispiel davon, dass der Anrufer versucht habe, ihm ein "Ja" zu entlocken – ein klares Zeichen für eine Kostenfalle. Auch Spam-Anrufe aus den Niederlanden würden nach Angaben der Nutzer mehrmals in der Woche und zu allen möglichen Tageszeiten erfolgen.

Besonders dreist sind Anrufer, die angeblich 39.000 Euro in bar liefern wollen. Der Haken: Vorher soll eine "Gebühr" von 900 Euro überwiesen werden. Andere Betrüger bieten ein "Projekt-Schutz-Paket" für 45 Euro an, bevor der vermeintliche Gewinn ausgezahlt wird.

(Quelle: Clever Dialer)

**Hier die Nummern noch einmal als Text, damit Sie diese per Copy-and-paste übertragen können:**

- 01521 9225837 (Kostenfalle)
- +31 6 44906164 (Kostenfalle)
- 01521 9466469 (Kostenfalle)
- +31 6 49434471 (Kostenfalle)
- 01525 8300453 (Kostenfalle)

### So können Sie eine Telefonnummer blockieren

Wie Sie eine Nummer auf Ihrem Mobiltelefon sperren können, erfahren Sie in dieser Anleitung. Grundsätzlich gilt: Geben Sie niemals persönliche Informationen wie Adressen, Kontonummern oder Passwörter am Telefon an Unbekannte weiter. Wenn Sie dazu aufgefordert werden, sollten Sie das Gespräch sofort beenden.

Lesen Sie hier auch: Was Sie nie zu Fremden am Telefon sagen sollten.

**Tipp:**

Spam-Liste für Oktober: Diese Telefonnummern sollten Sie sofort blockieren

*Alle Daten wurden vom Telefonspam-Check des Anbieters Clever Dialer bereitgestellt.*

Quelle:https://www.t-online.de/digital/aktuelles/id_100485530/spam-anrufe-blockieren-diese-nummern-drohen-im-september.html

# Anwenderinformationen:

## 1) Spam-Flut in Deutschland – E-Mail-Anbieter filtern 1,9 Milliarden Nachrichten pro Woche

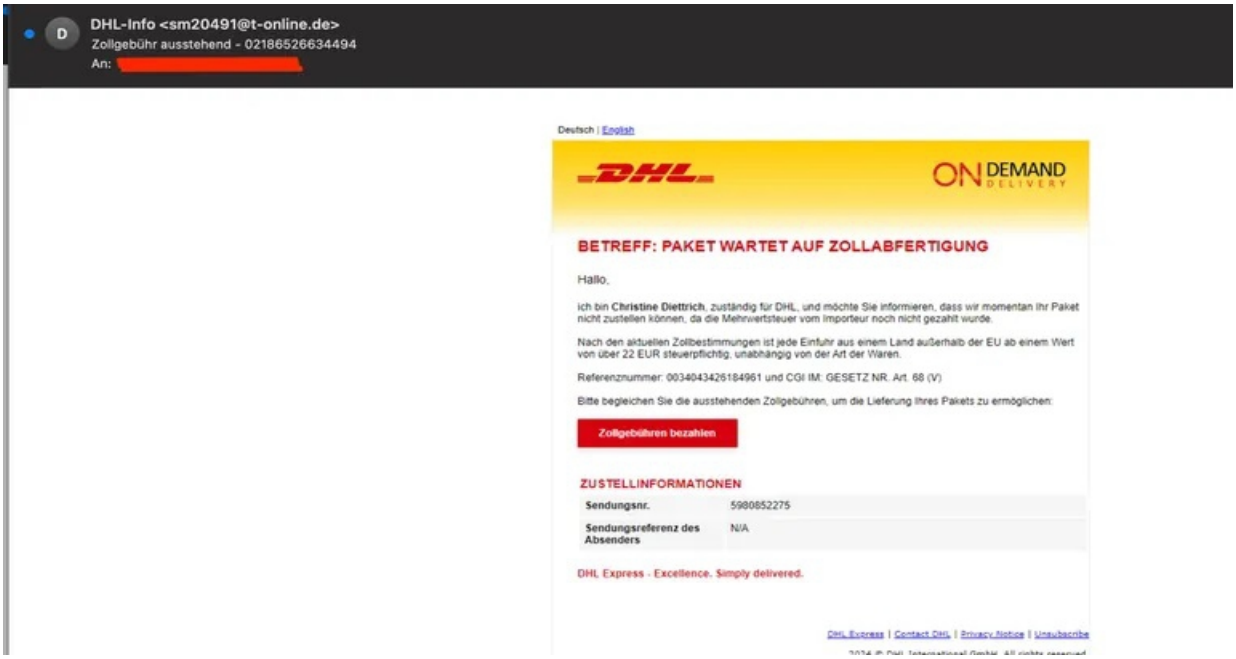
**Die Spam-Flut in deutschen E-Mail-Postfächern nimmt zu. Besonders gefährlich sind gefälschte Nachrichten von Paketdiensten – die Anbieter reagieren mit besonderen Tricks.**

Die beiden größten deutschen E-Mail-Anbieter, web.de und GMX, haben im dritten Quartal 2024 rund 1,9 Milliarden Spam-Mails pro Woche registriert. Das entspricht einem Anstieg von 35 Prozent im Vergleich zum Vorjahreszeitraum, als wöchentlich etwa 1,4 Milliarden solcher Nachrichten gefiltert wurden. Besonders auffällig sind dabei gefälschte E-Mails von Paketunternehmen sowie falsche Kundenservice-Nachrichten.

Laut einer gemeinsamen Pressemitteilung der beiden Unternehmen, die zu United Internet gehören, stammen die Spam-Mails nicht mehr nur von missbrauchten Accounts großer Anbieter wie Microsoft oder Gmail. "Wir sehen aktuell, dass die Angreifer in die Systeme kleiner und mittelständischer Cloud- und Hosting-Anbieter im europäischen Ausland eindringen", erklärt Arne Allisat von web.de und GMX.

### Gefälschte Paketdienst-Mails als häufigste Betrugsmasche

Besonders häufig täuschen die Betrüger Nachrichten von Paketdiensten wie DHL, Hermes oder DPD vor. Die gefälschten E-Mails informieren die Empfänger über angeblich im Zoll festgehaltene Pakete. Über einen Link sollen die Nutzer eine Bearbeitungsgebühr bezahlen, damit das Paket weitergeleitet wird. Der Link in der Mail führt jedoch zu einer betrügerischen Seite, über die Online-Kriminelle Geld und persönliche Daten abgreifen.



Gefälschte E-Mail von DHL: Das sogenannte Paketdienst-Phishing ist eine derzeit beliebte Betrugsmasche. Quelle WEB.DE

Eine weitere beliebte Masche ist das "Kundenservice-Phishing", bei dem sich die Betrüger als Kundendienst des E-Mail-Anbieters ausgeben und die Nutzer auffordern, sich über einen Link in ihren Account einzuloggen. Dadurch erhalten die Betrüger Zugriff auf weitere E-Mail-Konten, die sie für Spam-Versand oder Online-Shopping missbrauchen.

### Künstliche Intelligenz hilft bei der Abwehr

Bei der Bekämpfung der Spam-Flut setzen die E-Mail-Anbieter verstärkt auf den Einsatz Künstlicher Intelligenz. "KI hat die Spam-Welt in den letzten beiden Jahren radikal verändert – für die Angreifer, aber auch bei uns auf der Verteidigerseite", erklärt Allisat. Demnach könnten die KI-gestützten Analysesysteme innerhalb von Millisekunden entscheiden, wie viele E-Mails ein Absender-Server in einer bestimmten Zeit versenden darf. Ein plötzlicher Anstieg dieser Menge sei ein deutlicher Hinweis auf Spam-Versand.

Ein weiterer wichtiger Baustein der Spam-Abwehr ist die sogenannte "Reject and Defer Policy". Dabei wird die Zustellung verdächtiger E-Mails bereits beim Verbindungsaufbau abgelehnt oder verzögert. Seriöse Absender versuchen es in diesem Fall später erneut.

Die Kriminellen stehen dagegen unter Zeitdruck, da sie den Zugriff auf gekaperte E-Mail-Server jederzeit wieder verlieren können. Daher versuchen sie, ihre Spam-Mails direkt beim ersten Mal zuzustellen. Dadurch gelingt es den Anbietern mit einer Erkennungsrate von 99,9 Prozent, fast alle betrügerischen Nachrichten zu erkennen und zu blockieren.

Quelle: https://www.t-online.de/digital/aktuelles/id_100512530/spam-mails-bei-web-de-und-gmx-anbieter-reagieren-mit-tricks.html

# 2) Aus für Share Mobile – Telekom-Tochter stellt Marke ein – das sollten Sie beachten

**Die Telekom-Tochter Congstar stellt ihre Prepaid-Marke Share Mobile ein. Kunden sollten handeln und sich nach alternativen Angeboten umsehen.**

Congstar stellt seine Prepaid-Marke Share Mobile ein. Das zur Telekom gehörende Unternehmen beendet das Angebot am 30. November 2024, wie Congstar auf seiner Seite mitteilt. Danach können Kunden der Marke mit ihrem Share-Mobile-Tarif weder telefonieren noch surfen.

Congstar hatte Share Mobile zusammen mit der sozialen Marke Share im vergangenen Jahr gestartet. Pro gebuchter Allnet-Flat wurde pro Monat ein Bildungsprojekt in Kenia mit einem Euro unterstützt. Die sogenannte "Tut Gutes Option" soll aber laut Congstar nicht eingestellt werden, heißt es.

### Können Kunden zu einem neuen Anbieter wechseln?

Stattdessen wollen beide Unternehmen die Option "ab 2025 für alle Congstar-Mobilfunktarife ermöglichen". Für bisherige Share-Mobile-Kunden bietet die Telekom-Tochter eine Wechselmöglichkeit zu Congstar an. Das Unternehmen verspricht Nutzern, die zu Congstar wechseln, dauerhaft monatlich 5 GB zu ihrem Tarif hinzuzubuchen.

Nutzern, die zu einem anderen Anbieter wechseln wollen, bietet Congstar eine Rufnummernmitnahme an – allerdings nur bis zum 28. Februar des kommenden Jahres. Erstattungen für bereits gekaufte Starterpakete oder Aufladekarten für Share Mobile will Congstar bis März 2027 ermöglichen. Die Karten gab es bei Rewe und der Drogeriemarkt-Kette dm.

### Was passiert mit gekauften und nicht aktivierten SIM-Karten?

Noch nicht genutzte SIM-Karten lassen sich laut Congstar seit dem 21. Oktober nicht mehr aktivieren. Ein Umtausch sei in den Filialen von Rewe und dm nicht möglich. Kunden sollten sich an die Congstar-Hotline wenden, heißt es.

In diesem Fall sollen Kunden laut Congstar die SIM-Kartennummer und den PUK1-Code bereithalten, der sich im Starterpaket befindet. Nachdem das Unternehmen die Daten geprüft hat, will es die Gutscheincodes für neue Congstar-Tarife per E-Mail verschicken.

Quelle: https://www.t-online.de/digital/aktuelles/id_100517340/congstar-stellt-share-mobile-ein-telekom-tochter-kuendigt-aus-fuer-marke-an.html

# 3) Verbesserter Datenschutz – Sparkassen-App bekommt Inkognito-Funktion

**Mit einem Inkognito-Modus erhöhen die Sparkassen bei ihrer App die Privatsphäre der Nutzer. Eine weitere Funktion wurde hinzugefügt.**

Die Sparkassen-App hat eine neue Funktion: den Inkognito-Modus. Das berichtet das Onlinemagazin "iPhone-ticker". In der Version 6.8.0 können Nutzer die Anzeige von Beträgen in der Anwendung verbergen, um diese vor neugierigen Blicken zu schützen.

Das kann sinnvoll sein, wenn Sparkassen-Kunden in der Bahn oder Tram ihre Kontobewegungen in der App prüfen wollen. Wenn der Inkognito-Modus eingeschaltet werde, seien statt der Geldbeträge fünf Punkte zu sehen, heißt es.

Die Funktion lasse sich über ein Augen-Symbol am linken oberen Rand der App aktivieren.

Wie "iPhone-ticker" weiter schreibt, seien in der neuen Version der Sparkassen-App weitere Neuerungen eingefügt worden. Dazu gehöre neben Leistungsverbesserungen auch die Möglichkeit, "ein Konto direkt in der App zu eröffnen".

## 2022 gab es das letzte große Update der App

Das letzte große Update erhielt die Sparkassen-App vor zwei Jahren mit Version 6.0 für Smartphones und Tablets. Ein neues Aussehen verbesserte die Bedienbarkeit der Anwendung.

Seitdem besitzt die Anwendung unter anderem neben einem Light Mode auch einen sogenannten Dark Mode. Anwender können das Programm seitdem in hellem oder dunklem Design nutzen. Die Nutzung im dunklen Design verbraucht weniger Strom und schont den Akku.

Auf der Startseite gibt es seit Version 6.0 außerdem eine Leiste für den Schnellzugriff auf Funktionen wie "Überweisung", "Filiale suchen" und "Karte sperren".

Mit der sogenannten Tab-Bar können Nutzer einfach in der App navigieren und Konten nach ihren Vorlieben sortieren. Die Navigation befindet sich auf der unteren Seite in der App. Auch ein persönlicher Kundenberater wird in der Anwendung angezeigt und lässt sich bei Bedarf kontaktieren.

Quelle: https://www.t-online.de/digital/aktuelles/id_100511758/sparkassen-app-bekommt-inkognito-funktion-verbesserter-datenschutz.html

# 4) Android 15 Update zerstört ältere Pixel-Smartphones – Keine Hilfe von Google

**Ältere Pixel-Geräte können offenbar durch das Update beschädigt werden. Nutzerberichte sprechen sogar von Totalausfällen. Das können Sie tun.**

**Update vom 28.10.**: Nach wie vor berichten Nutzer über Probleme mit Android 15. Pixel 6 Smartphones laufen nach wie vor Gefahr, durch das Update auf die neue Version nur noch einen schwarzen Bildschirm zu zeigen. Google äußerte sich bisher nicht öffentlich zu den Problemen und bietet Betroffenen nur kostspielige Reparaturen an. **Update Ende**

Vor Kurzem hat Google den Quellcode für Android 15 an Entwickler weitergegeben. Dadurch erhalten die ersten Smartphones die neue Version des Betriebssystems, wobei Googles eigene Pixel-Geräte als Erstes versorgt wurden. Gerade diese haben aber aktuell mit Problemen zu kämpfen.

Wie die Seite Android Police berichtet, kommt es auf älteren Pixel-Smartphones zu so erheblichen Schäden, dass sie nicht mehr benutzbar sind. Betroffen ist dabei vor allem das Pixel 6, aber die Auslöser sind unterschiedlich.

### Totalausfall durch Update

Einigen Nutzerberichten zufolge reicht oft das Update auf Android 15 allein schon aus, dass die Smartphones nicht mehr benutzbar sind. Bei anderen sorgte erst der Wechsel in den “Private Space”, also einer gesicherten Umgebung für Apps und sensible Daten, für einen Totalausfall.

Bei allen betroffenen Geräten hat das übliche Vorgehen, um das Smartphone wiederzubeleben, nicht geholfen. Weder ein Hard Reset noch das Anschließen an einen PC konnte die Pixel-Geräte zurück ins Leben holen, wie die Nutzer auf Reddit schreiben. Die Handys taugen nur noch als “Briefbeschwerer”.

### Ähnliche Probleme bei Android 14

Es ist leider nicht das erste Mal, dass ein Android-Update massive Probleme bereitet. Beim Wechsel auf Android 14 berichteten viele Nutzer ebenfalls über Schwierigkeiten, wobei damals eher Speicherprobleme und Datenverlust das Hauptthema war.

Generell ist ein Wechsel auf eine neue Version des Betriebssystems nicht ganz ohne Risiken, wenn Entwickler das Update nicht ausreichend getestet haben. Allerdings hätte Google ausreichend Zeit haben müssen, um solche Totalschäden zu vermeiden.

