47. Cybercrime Newsletter

29.04.2025

1) Kriminelle Kaufangebote Vorsicht Falle: Mercedes-Benz warnt vor Betrugsmasche

Die Täter nutzen den Namen von Mercedes-Benz, um an das Geld der Kundschaft zu kommen. Es sind bereits potenzielle Autokäufer den gefälschten Verträgen und Rechnungen zum Opfer gefallen.

Das per E-Mail eingegangene Angebot klingt verlockend. Ein Mercedes zum Schnäppchenpreis, deutlich unter den marktüblichen Konditionen. Und auf den ersten Blick scheint die Sache auch seriös zu sein. Der Absender, die beigefügten Informationen und der Kaufvertrag sind wie aus einem Mercedes-Benz-Guss. Auch die Standorte und die Ansprechpartner, auf die im Schreiben verwiesen wird, geben zunächst einmal keinen Anlass am Angebot zu zweifeln.

Und doch ist alles nur ein einziger großer Betrug. Denn die so bundesweit zum Verkauf angebotenen Mercedes-Fahrzeuge sind nichts Anderes als eine kriminelle Erfindung. „Mercedes-Benz bedauert, dass Kundinnen und Kunden durch diese Masche bereits geschädigt wurden“, schreibt der Konzern in einer Stellungnahme.

Mercedes erstattet Anzeige wegen Betrugs

Offenbar haben die Betrogenen den Tätern Geld überwiesen beziehungsweise Bankdaten übermittelt. Betroffene können sich in diesem Fall an jede Polizeidienststelle wenden. Der Konzern hat Strafanzeige unter anderem wegen Betrugs und Urkundenfälschung erstattet und unterstützt nach eigenen Angaben die Ermittlungen der Behörden.

Betrügereien mit teuren Autos sind indes kein Einzelfall. Er kürzlich hatte Porsche vor einer ähnlichen Masche gewarnt. Es wurden unter anderem gefälschte Kataloge verschickt.

Bei Verdachtsfällen und Unsicherheiten empfiehlt Mercedes-Benz, sorgfältig zu überprüfen, ob es sich beim Absender einer E-Mail um einen autorisierten Mercedes-Benz-Partner handelt. Im Zweifel kann man sich an das Customer Assistance Center von Mercedes-Benz (Hotline: 00800 977 77777) wenden.

Mercedes rät: Fahrzeuge vorher ansehen

Mercedes warnt weiter: „Im Falle eines verdächtigen Angebots oder bei Unsicherheiten sollte vor jeglicher Zahlung oder Weitergabe persönlicher Daten stets Rücksprache mit einem autorisierten Mercedes-Benz-Händler oder der Kundenhotline gehalten werden.“ Der Konzern rät, dass insbesondere bei Unsicherheit keine Zahlungen vorabgeleistet werden sollten, ohne das Fahrzeug gesehen zu haben.

Quelle: https://www.stuttgarter-zeitung.de/inhalt.kriminelle-kaufangebote-vorsicht-falle-mercedes-benz-warnt-vor-betrugsmasche.42dc40a8-e7d7-4ccc-b9b0-c4d5cc36280e.html

2) Warnung vor „Kontosperrung“: Millionen Amazon-Kunden droht Gefahr

Amazon-Kunden befinden sich aktuell im Visier von Betrügern. Eine vermeintliche Kontosperrung soll sie dazu bringen, ihre Daten preiszugeben.

Aktuell erhalten zahlreiche Verbraucher E-Mails, die angeblich von Amazon stammen und mit einer sofortigen Kontosperrung drohen. Die Verbraucherzentrale warnt: Hinter diesen Nachrichten stecken Kriminelle. Jährlich entstehen hohe finanzielle Schäden durch die Masche.

Warnung vor „Kontosperrung“: Millionen Amazon-Kunden droht Gefahr

In der sogenannten Phishing-Mail wird behauptet, das Amazon-Konto sei vorübergehend gesperrt und alle Bestellungen oder Abonnements seien storniert worden. Um den Zugang wiederherzustellen, sollen Empfänger einem Link folgen und persönliche Daten eingeben. Die Nachricht wirkt auf den ersten Blick professionell, weist jedoch typische Merkmale von Phishing auf: Die Anrede erfolgt mit der Mailadresse, es wird mit einer schnellen, dauerhaften Sperrung gedroht und eine sehr kurze Frist von nur drei Tagen gesetzt.

Dringende Warnung an Amazon-Kunden: So erkennen Verbraucher Phishing-Mails

Phishing-Mails, wie zuletzt auch eine an Kunden der Telekom versandt wurde, sind inzwischen oft täuschend echt gestaltet. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sollten Empfänger besonders dann misstrauisch werden, wenn eine E-Mail mindestens eines der folgenden Merkmale aufweist:

- Dringender Handlungsbedarf oder **Drohungen** wie beispielsweise eine Kontosperrung
- Aufforderung zur **Eingabe vertraulicher Daten** über einen Link oder ein Formular
- Die Mail scheint zwar von einer bekannten Organisation zu stammen, doch das **Anliegen ist ungewöhnlich**
- **Enthaltene Links** führen auf gefälschte Webseiten, die oft nur schwer vom Original zu unterscheiden sind


amazon.de

Hallo [redacted]

Wir haben Ihr Amazon-Konto vorübergehend gesperrt und alle ausstehenden Bestellungen oder Abonnements storniert, da ungewöhnliche Aktivitäten festgestellt wurden.

Um den Zugang zu Ihrem Konto wiederherzustellen, klicken Sie bitte auf die Schaltfläche unten und folgen Sie den Anweisungen auf dem Bildschirm. Sobald Sie die erforderlichen Informationen bereitgestellt haben, werden wir Ihre Anfrage prüfen und innerhalb von 24 Stunden antworten.