Android 15: Diese Smartphones bekommen als nächstes das Update

So reagieren Sie richtig

Aktuell ist nicht ausreichend geklärt, worin die Ursache des Problems liegt. Zwar haben alle betroffenen Nutzer zuvor auf Android 15 upgedatet, doch bei manchen viel das Gerät erst nach längerem Betrieb aus, während andere direkte Schäden bemerkten.

In jedem Fall muss sich Google die Problematik genau ansehen und möglichst bald eine Lösung finden. Bis dahin sollten Besitzer eines Google Pixel 6, die noch nicht auf Android 15 gewechselt sind, darauf vorerst verzichten.

- Wie kann man sein Smartphone vor den Problemen von Android 15 schützen?
- Was sind die Vorteile von Android 15 gegenüber älteren Versionen?
- Was sind die Auswirkungen von Android 15 auf die Leistung von Apps?
- Wie kann man sein Smartphone updaten, um die Sicherheitsfunktionen von Android 15 zu nutzen?
- Was sind die Hauptprobleme bei der Installation von Android 15 auf älteren Pixel-Smartphones?

Sollten Sie bereits Probleme haben, müssen Sie sich direkt bei Google melden und prüfen, ob es sich um einen Garantiefall handelt oder diese nicht mehr gültig ist. Im zweiten Fall kann Google möglicherweise nur eine kostenpflichtige Reparatur anbieten.

Alternativ können Sie auch ein neueres Pixel-Smartphone kaufen. Bei der aktuellen Pixel-9-Serie von Google konnten keine solchen Schäden festgestellt werden. Bei manchen Nutzern funktionieren nur ein paar Apps nicht richtig nach dem Update auf Android 15, was mittlerweile aber mit einem Patch behoben sein sollte.

Android 15 macht Apps unbrauchbar: Das können Sie tun

**Nicht nur Probleme**

Meldungen wie diese könnten den Eindruck erwecken, dass Android 15 ein Reinfall für die Nutzer ist. Da allerdings nur wenige von Problemen berichten, sollten Sie nicht gänzlich auf die neue Version verzichten, sobald sie für Sie verfügbar ist.

Android 15 bringt nämlich auch einige geniale Sicherheitsfunktionen auf Ihr Smartphone, auf die Sie nicht verzichten sollten. Dazu gehört etwa ein besserer Schutz für Zwei-Faktor-Authentifizierung. Um zu sehen, ob Ihr Gerät für Android 15 qualifiziert ist, hilft unsere Liste der wichtigsten Smartphones, die das Update erhalten.

Quelle: https://www.pcwelt.de/article/2498210/android-15-update-pixel-smartphones-kaputt-fehler.html?utm_date=20241028123049&utm_campaign=Best-of%20PC-WELT&utm_content=slotno7-title-Android%2015%20Update%20zerst%C3%B6rt%20%C3%A4ltere%20Pixel-Smartphones%20%E2%80%93%20Keine%20Hilfe%20von%20Google&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 5) Cyber Security Month im Oktober – So schützen Sie Ihre Daten und Ihr Geld im digitalen Dschungel

**Der Oktober steht im Zeichen der Cyber-Sicherheit. Wie Sie Ihre persönlichen Daten und auch Ihr Geld effektiv vor Missbrauch und Betrug im Internet schützen, erfahren Sie bei COMPUTER BILD.**

In einer Zeit, in der unser Leben zunehmend digital geprägt ist, wird der Schutz persönlicher Daten und finanzieller Mittel im Internet immer wichtiger. Das weltumspannende Datennetz bietet zahlreiche Möglichkeiten, birgt aber auch erhebliche Risiken. Cyberkriminelle entwickeln ständig neue Methoden, um an sensible Informationen zu gelangen oder finanzielle Schäden zu verursachen. Ein einziger Fehltritt im Web kann massive Auswirkungen auf das reale Leben haben, wenn Ihre Privatsphäre verletzt oder Ihr hart verdientes Geld gestohlen wird.

Doch keine Sorge! Mit dem Themenschwerpunkt "Sicherheit im Internet" legt COMPUTER BILD im Oktober den Fokus auf nützliche Ratgeber und spannende Hintergrundgeschichten. Diese helfen Ihnen, die Maschen der Kriminellen zu erkennen, sich effektiv dagegen zu wehren und im Idealfall deren Fallen großräumig zu umgehen. Tauchen Sie ein in die Welt der Cyber-Sicherheit und lernen Sie, wie Sie den Bedrohungen im Netz die Stirn bieten können:

**Ransomware: Schutz gegen digitale Geiselnahme**

Die Gefahr durch Ransomware-Angriffe bleibt aktuell und kann jeden treffen – ob Unternehmen oder Privatperson. Diese digitalen Erpresser verschlüsseln Ihre wertvollen Daten und fordern ein Lösegeld für deren Freigabe. Doch wie können Sie sich davor

schützen? Der Ransomware-Leitfaden unterstützt Sie bei der Abwehr solcher Bedrohungen. Erfahren Sie, wie moderne Antiviren-Programme mit speziellen Funktionen wie Zugriffsbeschränkungen auf private Ordner und automatischen Sicherheitskopien Sie schützen können. Entdecken Sie Tools wie den COMPUTER BILD-Erpresserviren-Stopper, der verdächtige Aktivitäten erkennt und Ihren PC präventiv in den abgesicherten Modus versetzt. Falls Sie bereits Opfer eines Angriffs geworden sind, zeigt COMPUTER BILD Schritt für Schritt, wie Sie vorgehen sollten – von der Nutzung von Notfall-Systemen bis hin zur Möglichkeit, kostenlose Entschlüsselungs-Tools (Decryptors) zu finden. Erfahren Sie auch mehr über die neuesten Trends, wie etwa Ransomware-as-a-Service oder die Drohung, erbeutete Daten zu veröffentlichen, und warum in den meisten Fällen von einer Lösegeldzahlung abgeraten wird.

**Sicherheitslücken: Einfallstor für Malware**

Sicherheitslücken sind wie unauffällige Hintertüren in der digitalen Welt, durch die ungebetene Gäste eintreten können. Diese Schwachstellen in Software, Betriebssystemen oder sogar Firmware können schwerwiegende Folgen haben. COMPUTER BILD erklärt in einem umfassenden Ratgeber, wie Sicherheitslücken entstehen, welche Auswirkungen sie haben können und vor allem, wie Sie sich davor schützen. Erfahren Sie mehr über die Gefahren von Zero-Day-Lücken und warum regelmäßige Updates der wichtigste Schutz sind. Der Ratgeber beleuchtet auch die Rolle von Antivirus-Programmen bei der Abwehr von Angriffen durch Sicherheitslücken und gibt praktische Tipps, wie Sie Ihre Geräte, von PCs bis hin zu smarten Haushaltsgeräten, bestmöglich absichern können. Entdecken Sie, warum es sich lohnt, regelmäßig die Herstellerseiten auf Firmware-Updates zu überprüfen und wie Sie mit Software- oder Treiber-Updater-Tools Ihre digitale Sicherheit erhöhen können.

**Identitätsdiebstahl: So schützen Sie Ihr virtuelles Ich**

Cyberkriminelle sind ständig auf der Lauer, um persönliche Daten zu stehlen und für betrügerische Zwecke zu missbrauchen. Welche Risiken bestehen und wie Sie sich effektiv schützen können, erläutert der Ratgeber über Identitätsdiebstahl. Erfahren Sie, welche Schritte Sie unternehmen sollten, wenn Ihre Online-Identität bereits kompromittiert wurde – von der Kontaktaufnahme mit Zahlungsdiensten über die Einrichtung einer Kreditsperre bei der SCHUFA bis hin zur Erstattung einer Anzeige bei der Polizei. Der Ratgeber beleuchtet auch die verschiedenen Methoden, die Hacker nutzen, um an Ihre Daten zu gelangen, sei es durch Schadsoftware, Angriffe auf Websites oder Phishing. COMPUTER BILD gibt praktische Tipps, wie Sie Ihre digitale Identität präventiv schützen können, etwa durch die Nutzung von Passwort-Managern, Zwei-Faktor-Authentifizierung und den vorsichtigen Umgang mit persönlichen Daten im Internet. Entdecken Sie zudem, wie Sie die Kontrolle über Ihre digitale Identität zurückgewinnen und zukünftige Angriffe verhindern können.

**Sicherheit im Urlaub: Online-Schutz unter Palmen**

Die Vorfreude auf den Urlaub ist groß, doch die digitale Welt schläft auch in der Ferne nie. Cyberkriminelle haben Reisende besonders im Visier und locken mit verlockenden Angeboten in gefährliche Fallen. Mit den IT-Security-Tipps für Ihren Urlaub verlieren Sie auch in der entspannten Zeit des Jahres Ihre digitale Sicherheit nicht aus den Augen. Erfahren Sie, wie Sie sich vor Betrug bei der Buchung von Unterkünften schützen, welche Vorsichtsmaßnahmen in öffentlichen WLANs nötig sind und warum Sie behutsam mit öffentlichen Ladestationen umgehen sollten. Der Ratgeber deckt ein breites Spektrum ab: vom Schutz vor Diebstahl über den sicheren Umgang mit QR-Codes bis hin zu Vorsichtsmaßnahmen beim Online-Banking im Ausland. Entdecken Sie, warum es ratsam ist, Bluetooth zu deaktivieren, wenn Sie es nicht nutzen, und weshalb Sie in Internet-Cafés besonders vorsichtig sein sollten. Mit praktischen Tipps wie der Nutzung von Passwort-

Managern, der Installation von Updates vor der Reise und dem Schutz vor neugierigen Blicken in öffentlichen Verkehrsmitteln stellt COMPUTER BILD sicher, dass Sie gut vorbereitet in den Urlaub starten.

**Fake-Shops: Echte Schnäppchen oder fiese Falle?**

Ein verlockendes Angebot in einem unbekannten Online-Shop entdeckt? Bevor Sie zugreifen, sollten Sie einen Moment innehalten. COMPUTER BILD erklärt, warum nicht alle Schnäppchen echt und nicht alle Online-Shops seriös sind. Nutzen Sie den Fakeshop-Finder, ein cleveres Tool der Verbraucherzentrale NRW, das Sie vor Betrug schützt. Dieses Prüf-Tool hilft Ihnen, betrügerische Shops zu enttarnen, bevor Ihr Geld unwiederbringlich verloren geht. Erfahren Sie, wie der Fakeshop-Finder mithilfe künstlicher Intelligenz und eines Ampelsystems die Seriosität eines Online-Shops schnell und einfach überprüft. COMPUTER BILD gibt Ihnen zusätzliche Tipps, wie Sie selbst Fake-Shops erkennen können – von der Überprüfung der Bezahlwege bis hin zur Analyse der Website auf Ungereimtheiten. Entdecken Sie, warum Fake-Shops besonders bei knappen Waren auftreten und wie sie mit gut gemachten Webseiten täuschen. Mit dem Wissen, dass der jährliche Schaden durch Fake-Shops Millionenhöhe erreicht, wird deutlich, wie wichtig Vorsicht beim Online-Shopping ist.

**Banking-Betrug: Es geht um Ihr Geld**

Online-Banking ist bequem – zweifellos. Doch gerade hier wird es richtig teuer, wenn Sie Cyberkriminellen in die Falle tappen. COMPUTER BILD erklärt, wie sicheres Online-Banking funktioniert und welche Vorsichtsmaßnahmen Sie treffen sollten. Erfahren Sie, wie das von Ihnen genutzte Betriebssystem Ihre Sicherheit beeinflusst: iOS gilt als relativ sicher, Windows lässt sich gut absichern, während von Online-Banking auf Android-Geräten derzeit abgeraten wird. Entdecken Sie, warum die Wahl Ihrer Bank entscheidend für die Sicherheit ist und welche Authentifizierungsmethoden als besonders zuverlässig gelten. Der Ratgeber beleuchtet auch die Gefahren durch Phishing und Banking-Trojaner und gibt praktische Tipps, wie Sie sich davor schützen können. Von der Nutzung offizieller Banking-Apps über die Überprüfung von Browser-Adressen bis hin zur Einrichtung von Tageslimits – COMPUTER BILD liefert konkrete Handlungsempfehlungen für Ihr finanzielles Wohlergehen im digitalen Raum. Lernen Sie, wie Sie verdächtige Aktivitäten erkennen und im Zweifelsfall richtig reagieren.

Quelle: https://www.computerbild.de/artikel/cb-News-Sicherheit-Cyber-Security-Monat-Oktober-36800655.html

# 6) Ratgeber – Diese 20 Tastenkombinationen für Windows 11 müssen Sie kennen

**Selbst nach vielen Jahren mit sämtlichen Windows-Versionen gibt es noch immer viele unbekannte Tastaturkürzel, die den PC-Alltag schneller und komfortabler machen können. Eine Auswahl der nützlichsten Hotkeys für Windows 11.**

Als langjähriger Windows-Freak liebe ich Tastenkombinationen. Diese Hotkeys sind wie eine Sammlung geheimer Handzeichen, mit denen Sie schnell nützliche Aufgaben ausführen und die Arbeit an Ihrem PC erheblich beschleunigen können.

Und ja, Tastenkombinationen sind ziemlich geheim. Windows bietet Ihnen keinen Coach, der Sie durch die Hunderte von Hotkeys führt, die Sie nützlich finden könnten. Sie sind einfach da und warten im Hintergrund darauf, aktiviert zu werden.

Wir zeigen Ihnen die besten und praktischsten Tastaturkürzel, die Sie mit Sicherheit zukünftig nutzen werden.

### 1. Datei-Explorer starten

Wenn Sie so arbeiten wie ich, werden Sie den Datei-Explorer von Windows wahrscheinlich häufig aufrufen. Mit einem Tastaturkürzel haben Sie ihn immer griffbereit. Drücken Sie einfach die **Windows-Taste + E**, um ein neues Datei-Explorer-Fenster zu öffnen, wann immer Sie es benötigen.

### 2. Direkt zum Task-Manager wechseln

Wahrscheinlich kennen Sie die Tastenkombination Strg + Alt + Entf, aber wenn Sie damit den Task-Manager öffnen wollen, gibt es einen besseren Weg: Verwenden Sie stattdessen die Tastenkombination **Strg + Umschalt + Esc**.

### 3. Öffnen Sie die Einstellungen-App

Sie möchten eine Einstellung des Betriebssystems ändern? Normalerweise erledigen Sie das über die Einstellungen-App. Anstatt das Startmenü zu durchsuchen, können Sie auch eine Tastenkombination verwenden: **Windows-Taste+ I**. Dann können Sie direkt in der Einstellungen-App nach dem suchen, was Sie brauchen.

### 4. Durchsuchen Sie den Verlauf der Zwischenablage

Wussten Sie, dass Windows jedes Mal, wenn Sie ein Bild oder einen Text in die Zwischenablage kopieren, einen Verlauf speichert? Die übliche Tastenkombination Strg+V fügt nur das ein, was Sie zuletzt kopiert haben. Wollen Sie etwas einfügen, das Sie viel früher kopiert haben, können Sie das ebenfalls tun!

Sie müssen nur den Verlauf der Zwischenablage mit dem Tastaturkürzel **Windows-Taste + V** aufrufen. Beachten Sie: Wenn Sie die Zwischenablage noch nie geöffnet haben, werden Sie um Erlaubnis gebeten, die Funktion zu aktivieren.

Das Schöne am Verlauf der Zwischenablage ist, dass Sie bestimmte kopierte Objekte sogar an das Bedienfeld anheften können, damit Sie sie in Zukunft schnell wiederfinden.

**Mehr dazu lesen**: Windows-Zwischenablage clever nutzen – So geht's mit dem Zwischenablageverlauf

### 5. Emojis überall einfügen

Ob Sie sie lieben oder hassen, Emojis sind Teil der modernen Kommunikation geworden − und Microsoft weiß das. Deshalb macht es Ihnen Windows leicht, Emojis in fast jeder Anwendung einzugeben.

Alles, was Sie tun müssen, ist, die Tastenkombinationen **Windows-Taste + Punkt** oder **Windows-Taste + Semikolon** zu drücken. Verwenden Sie dann das Suchfeld, um das gewünschte Emoji zu finden (oder blättern Sie einfach durch).

### 6. Tippen Sie mit Ihrer Stimme

Mit Windows können Sie in fast jeder Anwendung Text mit Ihrer Stimme eingeben. Um die Oberfläche für die Spracheingabe aufzurufen, drücken Sie einfach die **Windows-Taste + H.** Sie sehen dann ein schwebendes Fenster (bei Windows 11) oder eine Leiste (bei Windows 10).

Diese Funktion nennt sich Spracheingabe. Über das Einstellungsmenü in dem Fenster/der Leiste können Sie Funktionen wie die automatische Zeichensetzung aktivieren. In der Standardeinstellung müssen Sie Wörter wie “Punkt” sprechen, während Sie den Text diktieren.

### 7. Entdecken Sie das Power-User-Menü

Als Microsoft das Startmenü in Windows 8 abgeschafft hat, war man wenigstens so höflich, den Power-Usern ein verstecktes “Power-User-Menü” mit schnellem Zugriff auf verschiedene Systemeinstellungen zu bieten.

Und obwohl Windows 10 das Startmenü zurückgebracht hat − das auch in Windows 11 weiterbesteht − ist das Power-User-Menü nie verschwunden. Um es zu öffnen, drücken Sie die **Windows-Taste + X** oder klicken Sie mit der rechten Maustaste auf die Schaltfläche Start.

### 8. Sperren Sie Ihren Computer

Um Ihren Computer vor unbefugtem Zugriff zu schützen – vor allem in einer Umgebung wie einem Büro oder auf dem Campus – sollten Sie Ihren Computer sperren, sobald Sie sich entfernen. Um Ihren PC schnell zu sperren, drücken Sie einfach das Tastaturkürzel **Windows-Taste + L**.

### 9. Sound-Einstellungen kontrollieren

Wenn Sie mehrere Tonausgabegeräte wie Lautsprecher, Kopfhörer und drahtlose Ohrhörer oder mehrere Toneingabegeräte wie Laptop-Mikrofon, Headset und externes Mikrofon besitzen, wechseln Sie wahrscheinlich häufig zwischen diesen Geräten.

Nun, Sie müssen nicht tief in die Einstellungen-App gehen, um zwischen ihnen zu wechseln. Sie können auch einfach die Tastenkombination **Strg+Windows-Taste+V** drücken, um das Menü für die Soundeinstellungen aufzurufen.

Es ist auch eine Abkürzung zum Anpassen der Systemlautstärke und der Lautstärke pro Anwendung (mit den Schiebereglern) und eine schnelle Möglichkeit, den Abschnitt Sound in der Einstellungen-App zu öffnen (indem Sie auf **Weitere Lautstärkeeinstellungen** klicken).

***Diese Funktion ist neu in Windows 11 und daher in Windows 10 nicht verfügbar.***

### 10. Fenster anheften

Die Snap-Funktion ist ein wichtiges Fensterverwaltungs-Tool für das Multitasking in Windows 11. Sie können App-Fenster ganz einfach mithilfe Ihrer Tastatur an den Bildschirmrändern einrasten.

Verwenden Sie zunächst die **Windows-Taste + Pfeil nach links** und die **Windows-Taste + Pfeil nach rechts**, um das aktuell fokussierte Fenster entweder in der linken oder in der rechten Hälfte des Bildschirms auszurichten. Ähnlich verfahren Sie mit der **Windows-Taste + Alt + Pfeil + nach oben** und der **Windows-Taste + Alt + Pfeil nach unten**, um Fenster in der oberen beziehungsweise unteren Hälfte des Bildschirms zu platzieren.
Sie können auch Tastenkombinationen verwenden, um Fenster in Quadranten des Bildschirms zu verschieben. Wenn Sie zum Beispiel ein Fenster in der linken Hälfte des Bildschirms einrasten lassen (mit der oben genannten Tastenkombination), halten Sie die **Windows-Taste** gedrückt und tippen Sie auf den **Pfeil nach oben**, um es im linken oberen Quadranten einzurasten.

### 11. Snap Layouts aktivieren

Als ob das Einrasten selbst nicht schon nützlich genug wäre, verfügt Windows 11 auch über eine zusätzliche Funktion zum Einrasten von Layouts, die das Einrasten von Fenstern in verschiedenen Konfigurationen erleichtert.

Um Snap Layouts zu aktivieren, verwenden Sie das Tastaturkürzel **Windows-Taste + Z**. Sie sehen ein Pop-up-Fenster mit nummerierten Optionen. Drücken Sie einfach die entsprechende Zifferntaste, um das entsprechende Fensterlayout auszuwählen.

Sie können die Snap-Layouts auch anzeigen, indem Sie den Mauszeiger über die Schaltfläche Maximieren eines Fensters bewegen. Oder ziehen Sie ein beliebiges Fenster an den oberen Rand des Bildschirms, um die Optionen für das Snap-Layout anzuzeigen.

### 12. Umschalten zwischen Fenster- und Vollbildmodus in PC-Spielen

Viele PC-Spiele bieten sowohl den Fenster- als auch den Vollbildmodus. Wenn Sie zwischen diesen beiden Modi umschalten möchten, kann es ziemlich mühsam sein, zum Einstellungsmenü des Spiels zu navigieren – vor allem, wenn Sie dies häufig tun.

Hier ist ein schnellerer Weg, um in vielen PC-Spielen zwischen dem Fenster- und dem Vollbildmodus zu wechseln: Drücken Sie einfach **Alt + Enter**. Das funktioniert nicht bei jedem Spiel, aber bei vielen. Ich versuche es immer als Erstes, wenn ich zwischen dem Vollbild- und dem Fenstermodus wechseln möchte.

### 13. Zwischen virtuellen Desktops springen

Windows 11 verfügt über eine Funktion namens Task View, mit der Sie “virtuelle Desktops” erstellen, zwischen denen Sie wechseln können. Ein virtueller Desktop ist wie eine separate Instanz des Desktops. Jeder virtuelle Desktop kann eine eigene Gruppe von laufenden Anwendungsfenstern enthalten.

Es gibt mehrere Tastenkombinationen für die Task-Ansicht, wie die **Windows-Taste + Tab**, mit der Sie leicht neue virtuelle Desktops erstellen, bestehende löschen und zwischen ihnen wechseln können.

Wenn Sie jedoch einige virtuelle Desktops erstellt haben, können Sie noch einfacher zwischen ihnen wechseln, indem Sie die Tastenkombinationen **Windows-Taste + Strg + Pfeil nach links** und **Windows-Taste + Strg + Pfeil nach rechts** verwenden.

### 14. Fenster zwischen Monitoren verschieben

Haben Sie einen weitläufigen Arbeitsplatz mit mehreren Monitoren? Sie können Fenster von einem Bildschirm zum nächsten verschieben, indem Sie die **Windows-Taste + Umschaltpfeil nach links** (um das aktuell fokussierte Fenster auf den linken Bildschirm zu verschieben) oder die **Windows-Taste + Umschaltpfeil nach rechts** (um das aktuell fokussierte Fenster auf den rechten Bildschirm zu verschieben) drücken.

### 15. Öffnen Sie sofort das klassische Datei-Explorer-Kontextmenü

In Windows 11 hat sich der Datei-Explorer im Vergleich zu früher stark verändert, insbesondere durch ein optimiertes Kontextmenü. Einige Optionen sind jedoch nur in diesem klassischen, altmodischen Kontextmenü zu finden.

Anstatt erst das Kontextmenü zu öffnen und dann die Option **Weitere Optionen anzeigen zu** wählen (oder sogar die Windows-Registry bearbeiten), können Sie auch einfach eine Tastenkombination verwenden, um das alte Kontextmenü sofort zu öffnen: Halten Sie die **Umschalttaste** gedrückt, während Sie im Datei-Explorer mit der rechten Maustaste klicken, um das klassische Kontextmenü zu sehen.

***Diese Funktion ist neu in Windows 11 und steht daher in Windows 10 nicht zur Verfügung.***

### 16. Schnelleres Bearbeiten von Text

Die Strg-Taste ist eine meiner Lieblingstasten, wenn es um die schnelle Textbearbeitung geht. Kurz gesagt, wenn Sie die **Strg-Taste** gedrückt halten, wirken die meisten Tasten auf ganze Wörter und nicht auf einzelne Zeichen.

Die Rücktaste zum Beispiel löscht das vorherige Zeichen, aber **Strg + Rücktaste** löscht das vorherige Wort. Ein anderes Beispiel: **Pfeil nach links** und **Pfeil nach rechts** bewegen den Cursor um ein Zeichen, aber **Strg + Pfeil nach links** und **Strg + Pfeil nach rechts** bewegen den Cursor von Wort zu Wort.

Und das funktioniert auch mit der Umschalttaste. Wenn Sie die Umschalttaste gedrückt halten, können Sie Text markieren, während sich der Cursor bewegt. Wenn Sie also schnell mehrere Wörter in einer Reihe markieren möchten, **halten Sie** einfach **die Umschalttaste gedrückt** und **tippen Sie** dann **auf die Pfeile nach links und rechts**. Versuchen Sie einmal, die Umschalttaste zusammen mit der Start- und Endtaste gedrückt zu halten, um ganze Textzeilen mit nur wenigen Tastenanschlägen zu markieren!

### 17. Eine geschlossene Browser-Registerkarte wieder öffnen

Alle modernen Webbrowser − einschließlich Chrome, Firefox, Opera und Edge − ermöglichen es Ihnen, geschlossene Registerkarten schnell wieder zu öffnen. Das ist auch leicht zu merken: Wenn Sie mit der Tastenkombination **Strg + T** eine neue Registerkarte erstellen, können Sie mit der Tastenkombination **Strg + Umschalt + T** die zuletzt geschlossene Registerkarte wieder öffnen.

### 18. Alt + Tab in umgekehrter Reihenfolge

**Alt + Tab** ist eine der kultigsten Windows-Tastenkombinationen. Wenn Sie jedoch viele Fenster geöffnet haben, die Sie durchlaufen müssen, kann es manchmal sinnvoller sein, den Zyklus umzukehren. In diesem Fall drücken Sie einfach **Shift + Alt + Tab**, um *rückwärts* durch die Liste der geöffneten Fenster zu gehen.

Und das ist noch nicht alles: Während das Dialogfeld Alt + Tab geöffnet ist, können Sie auch die **Pfeiltasten** verwenden, um sofort zum Fenster der ausgewählten Miniaturansicht zu springen.

### 19. Dateien schnell umbenennen

Sie möchten eine Datei schnell umbenennen? Wenn Sie eine Datei im Datei-Explorer ausgewählt haben, drücken Sie einfach **F2**, geben den Namen ein und drücken die Eingabetaste.

Ich navigiere gerne mit den Pfeiltasten zwischen den Dateien und benutze dann die F2-Taste, um sie schnell umzubenennen. Oder noch besser: Nachdem Sie F2 gedrückt und einen Dateinamen eingegeben haben, drücken Sie die **Tabulatortaste** (statt der Eingabetaste), um sofort mit der Umbenennung der nächsten Datei im Ordner zu beginnen.

### 20. Speichern Sie Screenshots als Datei

Die in Windows integrierten Screenshot-Tools sind immer besser geworden, aber manchmal möchten Sie die Tools überspringen und sofort den Screen als Bilddatei speichern.

Um einen Screenshot ohne die ganzen Zwischenschritte auf der Festplatte zu speichern, drücken Sie die **Windows-Taste + Bildschirm drucken**. Ihr Bildschirm wird blinken,

während Windows den Screenshot speichert. Danach finden Sie den Screenshot im Ordner “Bilder – Screenshots” Ihres Benutzerkontos.

Quelle: https://www.pcwelt.de/article/2468776/20-nuetzliche-windows-11-tastenkombinationen-die-ich-jeden-tag-verwende.html?utm_date=20241029102233&utm_campaign=Best-of%20PC-WELT&utm_content=slotno7-title-Diese%2020%20Tastenkombinationen%20f%C3%BCr%20Windows%2011%20m%C3%BCssen%20Sie%20kennen&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 7) Gut versteckt in Android: Diese 5 genialen Features kennen Sie bestimmt noch nicht

**In den Android-Einstellungen verstecken sich viele starke Funktionen, die kaum ein Nutzer kennt. Wir zeigen Ihnen fünf praktische Tricks, um mehr aus Ihrem Smartphone herauszuholen.**

Ein großer Vorteil von Android im Vergleich zu Apples iOS sind seit jeher die umfangreichen Möglichkeiten zur Anpassung. Im System sind zahlreiche Features versteckt, die im Alltag sehr praktisch sein können, den meisten Nutzern aber gar nicht bekannt sind.

Wir zeigen Ihnen daher **fünf geniale Android-Funktionen**, die wir nicht mehr missen möchten. Zusatz-Apps benötigen Sie dafür nicht – es steckt alles bereits in Ihrem Gerät.

### Funktion 1: Profi-Multitasking

Smartphones sind über die Jahre immer mehr gewachsen. Was früher schon fast als Tablet galt, geht heute als normale Displaygröße durch. Doch die meisten Nutzer beschränken sich noch immer darauf, nur eine App anzuzeigen.

Dabei kann Android viel mehr: Über den **Splitscreen-Modus** können Sie einfach mehrere Apps gleichzeitig auf den Bildschirm zaubern. Der Bildschirm wird damit in zwei Hälften geteilt und sie können die jeweilige Größe der Apps frei einstellen. Ständiges Hin- und herspringen gehört damit der Vergangenheit an.

**So aktivieren Sie das Feature**:

1. Eine der beiden gewünschten Apps öffnen
2. In den Task-Switcher wechseln ("Zuletzt verwendete Apps")
3. Auf das Icon der aktuellen App drücken
4. In den erscheinenden Einstellungen die Option "Geteilter Bildschirm" wählen
5. Zweite App auswählen

Wenn Sie das Bildschirmformat noch mehr ausreizen wollen, können Sie Apps sogar in schwebenden Fenstern anzeigen. Ähnlich wie am PC lassen sich die App-Fenster verschieben und skalieren. Der sogenannte **Freeform-Modus** muss aber möglicherweise erst in den Entwickleroptionen freigeschaltet werden. Das geht so:

1. Gehen Sie in den Einstellungen zum Bereich "Über das Telefon"
2. Tippen Sie unten mehrfach hintereinander auf die Build-Nummer, um den Entwicklermodus zu aktivieren
3. Scrollen Sie etwas nach unten und aktivieren Sie die Option "Freiform-Fenster zulassen"
4. Nun finden Sie im Task-Switcher neben der Split-Screen-Option auch den "Freeform-Modus"

**Funktion 2: Einhandmodus aktivieren**

Apropos Displaygröße: Wenn Ihr Smartphone mittlerweile so groß ist, dass Sie es nicht mehr mit einer Hand bedienen können, löst der **Einhandmodus** dieses Problem für Sie. Die Anordnung der Bildschirmelemente wird so verändert, dass Sie das Gerät auch mit einer Hand komfortabel bedienen können.

Seit Android 12 ist das Feature standardmäßig mit an Bord und kann unter Einstellungen >> System >> Gesten und Bewegungen aktiviert werden.

Aber auch Nutzer älterer Android-Versionen können über die Gboard-App von Google zumindest die Tastatur im Einhandmodus nutzen.

**So aktivieren Sie das Feature:**

1. Öffnen Sie die Gboard-Tastatur
2. Klicken Sie auf die drei Punkte und wählen Sie "Einhändiger Modus"

Funktion 3: App-Sperren einrichten

Im Familien- und Freundeskreis ist es schnell passiert: Jemand braucht Ihr Smartphone für irgendetwas und schon geben Sie es aus der Hand - manchmal länger als einem lieb ist.

Wenn Sie nicht wollen, dass andere in einem solchen Fall den vollständigen Zugriff auf Ihr Gerät haben, können Sie einfach eine einzelne App an den Bildschirm fixieren. Nutzer müssen dann erst die PIN eingeben, um an den restlichen Inhalt des Geräts zu kommen.

**So aktivieren Sie das Feature:**

1. Öffnen Sie die Einstellungen im Bereich "Sicherheit"
2. Wählen Sie den Punkt "Weitere Sicherheitseinstellungen" beziehungsweise "Erweitert"
3. Klicken Sie auf die Funktion "Bildschirmfixierung", setzen den Regler auf "Ein" und folgen Sie den dort beschriebenen Anweisungen

Einige Apps, wie etwa WhatsApp lassen sich auch einzeln mit einer Bildschirmsperre schützen. Über Zusatz-Apps, wie z.B. App Lock können Sie eine solche Sperre für jede beliebige App einrichten.

**Funktion 4: Weggewischte Benachrichtigungen zurückholen**

Push-Benachrichtigungen trudeln auf vielen Smartphones am laufenden Band ein – und werden genauso schnell wieder weggewischt.

Da ist es schnell passiert, dass sich darunter auch mal eine wichtige **Benachrichtigung** befindet, die man gerne **wieder zurückholen** würde. Was viele nicht wissen: Android macht genau das möglich.

**So aktivieren Sie das Feature**:

1. Öffnen Sie die Einstellungen
2. Gehen Sie zum Punkt "Benachrichtigungen"
3. Tippen Sie auf "Benachrichtigungsverlauf", um eine Chronik der vergangenen Benachrichtigungen anzuzeigen

Wenn Sie durch häufige Benachrichtigungen bestimmter Apps gestört werden, können Sie diese übrigens ebenfalls in den Einstellungen deaktivieren. Noch weiter lassen sich Benachrichtigungen mit Zusatz-Apps, wie z.B. Daywise personalisieren.

**Funktion 5: Clevere Bildschirmsperre mit Smart Lock**

Sie wollen Ihr Smartphone nicht jedes Mal entsperren, wenn Sie zu Hause sind, es unterwegs aber trotzdem mit einer Bildschirmsperre schützen? Dann kommt die **Smart Lock-Funktion** wie gerufen.

Damit bleibt das Smartphone an vertrauenswürdigen Orten wie etwa der eigenen Wohnung dauerhaft entsperrt. Alternativ funktioniert das Feature auch, wenn Ihr Android-Smartphone mit vertrauenswürdigen Geräten verbunden ist, etwa dem Bluetooth-Speaker im Wohnzimmer.

**So aktivieren Sie das Feature:**

1. Öffnen Sie die Einstellungen Ihres Smartphones
2. Gehen Sie zum Punkt "Sicherheit" und dann zu "Weitere Sicherheitseinstellungen"
3. Wählen Sie "Smart Lock" und folgen Sie den Anweisungen

*Hinweis: Wie Sie die Features aktivieren, kann sich von Gerät zu Gerät unterscheiden. Möglicherweise gibt es bei den oben beschriebenen Anleitungen Abweichungen für Ihr Smartphone.*

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

Quelle: https://www.chip.de/news/Gut-versteckt-in-Android-Diese-5-genialen-Features-kennen-Sie-bestimmt-noch-nicht_184361438.html?utm_source=flipboard&utm_content=topic%2Fde-digital

# 8) Tipp – Whatsapp: So erkennen Sie, ob Sie ausspioniert werden

**Haben Sie das Gefühl, dass jemand Ihre Chats mitliest? Und wie nimmt es Whatsapp mit dem Schutz Ihrer Daten? Hier finden Sie es heraus.**

**Inhaltsverzeichnis**



Wie sicher sind Ihre Whatsapp-Nachrichten wirklich? Wie merkt man, ob jemand heimlich mitliest? Und ist der Datenschutz und die Verschlüsselung auf Whatsapp wirklich so gut?

Angesichts der wachsenden Bedrohungen durch Cyberkriminelle ist es entscheidend, wachsam zu bleiben und zu wissen, wie man potenzielle Sicherheitslücken erkennt und schließt.

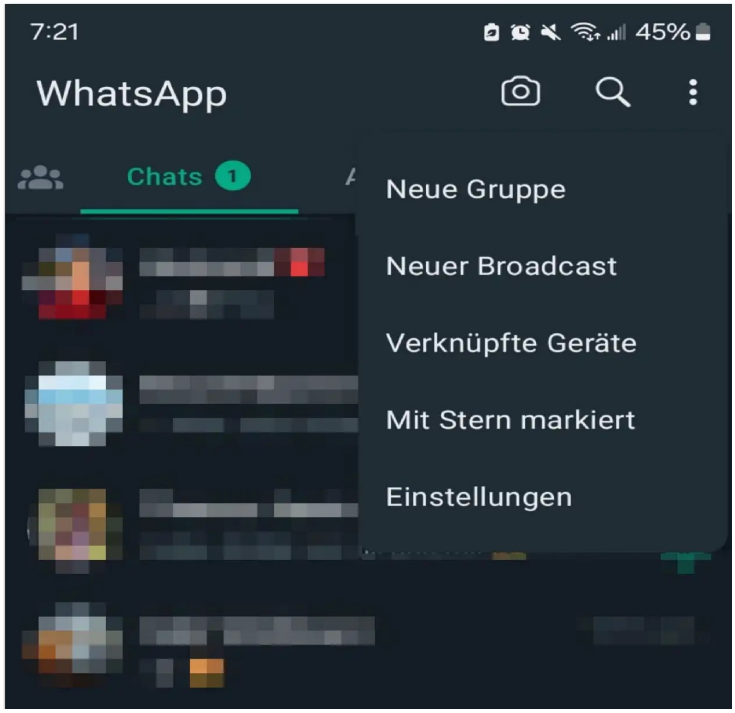
In unserem Artikel erfahren Sie daher, wie Sie überprüfen können, ob jemand unbefugt Zugriff auf Ihr Whatsapp-Konto hat und welche Schritte Sie unternehmen können, um Ihre privaten Unterhaltungen zu schützen. Zudem geben wir einen kurzen Überblick zu den Datenschutz-Risiken auf Whatsapp.

**Mit diesem Trick erkennen Sie, ob jemand heimlich mitliest**

Seit 2016 schützt Whatsapp Nachrichten mit einer Ende-zu-Ende-Verschlüsselung, wodurch diese nur vom Absender und Empfänger gelesen werden können. Doch Vorsicht: Whatsapp im Browser zu nutzen, birgt nach wie vor Risiken.

Ein unbefugter Zugriff über Whatsapp-Web ermöglicht es, Ihre Nachrichten mitzulesen, selbst wenn das Smartphone und der Computer nicht im gleichen Netzwerk sind. Überprüfen Sie daher regelmäßig die mit Ihrem Konto verknüpften Geräte:

1. Öffnen Sie die App auf Ihrem Smartphone.
2. Tippen Sie in der Chats-Übersicht rechts oben auf die drei Punkte (Android) oder unten rechts auf “Einstellungen” (iOS).
3. Wählen Sie die Option “Verknüpfte Geräte” aus und prüfen Sie, ob dort fremde Geräte verlinkt sind.





Prüfen Sie anschließend, ob unbekannte Geräte über Whatsapp Web mit Ihrem Konto verknüpft sind. Bild IDG

**Was tun, wenn ein fremdes Gerät verknüpft ist?**

Halten Sie den Finger auf das Gerät gedrückt, das Sie entfernen möchten. Im Pop-up-Fenster tippen Sie anschließend auf “Abmelden”, um die Verbindung zu trennen.


Halten Sie den Finger auf das Gerät gedrückt, um die Verbindung zu trennen. Bild IDG

**So schützen Sie sich vor fremden Mitlesern**

Damit jemand sich unbemerkt mit Ihrem Whatsapp Web verknüpfen kann, muss er den entsprechenden QR-Code in Ihrer Smartphone-App gescannt haben. Achten Sie also darauf, wem Sie Ihr Handy überlassen.

**Tipp:** Aktivieren Sie die **Zwei-Faktor-Authentifizierung** in den App-Einstellungen unter “Account”. Dazu müssen Sie eine sechsstellige PIN festlegen, die bei jedem Aufruf der App erforderlich ist. Geben Sie diese PIN an niemanden weiter.

Weitere Vorsichtsmaßnahmen zum Schutz Ihres Kontos sind:

- **Vorsicht bei Dateien und Links:** Öffnen Sie nichts, was von unbekannten Kontakten stammt oder Ihnen komisch vorkommt. Auch Freunde können unbeabsichtigt Spam oder schadhafte Links senden, etwa für Fake-Gewinnspiele.
- **Apps auf dem neuesten Stand halten:** Aktualisieren Sie Whatsapp und andere Apps regelmäßig, um sicherzustellen, dass Sicherheitslücken geschlossen werden.
- **Kettenbriefe ignorieren:** Vermeiden Sie das Weiterleiten von Kettenbriefen, denn hinter vielen stecken Betrugsmaschen.

**Wie gut sind Verschlüsselung und Datenschutz bei Whatsapp?**

Whatsapp gibt an, dass der Schutz der Privatsphäre und Sicherheit “Teil der DNA” sei. Daher sind seit jeher sämtliche Chats durch Ende-zu-Ende-Verschlüsselung geschützt. Das gilt für den Nachrichtenaustausch mit Personen ebenso wie mit Unternehmen, für das Versenden von Bildern und für Zahlungen über Whatsapp, sofern verfügbar.

Informationen werden somit nur über das benutzte Gerät gesendet und empfangen, laut Whatsapp selbst. Dennoch gibt es Risiken, die dafür sorgen könnten, dass Unbefugte Ihre Nachrichten mitlesen.

Dazu gehören unter anderem die beliebten Gruppenchats, da hier die Verschlüsselung nicht ganz so einfach funktioniert wie bei 1zu1-Gesprächen. Je mehr Teilnehmerinnen und Teilnehmer vorhanden sind, desto mehr Geräte müssen mitwirken. Zudem können Gruppen-Admins Mitglieder hinzufügen, die Sie nicht kennen, und somit Ihre Nummer preisgeben.

Auch die Backups von Chats war lange Zeit nicht gut geschützt. Erst 2021 führte Whatsapp die Option ein, Backups ebenfalls zu verschlüsseln und zusätzlich mit einem Passwort zu versehen. Diese Option müssen Sie aber erst aktivieren, und zwar in den Einstellungen unter **Chats** und dann **Chat-Backup**.

Zudem gibt es immer wieder Ansätze von Regierungen und Behörden, Zugriff auf die Daten von Whatsapp zu erhalten, inklusive Chats. Der Wunsch nach Vorratsdatenspeicherung sowie einer Art “Generalschlüssel” ist immer wieder alarmierend für viele Datenschützer. Momentan bleiben Nachrichten auf Whatsapp aber verschlüsselt und für Dritte unzugänglich.

Quelle: https://www.pcwelt.de/article/2261423/whatsapp-spionage-erkennen-wer-liest-ihre-chats-mit.html?utm_source=flipboard&utm_content=topic/de-apps

# 9) download – Prey

**Die Ortungs-Software Prey macht Laptops und mobile Geräte ausfindig, wenn diese verloren gegangen sind oder gestohlen wurden. Mit dem Programm lassen sich darüber hinaus (sensible) Daten auf den verloren gegangenen Geräten aus der Ferne löschen.**

Das Tool Prey wird vom Hersteller als Diebstahlschutz beworben, aber es handelt sich dabei eher um eine Unterstützung bei der Wiederbeschaffung eines entwendeten Geräts. Prey läuft im Hintergrund als Windows-Systemdienst und wartet auf seine Aktivierung, die einfach über die Steuerkonsole auf der Hersteller-Website gestartet werden kann.

Nach der Aktivierung sammelt die Software Informationen, die für die Wiederbeschaffung des jeweiligen Gerätes nützlich sind. Dazu gehört die Möglichkeit, die Position des Geräts mittels GPS oder benachbarter WLANs einzugrenzen. Außerdem können Screenshots der aktiven Sitzung verfolgt werden, um zu sehen, welche Internetseiten der aktuelle Nutzer besucht, und durch die Webcam kann man eventuell sogar ein Foto des Nutzers machen.

Außerdem lassen sich remote steuerbare Aktionen auf dem gestohlenen Gerät ausführen. Prey kann Alarmtöne auslösen, Alarmmeldungen anzeigen, den Computer sperren, E-Mails und gespeicherte Passwörter verbergen. Die gesammelten Informationen werden regelmäßig an die Steuerkonsole gesendet und als Berichte zur Verfügung gestellt. Bei fehlender Internetverbindung kann das Tool, falls gewünscht, die Informationen über den nächstgelegenen Hotspot übertragen.

Die Grundversion von Prey ist kostenlos und ermöglicht das Überwachen von bis zu drei

Geräten mit bis zu zehn Berichten pro Gerät. Wer mehr Funktionen benötigt, kann einen Pro-Account erwerben, der zusätzliche Funktionen wie SSL-verschlüsselte Berichte bietet. Weitere Informationen finden sich auf der Herstellerseite.

**Tipp:** Auch Prey ist kein Erfolgsgarant. Vor allem unterwegs sollten Sie sehr vorsichtig sein. Notebookschlösser schützen Sie zum Beispiel immerhin vor Gelegenheitsdieben. Fertigen Sie auch regelmäßig Backups an, um wenigstens Ihre Daten vor Verlust durch Diebstahl zu sichern. Toucan ist ein Backup-Tool, das Sie dabei unterstützt.

**Tipp:** Wer war an meinem Rechner, wer in der Küche und wie finde ich heraus, wo genau dieses Foto aufgenommen wurde? Wir zeigen Tools für Spionage und Gegenspionage.

**Anmerkung der Redaktion:** Unter dem u.g. Link kann ein Download der Software erfolgen

Quelle: https://www.pcwelt.de/article/1142841/sicherheits-tool-prey.html?utm_date=20241029140347&utm_campaign=Security&utm_content=slotno9-description-Die%20Ortungs-Software%20Prey%20macht%20Laptops%20und%20mobile%20Ger%C3%A4te%20ausfindig%2C%20wenn%20diese%20verloren%20gegangen%20sind%20oder%20gestohlen%20wurden.%20Mit%20dem%20Programm%20lassen%20sich%20dar%C3%BCber%20hinaus%20%28sensible%29%20Daten%20auf%20den%20verloren%20gegangenen%20Ger%C3%A4ten%20aus%20der%20F&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 10) Nie mehr Rundfunkbeitrag: Dieser Anbieter hat ein verlockendes Versprechen

**Über den Rundfunkbeitrag gibt es viele Diskussionen, manche Bürger möchten ihn am liebsten gar nicht mehr zahlen. Ein Anbieter im Internet will dabei helfen – aber es gibt einen großen Haken.**

Die öffentlich-rechtlichen Medien (ÖRR) stehen in den letzten Jahren immer wieder in der Kritik, etwa aufgrund von

- zu hoch empfundenen Intendantengehältern
- Doppelstrukturen
- oder einer sozial ungerechten Forderung des Rundfunkbeitrags

Genau diesen würden sich viele Bürger am liebsten komplett sparen. Immerhin sind das aktuell **18,36 Euro pro Monat und Haushalt** – also 220,32 Euro im Jahr. Dieser Beitrag ist Pflicht für alle, die entsprechende Empfangsgeräte für Inhalte des ÖRR besitzen. Das kann auch schon ein Autoradio oder ein internetfähiges Handy sein.

Entziehen kann man sich dem Beitrag also nicht wirklich, wenn man nicht für eine Befreiung berechtigt ist. Es gibt mit dem "Beitragsblocker" einen Anbieter im Internet, der behauptet, dies trotzdem auf völlig legalem Weg möglich zu machen. Wer darauf hereinfällt, für den **wird es allerdings teuer.**

### Beitragsblocker: Ist der Dienst überhaupt legal?

Es gibt berechtigte Kritik am ÖRR und die Rufe nach einer grundlegenden Reform werden immer lauter. Jedoch nutzt die Website von "Beitragsblocker" Begriffe, die man eher aus Kreisen von Verschwörungstheoretikern kennt: Es ist die Rede von "Zwangspropaganda" und der ÖRR wird als "parasitäre, destruktive Organisation" bezeichnet.

Der Anbieter will seine Kunden von der Zahlung des Rundfunkbeitrags befreien – für eine **einmalige Gebühr von 55,08 Euro**, was exakt drei Monaten Rundfunkbeitrag entspricht. Als

Gegenleistung erhält man *"alle anwaltlich erarbeiteten Schreiben, um sich in drei Schriftsatz-Wellen gegen den Rundfunkbeitrag zu wehren."*

Der Rechtsanwalt Christian Solmecke hat sich das genauer angeschaut und warnt ausdrücklich vor dieser **juristisch fragwürdigen Dienstleistung**, die für Kunden teuer werden kann.

### Komplett haltlos: Finger weg von Beitragsblocker

Der Anbieter behauptet, dass seine Kunden die Zahlung des Rundfunkbeitrags beenden und sich anschließend gegen sämtliche Forderungen von Gerichtsvollziehern mit den angebotenen Schriftstücken wehren können. Dafür zieht "Beitragsblocker" zahlreiche juristisch anmutende Erklärungen in einem Gutachten heran.

Dieses behauptet unter anderem, dass die Gerichtsvollzieher laut Gerichtsvollzieherordnung (GVO) seit 2012 nicht mehr als Beamte tätig seien und somit auch keine Zwangsvollstreckungen im Auftrag des Staates durchführen dürften – auch nicht im Zusammenhang mit dem Rundfunkbeitrag. Laut Geschäftsführer Markus Böhning handeln die Gerichtsvollzieher somit verfassungswidrig. Dies genügt laut dem Anbieter als Legitimation, den **Rundfunkbeitrag einfach nicht mehr zu zahlen.**

Die Analyse von Christian Solmecke zeigt jedoch, dass das juristisch betrachtet unwirksam ist und bezeichnet es sogar als "kompletten Bullshit" und "haltlos".

### Darum liegt Beitragsblocker laut Solmecke falsch

Christian Solmecke nimmt in seiner Untersuchung das Rechtsgutachten von "Beitragsblocker" auseinander und zeigt auf, dass es **grundlegende juristische Fehler** enthält. Die Argumente im Überblick:

1. Die Gerichtsvollzieherordnung (GVO) ist kein parlamentarisches Gesetz. Ihm übergeordnet ist das Gerichtsverfassungsgesetz (GVG). In Paragraf 154 ist klar geregelt, dass Gerichtsvollzieher Beamte sind.
2. "Beitragsblocker" behauptet, dass Gerichtsvollzieher nicht mehr als Beamte besoldet werden. Solmecke zieht als Beispiel das Landesbesoldungsgesetz von NRW heran, wo diese Berufsgruppe mit A8 besoldet werden.
3. "Beitragsblocker" behauptet, dass durch die Aufhebung des Paragrafen 15 GVO Regeln zur Strafbarkeit wegen Bestechlichkeit entfallen seien. Jedoch gibt es auch hier ein übergeordnetes Gesetz, mit dem Bundesbeamtengesetz (BBG), wo in Paragraf 71 ebenfalls klar geregelt ist, dass Beamte *"keine Belohungen, Geschenke oder sonstigen Vorteile"* annehmen dürfen.
4. Entgegen der Behauptung von Beitragsblocker gibt es für die Vollstreckung des Rundfunkbeitrages eine Ermächtigungsgrundlage.

Die rechtlichen Grundannahmen von "Beitragsblocker" seien demnach falsch. Auch ein Gerichtsurteil, welches der Anbieter für sich als Rechtfertigung heranzieht, enthielt lediglich einen formellen Fehler, wie das Landgericht München I richtigstellte.

### Kunden berichten von Mahngebühren

Wer also eigenmächtig aufhört, den Rundfunkbeitrag zu zahlen, der **bringt sich selbst in Schwierigkeiten**. Es fallen zunächst immer mehr Mahngebühren an. Werden weitere Zahlungsaufforderungen ignoriert, dann werden verschiedene Vollstreckungsmaßnahmen durchgeführt:

- Gütliche Einigung (Ratenzahlung)

- Sachpfändungen
- Kontopfändung
- Lohn- und Gehaltspfändung
- Pfändung von Sozialleistungen (beispielsweise Krankengeld, Rente, Arbeitslosengeld)
- Pfändung von Lebensversicherungsansprüchen

Wer nicht zahlt, dem drohen auch **negative Schufa-Einträge**, was die Kreditwürdigkeit beeinträchtigen kann. Es sind auch Gerichtsverfahren möglich, deren Kosten die Betroffenen dann möglicherweise selbst tragen müssen.

Zahlreiche Kunden berichten auf der Plattform Trustpilot darüber, dass der Dienstleister sie nur viel Geld gekostet habe. Die 55,08 Euro für den "Beitragsblocker" sind laut Solmecke also "rausgeschmissenes Geld".

Quelle: https://www.chip.de/news/Nie-mehr-Rundfunkbeitrag-Dieser-Anbieter-hat-ein-verlockendes-Versprechen_185544900.html?utm_source=chip_1001310&utm_content=29.10.2024&utm_medium=email&utm_campaign=1015952

# 11) Tipp – Youtube-Videos ohne Werbung anschauen, mit diesem einfachen Trick

**Genervt von Werbung auf Youtube? Wer nicht. Mithilfe eines Bugs können Sie die Werbung aber einfach überspringen. Das funktioniert einfach im Browser ohne Adblocker oder andere Tools.**

Werbung auf Youtube ist für viele Nutzer eine lästige Angelegenheit. In den vergangenen Jahren sind die Werbepausen so häufig und penetrant geworden, dass man sie am liebsten sofort überspringen möchte. Doch einige Einblendungen muss man bis zum Ende durchschauen, oder wir bekommen eine überspringbare Werbung nach der anderen.

Viele greifen daher zu Adblockern, doch diesen hat Google offenbar den Kampf angesagt. Einige funktionieren nicht mehr oder zeigen ein schwarzes Bild. Doch es gibt eine Alternative, wie Sie Werbung vor Youtube-Videos überspringen, für die Sie keine Browser-Erweiterung oder sonstige Tools brauchen.

**Lesetipp:** 4 Werbeblocker, die noch mit Chrome funktionieren

Youtube ohne Werbung: So funktioniert es

Der Trick zum werbefreien Youtube basiert auf einem Bug, der aktuell in der Suchmaschine Bing existiert. Er funktioniert in so gut wie jedem Browser (wir testeten Chrome, Firefox und Edge) und ist nicht nur einfach, sondern auch schnell erledigt.

Alles, was Sie tun müssen, ist die URL des Youtube-Videos, das Sie ansehen wollen, in die Suchleiste von Bing zu kopieren. Wenn das Video direkt erscheint, klicken Sie auf den neuen Link. Falls nicht, müssen Sie eventuell den Titel des Videos kopieren und stattdessen einfügen.

Das war es auch schon. Sie können das Video nun im erscheinenden Fenster ohne Werbung ansehen. Auch wenn Sie auf den Button “auf Youtube ansehen” klicken, sollte in der Regel keine Werbepause am Anfang auftauchen.

**Hinweis:** Bei längeren Videos kann es vorkommen, dass Youtube sich später im Video noch einmal aktualisiert und weitere Werbung lädt. In diesem Fall kommt der Trick an seine

Grenzen. Die Werbung beim Start eines neuen Videos oder bei kürzeren Clips überspringt man damit aber immer.

Falls der Trick mal nicht funktionieren sollte, hat es bei uns übrigens geholfen, Bing noch einmal neu zu öffnen oder den Browser zu wechseln.

### Youtube Premium für viele zu teuer

Google sieht es natürlich nicht gerne, wenn Nutzer versuchen, ihre Werbung zu überspringen. Zumal mit Youtube Premium die Option geboten wird, alle Werbepausen per Abo loszuwerden.

Für viele ist dieses aber schlichtweg zu teuer geworden, zumal Youtube seit Kurzem einen beliebten VPN-Trick blockiert, mit dem man das Premium-Abo deutlich günstiger bekommen konnte. Auch bereits abgeschlossene Abos wurden gekündigt.

Wir möchten Sie deswegen nicht dazu ermutigen, Youtube-Werbung pauschal immer zu blockieren. Denn letztendlich schadet das nicht nur Youtube selbst, sondern auch den Kanälen, die Sie gerne schauen. Doch die Tatsache, dass dieser Trick funktioniert, ist in unseren Augen sehr kurios und berichtenswert. Auch wenn Google oder Microsoft ihn vielleicht bald weg patchen werden.

**Lesetipp:** Amazon Prime Video ohne Werbung? Diese Tricks machen es möglich

Quelle: https://www.pcwelt.de/article/2459109/so-schauen-sie-youtube-videos-ohne-werbung-mit-diesem-absurd-einfachen-trick.html?utm_date=20241029143957&utm_campaign=Best-of%20PC-WELT&utm_content=slotno7-title-Youtube-Videos%20ohne%20Werbung%20anschauen%2C%20mit%20diesem%20einfachen%20Trick&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 12) Überall kostenloses WLAN: WiFi4EU-Karte zeigt 100.000 freie Hotspots in Europa

**Wenn Sie ab und an auf der Suche nach kostenlosen WLANs sind, sollten Sie sich die App WiFi4EU Map ansehen. Die verzeichnet mittlerweile fast 100.000 kostenlose WLANs in ganz Europa, tracking- und werbefrei.**

Seit einigen Jahren gibt es schon die von der Europäischen Kommission geleitete Initiative Wifi4 EU. Sie soll Gemeinden und Städte dabei unterstützen, kostenlose öffentliche WLAN-Hotspots bereitzustellen. Wer hier mitgemacht hat, konnte ordentlich Fördergelder kriegen und das hat Wirkung gezeigt.

WiFi4EU hat mittlerweile mehr als 7.200 Kommunen in der gesamten Europäischen Union unterstützt, die zusammen fast 100.000 öffentliche WLAN-Hotspots für ihre Anwohner und Besucher eingerichtet haben. Über die kostenlose App WiFi4EU Map, die es für Android und iOS gibt, finden Sie das Gratis-WLAN in Ihrer Nähe.

### Kostenloses WLAN ohne Tracking und Werbung

Die kostenlosen WLANs sind deshalb interessant, weil sie von öffentlichen Stellen bereitgestellt werden. Nutzer werden dabei weder getrackt noch mit Werbung bombardiert. Was aber sein kann: Die Gemeinden können auf den Startseiten eigene Inhalte einbinden, etwa Infos für Touristen.

Ansonsten funktionieren die Apps in zwei Modi: Entweder Sie lassen die Standortfreigabe zu, dann sehen Sie den eigenen Standort auf der Karte plus die WLANs in der Umgebung. Oder Sie geben den eigenen Standort nicht preis und hangeln sich selbst zu den WLAN-Hotspots.

Die Suche der leider nur in englischer Sprache bereitgestellten App ist aber nicht besonders hilfreich, am besten zoomen Sie die Karte per Hand zurecht. Für die Nutzung der Hotspots müssen Sie keine Daten angeben. Verbinden Sie sich mit dem WLAN "WiFi4EU" und bestätigen Sie einmal die Nutzung im Browser.

Ist der WLAN-Hotspot noch zu weit entfernt, können Sie sich über einen praktischen Button dorthin navigieren lassen. Beachten Sie, dass die WLAN-Hotspots eher außerhalb von großen Städten bzw. in Randgebieten zu finden sind. In den meisten Großstädten dürfte es aber ohnehin an öffentlichen Plätzen oft Gratis-WLAN geben.

**Zusätzliche VPN-Nutzung empfohlen**

Der Ansatz, auf Tracking und Werbung zu verzichten, aber das WLAN trotzdem gratis anzubieten, klingt verlockend. Trotzdem raten wir, an öffentlichen Hotspots immer ein VPN zu nutzen.

VPNs gibt es grundsätzlich auch kostenlos, wobei Sie hier auch immer die Frage nach dem Geschäftsmodell beantworten sollten. Einige Angebote haben wir in einem eigenen Beitrag mit Vor- und Nachteilen gesammelt.

Wer für ein VPN Geld ausgibt, kann jedoch mit besserem Komfort, erhöhter Sicherheit und schnellerer Performance rechnen. Unser aktueller Test informiert Sie über passende Angebote.

**Anmerkung der Redaktion:** Die App kann unter dem u.g. Link heruntergeladen werden

Quelle: https://www.chip.de/news/Ueberall-kostenloses-WLAN-WiFi4EU-Karte-zeigt-100.000-freie-Hotspots-in-Europa_185525159.html?utm_source=flipboard&utm_content=topic%2Fde-digital

# 13) Ratgeber – Windows 11: So aktivieren Sie den integrierten Ransomware-Schutz und das sind die Vorteile

**Wussten Sie, dass Windows einen eingebauten Ransomware-Schutz enthält? Microsoft Defender kann Ihren PC schützen, aber die Funktion ist nicht automatisch aktiviert. Wir erklären Ihnen, wie es geht und was es bringt.**

Ransomware ist eine fiese Sache. Diese Art von Malware verschlüsselt Dateien auf Ihrem PC, so dass Sie nicht mehr darauf zugreifen können – es sei denn, Sie bezahlen dem Angreifer ein Lösegeld für Ihre Dateien. Die beste Verteidigung gegen Ransomware ist die Vermeidung von Websites und Downloads, die mit Ransomware verseucht sind. Moderne Antivirensoftware schränkt oft ein, welche Anwendungen Dateien in Ordnern ändern können, die häufig Ziel von Ransomware sind. Der Microsoft Defender, der in Windows integriert ist, kann dies ebenfalls tun. Einige Antiviren-Suites (hier stellen wir die aktuell besten Antiviren-Suites vor) führen auch automatische Backups durch, falls Sie Ihre Dateien wiederherstellen müssen.

Lesetipp: Die besten Antivirus-Programme 2024 im Test

Der Haken an der Sache? Anders als bei Antivirensoftware von Drittanbietern sind diese zusätzlichen Schutzmaßnahmen in Microsoft Defender *nicht* standardmäßig aktiviert. Sie müssen sie selbst aktivieren.

## So aktivieren Sie den Ransomware-Schutz in Windows

### Schritt Eins: Öffnen Sie Windows-Sicherheit

Öffnen Sie die Windows-Sicherheits-App auf Ihrem PC. Sie können sie auf verschiedene Weise aufrufen:

- Geben Sie etwa in das Sucheingabefeld auf dem Desktop *“windows sicherheit”* ein und drücken Sie dann Enter
- Öffnen Sie Ihr Startmenü, geben Sie *Windows-Sicherheit* ein und drücken Sie die Eingabetaste
- Öffnen Sie Ihre Einstellungen und wählen Sie dann unter “Datenschutz und Sicherheit” den Eintrag *Windows-Sicherheit* aus.

### Schritt Zwei: Finden Sie die Ransomware-Einstellungen

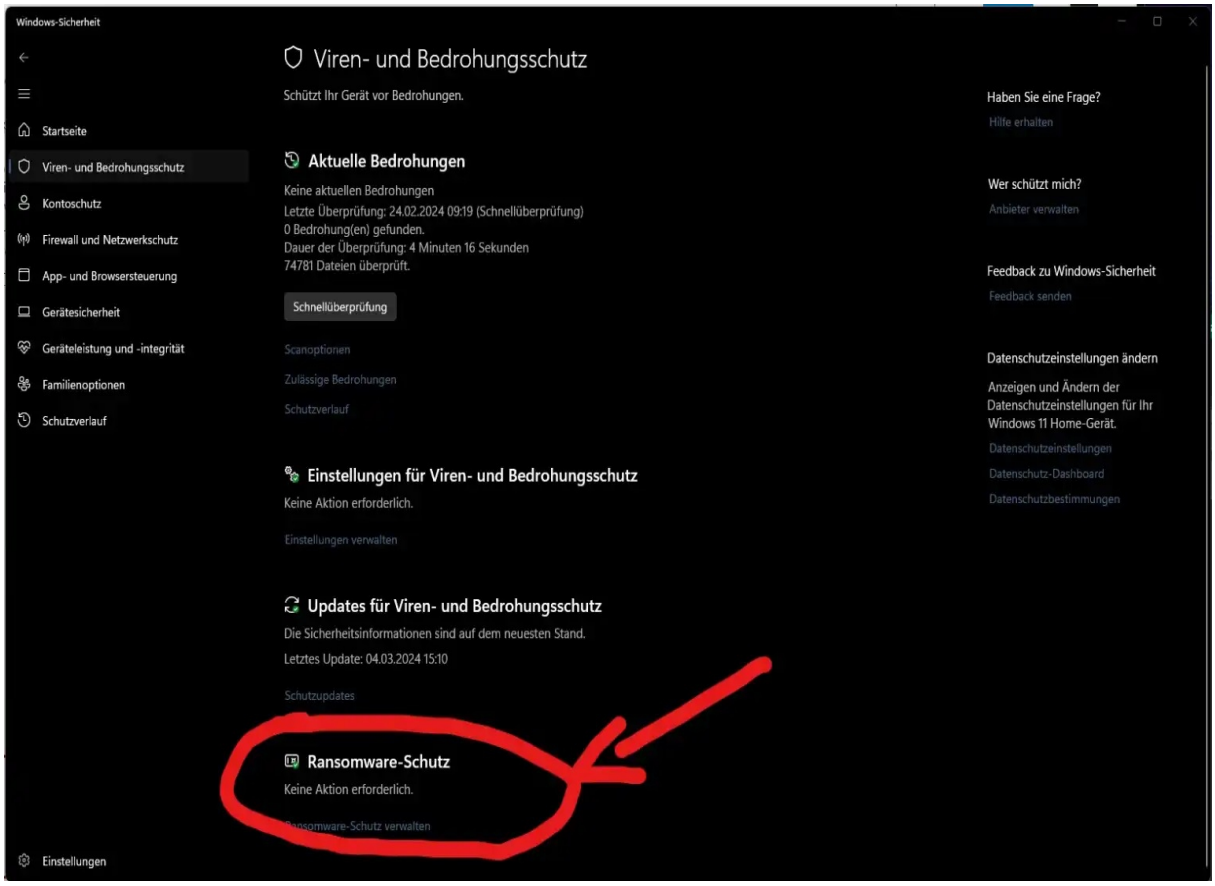


Bild: PC-WELT

Klicken Sie in der Windows-Sicherheits-App auf *Viren- und Bedrohungsschutz*. Klicken Sie dann auf *Ransomware-Schutz verwalten* am unteren Rand des Bildschirms.

Aktivieren Sie als Nächstes die Option *Überwachter Ordnerzugriff*. Diese Einstellung schränkt den Zugriff von Apps auf die Standardordner OneDrive, Dokumente, Bilder, Videos, Musik und Favoriten auf Ihrem PC ein. Sie können auch andere Ordner manuell zur Liste hinzufügen.

Nicht alle Apps werden von diesen Bereichen in Windows ausgeschlossen – Microsoft Office-Programme etwa dürfen automatisch Dateien öffnen und ändern. Aber wenn ein Programm nicht auf der internen Microsoft-Liste der vertrauenswürdigen Anwendungen steht, kann es nichts in diesen Ordnern sehen, bis es in der Windows-Sicherheitsfunktion ausdrücklich vom Nutzer zugelassen wird.

### Dritter Schritt: Stellen Sie sicher, dass Sie bei OneDrive angemeldet sind

Die Einschränkung des Zugriffs auf Dateien und Ordner reicht noch nicht aus, um sie vollständig zu schützen. Eine weitere wichtige Schutzmaßnahme ist eine gute Datensicherung, die Windows automatisch durchführt, wenn Sie bei OneDrive angemeldet sind. Sie können entweder ein Microsoft-Konto mit Ihrem gesamten Windows-PC oder nur mit der OneDrive-App verbinden.

Um zu überprüfen, ob dieser Schutz aktiviert ist, können Sie unter *Ransomware-Schutz* > *Ransomware-Datenwiederherstellung* nachsehen.

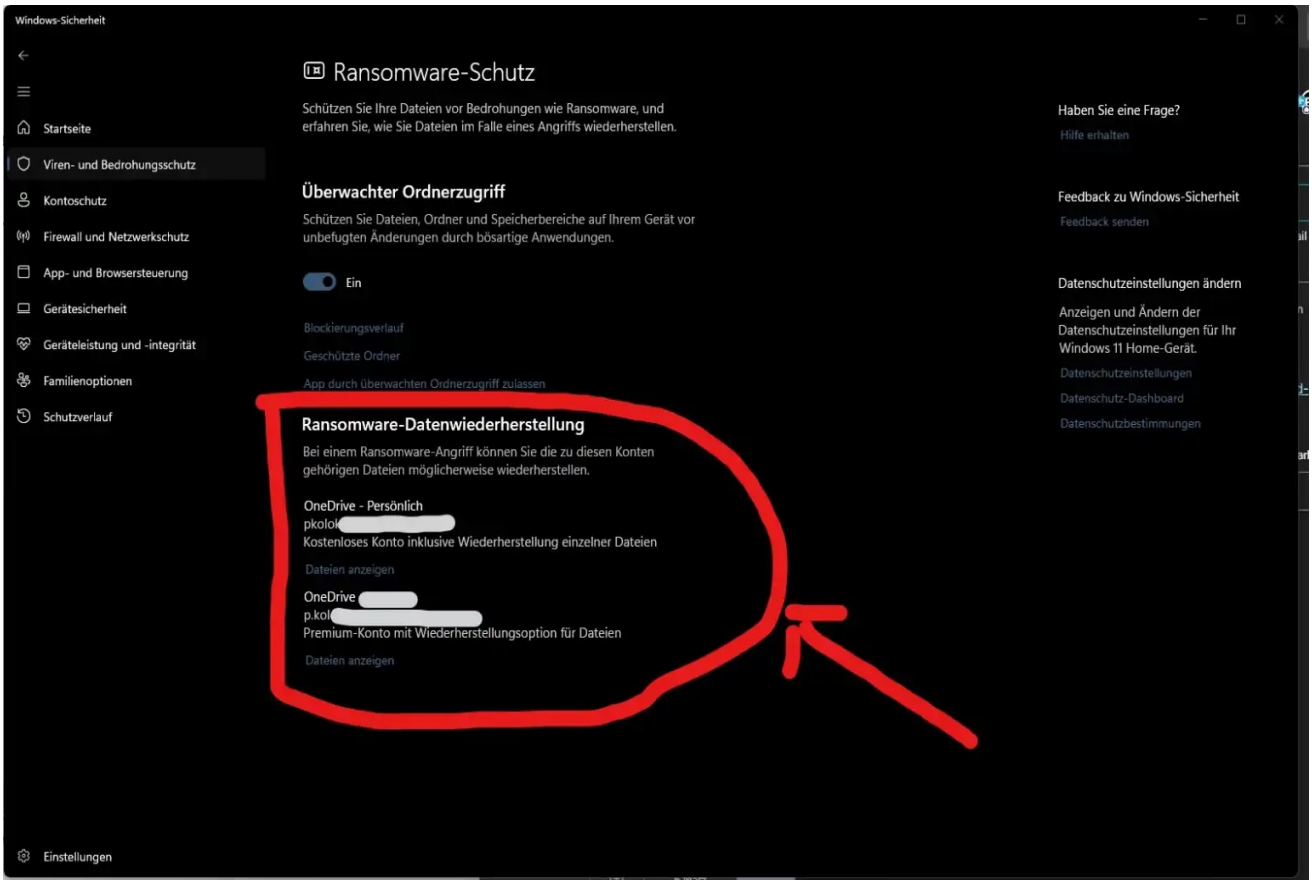


Bild PC-WELT

Um die schlimmsten Auswirkungen von Ransomware abzuwehren, ist das sicherste Backup Ihrer Dateien natürlich das, das Sie offline aufbewahren. Sie sollten zusätzlich zu den in der Cloud gespeicherten Daten eine weitere Kopie erstellen, um wirklich abgesichert zu sein.

### Sollten Sie den Ransomware-Schutz in Windows aktivieren?

Sicherheit und Komfort liegen an entgegengesetzten Enden eines Spektrums, und das ist auch hier der Fall. Die Kontrolle des Ordnerzugriffs in Windows kann Angreifer von Ihren wichtigen Dateien und Ordnern fernhalten, aber sie kann auch etwas unbequem sein. Gamer werden zum Beispiel feststellen, dass der Zugriff auf Speicherdateien standardmäßig blockiert wird, weil diese oft im Dokumente-Ordner gespeichert werden.

Sie können dieses Problem mit einem geringen Aufwand lösen – fügen Sie das Spiel einfach der Zugriffsliste hinzu. Oder speichern Sie Spieldateien in einem anderen Ordner auf Ihrem PC, auf den kein kontrollierter Zugriff besteht. Sie müssen dann lediglich eine Software eines Drittanbieters verwenden, um einen Zeitplan für regelmäßige Backups einzurichten.

### Schützen Sie Ihren Windows-PC auch vor anderen Online-Bedrohungen

Wenn Sie eine im Vergleich zu den Windows-Bordmitteln anspruchsvollere Software mit zusätzlichem Schutz bevorzugen, sollten Sie ein Upgrade Ihrer Antivirensoftware in Betracht ziehen. Norton 360 Deluxe gehört derzeit zu unseren Favoriten unter den Antivirenprogrammen. Die Software bietet einen starken Schutz vor Malware, ein VPN, einen Passwort-Manager, eine Dark-Web-Überwachung für Ihre persönlichen Daten und vieles mehr.

Quelle: https://www.pcwelt.de/article/2254566/windows-integrierten-ransomware-schutz-aktivieren.html?utm_date=20241030113300&utm_campaign=Best-of%20PC-WELT&utm_content=slotno4-title-Windows%2011%20besitzt%20einen%20integrierten%20Ransomware-Schutz%20und%20so%20aktivieren%20Sie%20ihn&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 14) Dringend aktualisieren – Google beseitigt Sicherheitslücken in Chrome

**In seinem wöchentlichen Chrome-Update hat Google diesmal zwei Sicherheitslücken geschlossen. Eine Schwachstelle stuft der Konzern als "kritisch" ein.**

Google hat ein Update für seinen Internetbrowser Chrome veröffentlicht und schließt damit zwei Sicherheitslücken, wie das Unternehmen auf seinem Blog mitteilt. Chrome-Nutzer sollten sich mit einem Update des Browsers beeilen.

Warum? Weil Google eine der Sicherheitslücken als "kritisch" einstuft. Wie das IT-Magazin "Heise online" berichtet, handle es sich um eine Schwachstelle, die Angreifern "Schreibzugriffe auf dafür nicht vorgesehene Speicherbereiche erlaubt" und es ermöglicht, Schadcode einzuschleusen und auszuführen.

Die zweite Schwachstelle mit der Bezeichnung "CVE-2024-10488" stuft Google mit dem Risiko "Hoch" ein. Laut "Heise online" könnten Angreifer über die Sicherheitslücke "auf bereits freigegebene Ressourcen zugreifen, deren Inhalte dadurch nicht definiert sind". Auch das könnte missbraucht werden, um Schadcode einzuschleusen, heißt es weiter.

Das von Google veröffentlichte Update bringt den Chrome-Browser auf Version 130.0.6723.91/.92 für Windows und Mac und 130.0.6723.91 für Linux.

### Chrome aktualisieren – so geht's

In den meisten Fällen aktualisiert sich Chrome automatisch, sobald Nutzer den Browser schließen und wieder öffnen. Die Updates lassen sich aber auch manuell ausführen.

Wer die aktuellen Versionen des Internetbrowsers bisher nicht nutzt, sollte dringend die neue Version installieren.

Wo Sie die aktuelle Versionsnummer sehen und wie ein manuelles Update des Browsers gestartet wird, erklären wir hier:

- Öffnen Sie Chrome auf dem Computer.
- Öffnen Sie rechts oben über die drei senkrechten Punkte das Menü.
- Klicken Sie auf Hilfe und dann auf "Über Google Chrome".
- Klicken Sie auf "Google Chrome aktualisieren". Sehen Sie diese Schaltfläche nicht, ist bereits die neueste Version installiert.
- Starten Sie nun den Browser neu. Das können Sie über die Schaltfläche "Neu starten" machen oder einfach, indem Sie den Browser schließen und erneut öffnen.

Die geöffneten Tabs und Fenster werden vom Browser gespeichert und beim Neustart automatisch geöffnet. Wenn Sie den Browser nicht sofort neu starten möchten, klicken Sie auf "Jetzt nicht". Das Update wird dann beim nächsten Start des Browsers installiert.

Quelle: https://www.t-online.de/digital/aktuelles/id_100520386/google-chrome-schnell-aktualisieren-kritische-sicherheitsluecke-beseitigt.html

# 15) News – Warum dein Smart TV heimlich Screenshots macht und wie du dich davor schützt

**Wenn du etwas auf deinem Smart TV schaust, schauen auch Samsung und LG zu: Die Software auf den Fernsehern macht mehrmals pro Sekunde einen Screenshot. Zum Glück kannst du das Feature auch deaktivieren. Was du jetzt wissen musst.**

Smart TVs sind mittlerweile Standard in deutschen Haushalten. Dabei scheinen sie ein großes Problem zu haben: die Privatsphäre. Das hat ein internationales Forschungsteam herausgefunden.

Laut einer Studie von Wissenschaftler:innen aus Großbritannien, Spanien und den USA machen Smart TVs mehrmals pro Sekunde einen Screenshot – selbst, wenn User:innen externe Geräte wie eine Konsole oder einen Laptop via HDMI-Anschluss verwenden. Die Hersteller der Geräte nutzen neben den Bildern auch Audioaufnahmen für die sogenannte Automatic Content Recognition (ACR). So soll das Verhalten von User:innen getrackt werden, um gezielt Werbung auszuspielen.

Die Forscher:innen haben nur Geräte der Marken Samsung und LG getestet. Auch bei anderen Herstellern ist es sehr wahrscheinlich, dass die Geräte ähnliche Funktionen nutzen. Schon 2020 kritisierte das Bundeskartellamt die Hersteller vieler Smart TVs. Fast alle Geräte weisen „schwerwiegende Transparenzmängel“ auf. Diese würden gegen die Datenschutzgrundverordnung verstoßen.

In einem Statement gegenüber t3n begründet Samsung, dass der Einsatz von ACR dazu diene, „das Fernseherlebnis seiner Nutzer:innen zu verbessern.“ Zusätzlich würden die Daten „ausschließlich über eine anonymisierte Identifikationsnummer erfasst“ werden. Auch Bilder würde Samsung nicht speichern. LG verweist gegenüber t3n darauf, dass LG Ads als eigenständiges Unternehmen für personalisierte Werbung verantwortlich sei und losgelöst von LG Electronics Deutschland agiere.

### Smart TVs haben Probleme mit dem Datenschutz

Die Forscher:innen haben sich zwar nur mit Smart TVs aus den USA und Großbritannien beschäftigt, doch auch hier konnten sie regionale Unterschiede erkennen.

Während die untersuchten Samsung-Fernseher alle 500 Millisekunden einen Screenshot machten, schossen LG-Fernseher alle zehn Millisekunden ein Bildschirmfoto. Im Anschluss sendete Samsung jede Minute die gesammelten Screenshots an einen Server. Bei LG waren es alle 15 Sekunden.

Auf den Server werden aber nicht alle Screenshots hochgeladen. Wenn die Inhalte von Netflix oder anderen Drittanbieter-Apps stammen oder Youtube-Videos sind, die von einem Smartphone oder Laptop gespiegelt wurden, landen sie nicht auf den ACR-Servern. Anders sieht es aus, wenn man Antennenfernsehen schaut oder Geräte nutzt, die via HDMI-Anschluss mit dem Fernseher verbunden sind.

### So macht dein Smart TV keine Screenshots mehr

Doch es gibt auch eine Lösung: Wer keine Screenshots von seinem Smart TV an Samsung und LG senden möchte, kann in den Datenschutzeinstellungen das ACR-Tracking abstellen. Dazu müssen die Kund:innen laut der Studie jedoch zwischen sechs und elf verschiedene Optionen in den TV-Einstellungen aktivieren oder deaktivieren.

Bei Samsung findet sich die Einstellung unter dem Aspekt „Support“ und „Nutzungsbedingungen“. Hier sollten Nutzer:innen die „Viewing Information Services“ deaktivieren. Bei LG versteckt sich das ACR hinter dem Namen „Live Plus“.

Quelle: https://t3n.de/news/warum-smart-tv-heinlich-screenshots-davor-schuetzen-1648307/

# 16) Schutz Ihrer Privatsphäre in WhatsApp: Ein einfacher Schalter für sichere Anrufe

**Sichere Anrufe dank einer kleinen Einstellung: Es gibt in WhatsApp eine Funktion, die gut versteckt ist und daher kaum genutzt wird.**

Meta lobt sich gern selbst für Sicherheit und Datenschutz in WhatsApp. So auch wieder in einem aktuellen Blog-Posting zu neuen Funktionen. Und bei aller Kritik, die man an dem Messenger üben kann, hat WhatsApp gezeigt, wie unkompliziert man zum Beispiel Ende-zu-Ende-Verschlüsselung an den Start bringen kann.

Doch es gibt noch Verbesserungspotenzial und **seit Oktober 2023** wird eine neue Funktion verteilt, die die IP-Adresse von Handys schützen soll. Sie ist mittlerweile bei sehr vielen WhatsApp-Nutzern angekommen, ist aber optional. Das bedeutet, Nutzer müssen den IP-Schutz explizit einschalten.

### IP-Adresse bei WhatsApp schützen

In WhatsApp wird nicht nur fleißig getextet, sondern auch klassische Anrufe sind beliebt. Technisch sind das direkte Peer-to-Peer-Verbindungen zwischen den Teilnehmern. Vorteile sind eine schnellere Datenübertragung sowie bessere Gesprächsqualität.

Jedoch müssen die Anruf-Teilnehmer die IP-Adressen der anderen kennen, damit die Datenpakete an das richtige Gerät weitergeleitet werden können. Bei 1:1-Anrufen kriegt also Ihr Gesprächspartner auch Ihre IP-Adresse mit. Über die IP-Adresse lassen sich aber interessante Sachen herausfinden, etwa der geografische Standort oder Ihr Internetanbieter. Nicht umsonst verwenden viele Nutzer einen VPN-Dienst, um die IP-Adresse zu verbergen.

Eine neue Funktion in WhatsApp schützt jetzt auf Wunsch die IP-Adresse bei Anrufen. Wenn Sie sie aktivieren, werden alle Ihre Anrufe über WhatsApp-Server weitergeleitet. Statt Ihrer IP-Adresse sehen Gesprächspartner dann nur die Server-IP.

Wichtig: Anrufe sind wie auch Text-Chats bei WhatsApp immer Ende-zu-Ende-verschlüsselt. Auch wenn die Gespräche über WhatsApp-Server weitergeleitet werden, kann Meta nicht mithören.

### IP-Schutz aktivieren

Leider ist der Schutz der IP-Adresse etwas versteckt. Sie müssen in den Einstellungen den Punkt "Datenschutz" aufrufen und sich dann ganz nach unten bis zu "Erweitert" durchhangeln. Schalten Sie dann die neue Funktion "IP-Adresse in Anrufen schützen" ein.

Wichtig: WhatsApp gibt an, dass durch die Anrufweiterleitung möglicherweise die Anrufqualität leidet. Am besten Sie probieren es selbst aus. Sollte es zu Anrufproblemen kommen, klemmen Sie den Zusatz-Schutz wieder ab.

Quelle: https://www.chip.de/news/Schutz-Ihrer-Privatsphaere-in-WhatsApp-Ein-einfacher-Schalter-fuer-sichere-Anrufe_185019360.html?utm_source=flipboard&utm_content=topic%2Fde-digital

# 17) Ohne SIM-Karte: Satellite-App ermöglicht kostenlose Anrufe mit echter Handynummer

**Die Smartphone-App Satellite ist gratis und bringt Ihnen eine echte deutsche Handynummer, unter der Sie weltweit erreichbar sind und 100 Minuten kostenlos telefonieren können. Praktisch vor allem als Zweitnummer.**

Zum Handy gehört entweder eine klassische SIM-Karte oder die modernere Form als virtuelle eSIM, zumindest ist das die landläufige Meinung. Die kostenlosen Satellite-App zeigt, dass es auch anders geht. Einzige Voraussetzung für die Internettelefonie VoIP ist eine aktive Datenverbindung, etwa per WLAN oder über eine beliebige Daten-SIM.

Im Unterschied zu Messengern kriegen Sie bei Satellite aber eine **echte deutsche Handynummer**, die weltweit gültig ist und 100 Gesprächsminuten für eigene Telefonate enthält. Die App ist sowohl für Android als auch für iOS erhältlich und erlaubt Telefonate in 61 Länder.

Neu ist eine KI-Funktion, die Nutzer aber in den Einstellungen explizit aktivieren müssen. Dann kann Satellite den Inhalt von Telefonaten als kurzen Text zusammenfassen. Keinen Bock auf KI? Dann lassen Sie den Schalter einfach aus.

### Kostenlose Telefonie-App Satellite

Im Prinzip sind die Android-Version und die iOS-Version gleich aufgebaut, die App ist schick und aufgeräumt. Unterteilt ist die Anwendung in vier Reiter. Von links nach rechts sind das die Inbox, die Kontaktliste, der Ziffernblock zum Wählen einer Rufnummer und die Einstellungen. Die Sprachqualität ist gut und die Verzögerung nur gering.

Ursprünglich ist die Satellite-App angetreten, um SIM-Karten komplett zu ersetzen. Aktuell hat man eher das Ziel, sich als smarte Zweitnummer zu zeigen, auch wenn es grundsätzlich möglich ist, komplett auf Satellite zu setzen. Geld verdient wird über Bezahltarife, die sich an Geschäftskunden richten. Privatnutzer können im Free-Tarif bleiben. Vorteile:

- **Echte Telefonie:** Dank echter deutscher Handynummer klappt telefonieren nicht nur innerhalb der App. Sie sind von jedem Telefonanschluss aus zu erreichen und können auch jeden anrufen. Für die Erreichbarkeit muss die App auch nicht im Vordergrund sein.
- **Unabhängig vom Provider:** Mit Satellite sind Sie unabhängig von einem Mobilfukn-Provider. Sie können die SIM-Karte beliebig wechseln, Ihre Handynummer bleibt immer gleich.
- **Freiminuten:** Im kostenlosen Tarif sind 100 Minuten pro Monat in die Mobilfunk-/Festnetze von 61 Ländern der Welt enthalten. Reicht das nicht, können Sie eine Flatrate zubuchen.
- **Sicherheit:** Gespräche werden per SRTP und TLS verschlüsselt
- **Mehrere Geräte**: Die parallele Installation auf mehreren Geräten ist möglich

### Was kostet Satellite?

Satellite ist **kostenlos** und bietet pro Monat **100 Freiminunten** für Anrufe in 61 Länder weltweit. Für rund **5 Euro monatlich** gibt es mit **unbegrenztes Telefonieren**.

### SMS fehlt noch

Ein großer Vorteil von Satellite ist, dass Sie damit unabhängig vom Mobilfunkprovider telefonieren können bzw. erreichbar sind. Doch es sind noch nicht alle wichtigen Funktionen an Bord.

Einen Anrufbeantworter gibt es zum Beispiel, der kann in der kostenlosen Version von Satellite aber nur mit Standardansage genutzt werden. Die SMS-Funktion fehlt aber leider immer noch. Für Kurznachrichten zwischen Nutzern braucht man die auch nicht mehr wirklich und das wird wohl auch nicht in Satellite kommen.

Was aber auf jeden Fall bald starten soll, ist A2P-SMS (Application to Person), also Kurznachrichten zur Verifizierung und für Onlinebanking. Für WhatsApp & Co. lässt sich die Satellite-Nummer also nur per Anruf mit Code freischalten, Messenger-Apps, die ausschließlich eine SMS-Verifikation anbieten, lassen sich mit der Satellite-Telefonnummer also nicht nutzen.

Nicht nur angerufen werden, sondern auch Anrufe tätigen ist über Satellite möglich: 100 Freiminuten monatlich für Gespräche in alle unterstützten Netze weltweit sowie eine deutsche Handynummer (015678-Vorwahl) samt Voice-Mailbox sind kostenlos. Für rund fünf Euro ist eine monatliche Telefonie-Flatrate zubuchbar.

Quelle: https://www.chip.de/news/Ohne-SIM-Karte-Satellite-App-ermoeglicht-kostenlose-Anrufe-mit-echter-Handynummer_134263212.html?utm_source=flipboard&utm_content=topic%2Fde-digital

# 18) Microsoft bietet kaum bekanntes Datenrettungs-Tool: Völlig kostenlos zum Download

**Wenn wichtige Dateien versehentlich gelöscht werden, ist der Schock erstmal groß. Ein kaum bekanntes Profi-Tool von Microsoft schafft Abhilfe und stellt versehentlich gelöschte Dateien wieder her.**

Wer versehentlich den Windows-Papierkorb leert oder einen USB-Stick etwas zu schnell formatiert, muss danach manchmal schmerzlich feststellen, dass wichtige Dokumente plötzlich nicht mehr auffindbar sind. Hat man dann auch kein aktuelles Backup abgespeichert, sollten Sie aber die Flinte noch nicht ins Korn werfen. Dateien lassen sich oft recht schnell wiederherstellen.

Mit Windows File Recovery hat Microsoft hier das passende Hilfswekzeug am Start. Doch es gibt einen großen Haken: Das Tool kann leider nur über die Kommandozeile bedient werden. Wenn Sie das nicht abschreckt, haben wir unten die Anleitung für Sie. Mit einer zusätzlichen grafischen Oberfläche kann es aber jeder nutzen.

### WinfrGUI: Rettung mit grafischer Oberfläche

WinfrGUI ist für alle Nutzer eine Option, die nicht gerne die Kommandozeile verwenden. Sie müssen die Software nur zusätzlich zu Windows File Recovery installieren und können dann ganz einfach mit der Maus Dateien wiederherstellen. Das geht in drei Schritten:

1. Bereich auswählen, der durchsucht werden soll
2. Bereich zur Wiederherstellung festlegen
3. Scan-Modus wählen

Es gibt zwei Scan-Modi: Der "Quick Scan" arbeitet schneller und durchforstet nur intakte NTFS-Dateisysteme. Gefundene Dateien können samt Ordnerstruktur und Dateinamen wiederhergestellt werden. Außerdem läuft die Suche vergleichsweise schnell. Der "Deep Scan" arbeitet langsamer, unterstützt mehr Dateisysteme und holt auch Daten ohne Dateinamen aus der Versenkung.

**Windows File Recovery: Rettung auf Kommandozeile**

Sie können Windows File Recovery aber auch minimalistisch mit der Kommandozeile nutzen. Das funktioniert selbst dann, wenn eine Datei gelöscht und der Windows-Papierkorb geleert ist oder eine Speicherkarte neu formatiert wurde. Windows File Recovery kann Ihre HDD, SSD, USB-Sticks und Speicherkarten scannen und dabei viele gängige Dateitypen wiederherstellen. Laut Microsoft sind das unter anderem JPEG, PDF, PNG, MPEG, MP3, MP4, ZIP und Office-Dateien. Voraussetzung für die Verwendung des Tools ist mindestens das Windows Mai Update 2020 (Windows 10 2004) oder Windows 11.

Um Windows File Recovery zu verwenden, rufen Sie die Kommandozeile als Administrator auf. Suchen Sie dazu nach CMD auf Ihrem PC und wählen per Rechtsklick "Als Administrator ausführen". Geben Sie den Befehl ***winfr*** ein, sehen Sie, ob das Tool erfolgreich installiert wurde und erhalten eine Auflistung aller Parameter. Um beispielsweise alle aus dem Ordner "Downloads" gelöschten Dateien in einen Zielordner auf Laufwerk "D:" wiederherzustellen, wählen Sie den Befehl:

***winfr C: D:\Zielordner /regular /n Users\<Benutzername>\Downloads***

Windows File Recovery bietet die beiden Modi "regular" (Quick Scan) und "extensiv" (Deep Scan) an.

**Tipp der Redaktion:** Die Anwendung kann unter dem u.g. Link heruntergeladen, sowie ein Video angeschaut werden.

Quelle: https://www.chip.de/news/Microsoft-bietet-kaum-bekanntes-Datenrettungs-Tool-Voellig-kostenlos-zum-Download_182803310.html?utm_source=flipboard&utm_content=topic%2Fde-digital

# 19) News – Hacker nutzen Chrome im Vollbildmodus, um Google-Passwörter zu stehlen

**Ein Tipp vom Leser Dirk K.**

**Ein hinterhältiger neuer Angriff nutzt den Vollbild-Modus von Chrome, um Sie zur Eingabe Ihres Passworts zu zwingen, das dann gestohlen wird.**

Es gibt eine neue Hacking-Methode, die die Runde macht und die ebenso clever wie lästig ist. Einem neuen Bericht zufolge nutzen Angreifer den Kiosk-Modus von Chrome, um den Browser in den Vollbildmodus zu versetzen, der dann keine weiteren Aktionen zulässt, bis Sie Ihr Google-Passwort eingeben. An diesem Punkt wird Ihr Passwort natürlich gestohlen.

In einem Bericht von OALabs wird diese neuartige Angriffstaktik für den Diebstahl von Google-Anmeldedaten beschrieben. Es handelt sich eigentlich um eine Kombination aus zwei Techniken.

**So funktioniert die Taktik**

Zunächst lädt ein Windows-Programm eine gefälschte Google-Anmeldeseite in Chrome und aktiviert dann den Kiosk-Modus. Dabei handelt es sich um eine Benutzeroberflächenfunktion, die eine Seite im Vollbildmodus anzeigt und es Ihnen nicht erlaubt, zu anderen Programmen zu navigieren. Selbst fortgeschrittene Benutzer könnten Schwierigkeiten haben, dies zu umgehen, da einige Eingaben (wie F11 zum Verlassen des Vollbildmodus) deaktiviert sind.

Das Einzige, was Sie auf der Seite tun können, ist, einen Google-Login und ein Passwort einzugeben. Sobald Sie das getan haben, schnappt sich ein anderes Programm diese Anmeldedaten und schickt sie an einen entfernten Hacker weiter. Im schlimmsten Fall ändert der Hacker dann Ihr Passwort und sperrt Sie sofort von Google Mail und allen anderen Konten aus, die mit diesen Daten verknüpft sind, einschließlich der Dienste von Drittanbietern, die die Login-Plattform von Google nutzen.

Das ist ein hinterhältiger Doppelschlag für Identitätsdiebe. Zwar wurde beobachtet, dass das Tool speziell auf Chrome abzielt, aber es ist auch in der Lage, andere Browser mit ähnlichen Implementierungen des Kiosk-Modus zu verwenden.

**Das können Sie dagegen tun**

Erfahrene Windows-Benutzer können die Anmeldeaufforderung vielleicht umgehen. Die Tastenkombination **Strg + Alt + Entf** sollte Sie immer noch in den Task-Manager bringen, wo Sie zum Beispiel den Browser herunterfahren können. Aber diese Kombination von Tools ist so direkt und so lästig, dass selbst langjährige PC-Benutzer ihre Google-Passwörter vielleicht nur aus Reflex eingeben.

Wie immer gilt: Seien Sie vorsichtig, wenn Sie etwas herunterladen und achten Sie darauf, woher Sie es herunterladen. Und wenn Sie jemals unerwartet eine bildschirmfüllende Google-Anmeldeseite sehen, sollten Sie als Erstes (nachdem Sie ihr entkommen sind) einen guten Virenscan durchführen.

Quelle: https://www.pcwelt.de/article/2462846/hacker-nutzen-chrome-im-kiosk-vollbildmodus-um-google-passwoerter-zu-stehlen.html

# Allgemeines:

## 1) Kfz-Versicherung: Mit diesen Angaben sparen Sie sofort Geld

**Mit den richtigen Angaben bei der Kfz-Versicherung sparen Sie viel Geld.**
**Ein Überblick über Kostenfallen und Sparpotenziale.**

Nicht vergessen: Bis zum 30.11.2024 müssen Sie Ihre Kfz-Versicherung wechseln, damit Sie Geld sparen. Was Sie beim Versicherungswechsel beachten müssen, lesen Sie hier. Doch aufgepasst: Autofahrer können die Kosten der Kfz-Versicherung entscheidend beeinflussen. Die Angaben beim Abschluss des Vertrages können den Beitrag verdoppeln oder deutlich senken, wie das Verbraucherportal Verivox betont.

**Ist der Fahrerkreis noch aktuell?** Niedrige Kosten lassen sich erreichen, wenn der Fahrerkreis auf den Versicherungsnehmer beschränkt ist. Teuer wird es, wenn man beispielsweise angibt, dass auch eine 18-jährige Person das Auto fährt. Durch Letzteres kann sich die durchschnittliche Versicherungsprämie fast verdoppeln.

Wer junge Fahrer mitversichert, zahlt einen hohen Risikoaufschlag. Wenn der Nachwuchs später ein eigenes Auto hat, ist das oft nicht mehr notwendig, so Verivox. In diesem Fall sollten Sie diese teure Option aus Ihrem Vertrag streichen lassen.

**Entspricht die Fahrleistung der Wirklichkeit?** Auch die jährlich zurückgelegten Kilometer haben großen Einfluss auf die Versicherungsprämie. Bei einer Fahrleistung von 5.000 Kilometern sinkt sie deutlich gegenüber einer Fahrleistung von 15.000 Kilometern. Daher sollten Autofahrer jährlich prüfen, ob die bei der Versicherung angegebenen Kilometer noch stimmen.

**Wurden möglicherweise Rabatte verpasst?** Kleine Zusatzangaben können die jährlichen Kosten deutlich mindern. Wer angibt, Beamter zu sein, kann die Prämie um etliche Prozent senken. Besitzer einer Garage erhalten ebenfalls einen Rabatt, ebenso wie oft auch Besitzer einer Bahncard. Der Besitz eines Eigenheims wird ebenfalls mit einem Preisnachlass berücksichtigt, um einige Beispiele zu nennen.

**Freie Werkstattwahl wirklich notwendig?** Wird das Fahrzeug im Schadensfall zu einer Partnerwerkstatt des Versicherers gebracht, sinkt die Jahresprämie bedeutend. Viele Versicherer verfügen über ein umfassendes Netz an Partnerwerkstätten und der Wagen wird unter Umständen geholt und gebracht. Wer selbst entscheiden möchte, wo das Auto repariert wird, zahlt durchschnittlich 14 Prozent mehr.

**Mehr Leistung kostet?** Eine Reihe von zusätzlichen Tarifleistungen verbessert den Versicherungsschutz, doch dadurch erhöht sich natürlich auch die jährliche Versicherungsprämie. Wer sich zum Beispiel für einen erweiterten Wildschutz entscheidet sowie Folgeschäden von Marderbissen und grobe Fahrlässigkeit mit absichert, zahlt einen Aufschlag.

Der Rabattschutz bei Kasko-Versicherungen verhindert die Rückstufung in eine teurere Schadenfreiheitsklasse im Schadensfall. Er erhöht jedoch die jährlichen Kosten deutlich.

**Falsche Angaben lohnen sich nicht** : Die lockenden Vergünstigungen sollten Verbraucher jedoch niemals dazu verleiten, gegenüber der Kfz-Versicherung falsche Angaben zu machen. Im Fall der Fälle können ansonsten Teile des Versicherungsschutzes verloren gehen und hohe Zusatzkosten drohen.

Quelle:https://www.pcwelt.de/article/1155904/kfz-versicherung-mit-diesen-angaben-sparen-sie-geld.html?utm_date=20241030112201&utm_campaign=Best-of%20PC-WELT&utm_content=slotno4-title-Kfz-Versicherung%3A%20Mit%20diesen%20Angaben%20sparen%20Sie%20sofort%20Geld&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

# 2) Achtung, Betrüger – Winterreifen: Vorsicht bei diesen Onlineshops

**Verlockende Angebote, unschlagbare Preise – doch hinter Reifen-Deals im Internet lauert oft eine böse Überraschung. Verbraucherschützer schlagen Alarm: Diese Fake-Shops bringen Sie um mehr als nur Ihr Geld.**

Der Onlinehandel mit Autoreifen boomt – leider auch bei Betrügern. Immer mehr Fake-

Shops locken mit unschlagbaren Preisen für Reifen und Autozubehör. Doch wer hier kauft, sieht weder Ware noch Geld wieder.

### Wie läuft die Masche der Betrüger?

Die Fake-Shops sehen täuschend echt aus. Alles wirkt seriös, die Preise sind verlockend niedrig. Doch wer bestellt, wartet vergebens. Das Geld ist weg, die Reifen kommen nie an.

### Welche Shops stehen auf der schwarzen Liste?

Die Verbraucherzentrale Hamburg warnt aktuell vor folgenden Fake-Shops

- :autoreifen-binder.shop
- bct-reifen.de
- bernhardt-reifenhandel.shop
- debica-reifen.de
- eberhardt-reifenhandel.com
- kopp-reifenhandel.shop
- lorenz-reifen.com
- opitz-reifenhandel.shop
- raab-reifen.com
- reifenhandel-rau.com
- reifen-glaser.de
- reifenhandel-albrecht.com
- reifenhandel-bach.com
- reifenhandel-kilian.shop
- reifen-motredu.de
- reifen-petlas.de
- reifen-reichert.com
- reifenversand-voigt.com
- reifenversand-weber.com
- reifen-ziemann.com
- roth-reifenversand.shop
- uhlig-autoreifen.shop
- voss-reifenversand.com
- weber-reifen.com
- zenlo-reifen.de

### Wie erkenne ich Fake-Shops?

Fake-Shops lassen sich an einigen typischen Merkmalen erkennen. Achten Sie besonders auf ein fehlendes oder unvollständiges Impressum, eine fehlende Handelsregisternummer und nicht erreichbare Telefonnummern. Ein weiteres Warnsignal ist, wenn nur Vorkasse als Zahlungsoption angeboten wird. Oft locken diese Shops zunächst mit verschiedenen Zahlungswegen, doch an der Kasse bleibt nur die riskante Überweisung.

### Wie schütze ich mich vor Betrug?

Um sich vor Betrug zu schützen, hilft eine kurze Recherche. Geben Sie den Shop-Namen in eine Suchmaschine ein und prüfen Sie die angegebene Adresse mit einem Kartendienst. Versuchen Sie auch, die angegebene Telefonnummer anzurufen. Seien Sie grundsätzlich misstrauisch bei extrem günstigen Angeboten.

### Was tun, wenn man hereingefallen ist?

Sollten Sie trotz aller Vorsicht Opfer eines Fake-Shops geworden sein, handeln Sie schnell. Informieren Sie sofort Ihre Bank – möglicherweise lässt sich die Überweisung noch stoppen. Erstatten Sie Anzeige bei der Polizei und melden Sie den Vorfall der Verbraucherzentrale.

Quelle: https://www.t-online.de/mobilitaet/reifen/winterreifen/id_100165626/reifen-fake-shops-verbraucherschuetzer-warnen-vor-betrugsmasche.html

# 3) Produktrückrufe – Fundstellenverzeichnis

**Die Idee eines zentralen Informationsportals zur Bekanntmachung von Rückrufaktionen, Produktwarnungen, Sicherheitshinweisen & mehr ist erstmals im Jahr 2007 durch einen einzelnen Verbraucher entstanden. Primäres Ziel: Betroffene durch einfach aufzufindende Informationen vor Schaden bewahren.**

Inzwischen hat sich diese Internetseite für namhafte Hersteller- und Handelsunternehmen zu einem **Presseportal für sicherheitsrelevante Verbraucherinformationen** entwickelt. Zudem dient "produktrueckrufe.info" nicht mehr alleine Konsumenten, sondern auch vielen weiteren "Interessengruppen" als Fundstelle: u. a. zur "Weiterverarbeitung" durch Medien (oft ohne Quellenangabe), zur Wettbewerbsbeobachtung durch Unternehmen bspw. für Zwecke der eigenen Qualitätssicherung und ... zur sog. "Marktüberwachung" durch Behörden.

**Tipp der Redaktion:** Einfach mal reinschauen und ev als Lesezeichen hinterlegen.

Quelle: https://www.produktrueckrufe.info/

# 4) Neun Direktsäfte im Test – Apfelsaft: viele gute Produkte, auch viele günstige

**Apfelsaft ist gesund, natürlich und regional. Könnte man denken. Ganz so leicht ist es aber nicht. Denn Pestizidrückstände und saftige Preise verderben den Trinkgenuss.**

Nirgends wird so viel Saft und Fruchtnektar getrunken wie in Deutschland – 2023 waren es durchschnittlich 26 Liter im Jahr pro Person. Damit sind wir Deutschen Weltmeister im Safttrinken. Aber was steckt im Saft eigentlich drin? Wie gesund ist er? Und wo kommt er her? Eine Klärung - am Beispiel von Apfelsaft. Von dem trinkt jeder Deutsche immerhin rund fünf Liter pro Jahr.

Hier finden Sie den Film zum Artikel in der ARD-Mediathek: Apfelsaft: nur Bio-Produkte frei von Pestizidrückständen

### Enorme Preisspanne bei Apfelsäften

Das Angebot ist riesig: aus konventionellem Anbau oder in der Bio-Variante, in klar oder naturtrüb. Wir haben neun Produkte getestet, darunter sechs konventionelle und drei Bio-Produkte aus Supermärkten und Discountern. Alle aus 100 Prozent Direktsaft, alle naturtrüb. Wie schneiden sie in der Geschmacksstichprobe ab? Wie im Labortest? Und wie steht es um die Nährwerte?

Die günstigsten Apfelsäfte in der Stichprobe sind ein Apfelsaft von **Penny** für 1,19 Euro, einer von **Netto** für 1,29 Euro und einer von **Edeka** für 1,49 Euro pro Liter. Daneben sind Markenprodukte von **Beckers Bester** für 2,29 Euro, von **Amecke** für 2,49 Euro und von

**Rauch** für 2,79 Euro im Test. Die untersuchten Bio-Säfte sind von **Rewe** (1,39 Euro), **Voelkel** (2,84 Euro) und **Bauer** - mit 3,56 pro Liter ist er der teuerste Saft im Test. Kann der etwas, was die anderen nicht können?

### Qualität ist, wenn der Saft wie ein Biss in den Apfel schmeckt

Achim Fießinger ist Geschäftsführer der Mosterei Ketzür im Brandenburger Betzseeheide. Für ihn ist klar: "Du musst das Glas nehmen, musst trinken und sagen, ja, das schmeckt genauso wie ein Apfel, wenn ich reinbeißen würde." Der Apfelfachmann mostet in seinem Betrieb ausschließlich regionale Äpfel von Bauern oder Privatkunden.

Und das geht so: Nach einer gründlichen Wäsche werden die Äpfel geschreddert, die entstandene Maische wird gepresst und heraus kommt der naturtrübe Saft. Bei Fießinger wird der Saft nur aufs Nötigste gefiltert. Alle anderen Trübstoffe, die sonst auch im Apfel sind, bleiben erhalten. Damit der frische Saft länger hält, wird er auf etwa 80 Grad erhitzt. Ein Kilo Äpfel ergeben je nach Sorte bis zu 0,7 Liter Saft, so Fießingers Erfahrung.

### Herkunft der Äpfel muss nicht angegeben werden

Anders als bei Fießinger ist auf den Verpackungen der Test-Säfte die Herkunft der Äpfel nicht angegeben. Laut Britta Schautz, Ernährungsexpertin der Verbraucherzentrale Berlin, ist das vollkommen in Ordnung. Werden verarbeitete Lebensmittel verkauft, ist es erlaubt, die Herkunft der Zutaten nicht zu deklarieren. Eine Pflicht besteht in dem Fall also nicht, viele Kunden wünschen sich diese Angabe allerdings.

Auf Nachfrage, wo die verwendeten Äpfel herkommen, antworten sieben der neun Saft-Hersteller. Ausschließlich deutsche Äpfel sind nur in den Säften von Völkel und Rauch. Die Äpfel für die anderen Säfte kommen aus Deutschland, Polen, Österreich, Italien oder Tschechien.

Edeka schreibt dazu: "Aufgrund der erschwerten Erntebedingungen (…) und zur Sicherstellung der Warenverfügbarkeit ist es derzeit nicht möglich, ausschließlich Äpfel aus deutschem Anbau zu verwenden."

### Ernteschäden treiben Preise in die Höhe

Tatsächlich fiel die deutsche Ernte in diesem Jahr um etwa 25 Prozent schlechter aus als im Jahr zuvor. In Hessen, Thüringen, Sachsen, Sachsen-Anhalt und Brandenburg ist die Situation noch schlechter: Durch massive Frostschäden brach die Ernte dort um bis zu 90 Prozent ein. Auch in Polen zerstörte der Frost viele Äpfel - der Verband der deutschen Fruchtsaft-Industrie erwartet deshalb drastische Preissteigerungen. Klaus Heitlinger ist Geschäftsführer des Verbands, er schätzt, "dass der Apfelsaft ein Drittel bis 50 Prozent teurer werden wird gegenüber dem Vorjahr".

Dabei sind einige konventionelle Säfte schon in den vergangenen zwei Jahren deutlich teurer geworden: Der Preis für den Amecke-Apfelsaft stieg zum Beispiel von durchschnittlich 1,79 auf 2,49 Euro. Ein Anstieg von fast 40 Prozent.

### Pestizide in allen konventionellen Säften

Ein stolzer Preis. Und wofür zahlen wir den? Im Labor wird ausgewertet, was in den getesteten Säften drinsteckt. Alle Säfte wurden auf fünf verschiedene Pestizidrückstände getestet. In den Biosäften wurde keine gefunden. Dafür aber in allen konventionellen Säften.

In den meisten Säften sind zwei oder drei verschiedene Rückstände nachweisbar. In dem von Rauch sogar vier. Der Hersteller antwortet auf Anfrage, es gebe laufende Kontrollen. Beim Anbau der Äpfel würden im Rahmen des Erlaubten Pestizide eingesetzt.

Ernährungsexpertin Britta Schautz ist von den Ergebnissen nicht überrascht. "Das Problem ist, dass sich Pestizide in ihrer negativen Wirkung auf die Gesundheit verstärken könnten." Heißt: Sind verschiedene Reste der sogenannten Pflanzenschutzmittel drin, kann die Wirkung des einen durch das andere noch verschlimmert werden. Allerdings lagen alle ermittelten Werte weit unter den gesetzlichen Grenzwerten. Laut Schautz sei die gute Nachricht - auch bei den Produkten mit Mehrfachrückständen - dass die Rückstände so gering waren, dass diese wahrscheinlich trotzdem kein Problem darstellen und die Säfte sicher sind.

Was in jedem Fall festgehalten werden kann: Teure Markensäfte schneiden bei den Pestizidrückständen nicht besser ab als günstige No-Name-Produkte.

### Preisexplosion auch durch Pestizideinsatz

Der Pestizideinsatz schlägt sich sogar im Preis nieder. Leider sorgt er aber nicht für günstigere Preise, das Gegenteil ist der Fall. „Ich brauche, um konventionell Äpfel herzustellen, relativ viele Pestizide und auch Düngemittel“, erläutert Britta Schautz. Diese Produkte seien energieaufwendig und daher teuer in der Herstellung. „Gerade in den letzten Jahren sind die teurer geworden - und das spiegelt sich natürlich im Preis des Saftes wider“, erläutert die Verbraucherschützerin.

Anders ist es bei Bio-Produkten, die kommen nämlich ohne chemisch-synthetische Pestizide aus. Dieser Umstand führt dann zum Beispiel dazu, dass der Bio-Apfelsaft von Rewe im Preis sank: von durchschnittlich 1,69 auf 1,39 Euro, ein Minus von gut 18 Prozent.

### Günstiger und gesünder wird der Saft als Schorle

In der Geschmacksstichprobe in einer Gruppe von Feuerwehrleuten, die hier gern einmal ihren Durst löschten, statt Feuer, schneiden sowohl ein Markensaft als auch ein günstiger am besten ab, der Saft von Amecke für 2,49 und der von Netto für 1,29. Auch hier gilt also: Der Preis macht nicht den Unterschied. Günstige Säfte können eine gute Alternative für alle sein, die auf Apfelsaft nicht verzichten wollen.

Aber egal ob konventionelle Säfte oder biologische, ob teuer oder günstig: In einem Liter Apfelsaft stecken etwa 37 Würfel Zucker. Das ist zwar Fruchtzucker - aber auch der ist in großen Mengen ungesund. Die Deutsche Gesellschaft für Ernährung empfiehlt daher, Apfelsaft lieber stark verdünnt als Schorle zu trinken.

Quelle: https://www.swr.de/verbraucher/ard-marktcheck/apfelsaft-im-test-bio-konventionell-100.html