Wenn der Konto-Wiederherstellungsprozess nicht innerhalb von 3 Tagen abgeschlossen wird, kann Ihr Amazon-Konto dauerhaft gesperrt werden.

Wir entschuldigen uns für etwaige Unannehmlichkeiten. Vielen Dank für Ihre Aufmerksamkeit und Ihr Verständnis.

Mit freundlichen Grüßen,
Das Amazon-Support-Team

In Amazon einloggen

amazon.de

Mit dieser E-Mail versuchen Kriminelle derzeit offenbar an Daten von Amazon-Kunden zu gelangen. © Verbraucherzentrale

Selbst korrekte Sprache und professionelle Gestaltung bieten keine Sicherheit mehr. Auch SSL-verschlüsselte Webseiten („https://“) sind kein Garant für Echtheit, da Betrüger solche Zertifikate mittlerweile ebenfalls nutzen.

Aktuelle Warnung an Amazon-Kunden: Nachricht sofort löschen

Wer eine Phishing-Mail erhält, sollte keinesfalls auf Links klicken oder persönliche Daten eingeben. Die Verbraucherzentrale empfiehlt stattdessen, verdächtige Nachrichten unbeantwortet in den Spam-Ordner zu verschieben.

Bei Unsicherheiten im aktuellen Fall hilft ein Blick in das eigene Amazon-Konto über die offizielle Webseite oder App – echte Warnungen und Handlungsaufforderungen sollten dort ebenfalls zu finden sein.

Angriff per E-Mail auf Amazon-Kunden: Phishing sorgt jährlich für Schaden in Millionenhöhe

Phishing ist eine der häufigsten Methoden von Cyberkriminellen, um an Passwörter und Zahlungsdaten zu gelangen. Die volkswirtschaftlichen Schäden durch Phishing und andere Cyber-Delikte werden in Deutschland jährlich auf einen zweistelligen Millionenbetrag geschätzt.

Neben finanziellen Verlusten drohen auch Identitätsdiebstahl und der Missbrauch persönlicher Daten. Laut aktuellen Studien sind rund 13,5 Prozent der Deutschen innerhalb eines Jahres Opfer von Cyberkriminalität geworden – Tendenz steigend.

Quelle: https://www.ruhr24.de/service/amazon-konto-warnung-kontosperrung-kunden-drohung-mail-phishing-finanzen-gefahr-daten-link-93695542.html

3) Per Telefon – Betrüger zocken vermehrt Pflegebedürftige ab

Pflegebedürftige werden zunehmend zum Ziel krimineller Aktivitäten, warnen Verbraucherschützer. Eine neue Masche löst besondere Verunsicherung aus.

Vor einer äußerst perfiden Betrugsmasche warnen Verbraucherschützer derzeit. Laut einer Mitteilung der Verbraucherzentrale Nordrhein-Westfalen haben Kriminelle es vermehrt auf pflegebedürftige Personen abgesehen.

Die Betrüger rufen diese an, um ihnen Pflegeleistungen anzubieten, für die normalerweise die Pflegekasse aufkommt und die für die Betroffenen somit kostenlos sind. Die Kriminellen rechnen die Leistungen anschließend von der Kasse ab.

Unbemerkt abgeschlossene Verträge

Dabei geben sich die Betrüger meist als Vertreter offizieller Stellen aus und nutzen das Unwissen der Pflegebedürftigen gezielt aus. Die Betroffenen, häufig allein lebende und ältere Menschen, wissen oft nicht, wie sie reagieren sollen. Die Folge: Verträge werden unbemerkt abgeschlossen und Leistungen bezogen, die gar nicht benötigt werden. Und die Kasse zahlt.

Welche Leistungen betrifft das? "Besonders häufig werden Pflegekurse für pflegende Angehörige und Pflegeboxen mit sogenannten Pflegehilfsmitteln zum Verbrauch aufgedrängt", berichtet die Verbraucherzentrale NRW. Dadurch entstehen nicht nur erhebliche finanzielle Schäden für das Pflegesystem. Auch die betroffenen Pflegebedürftigen bleiben oft verunsichert zurück.

Am besten sofort auflegen

Pflegerechtsexpertin Verena Querling erklärt, wie man sich vor solchen Anrufen schützen

kann. "Das Wichtigste ist, sofort aufzulegen", rät sie. Dadurch werde verhindert, dass die Angerufenen in ein Gespräch verwickelt werden und versehentlich oder absichtlich ein Angebot annehmen.

Ist es zu einem Vertragsabschluss gekommen, soll der Betroffene laut Querling sofort Kontakt mit der Pflegekasse aufnehmen, um Zahlungen zu stoppen. Bei Zahlungsaufforderungen oder Mahnungen sei rechtlicher Beistand ratsam, so die Pflegerechtsexpertin.

Woher die Betrüger die Kontaktdaten der Betroffenen haben, ist unklar. Firmen sind verpflichtet, auf Anfrage Auskunft über gespeicherte Daten zu geben. Betroffene sollten dies schriftlich einfordern und eine Sperrung der Daten verlangen, rät die Verbraucherzentrale NRW weiter.

Quelle: https://www.t-online.de/digital/aktuelles/id_100692968/betrugsmasche-am-telefon-kriminelle-zocken-pflegebeduerftige-ab.html

4) Datenschutz-Albtraum: Über 216.000 Samsung-Kundendaten im Netz – bist du betroffen?

Die Daten von zahlreichen deutschen Samsung-Nutzer:innen sind durch einen Cyberangriff im Netz gelandet. Ob ihr davon betroffen seid, könnt ihr jetzt in wenigen Augenblicken selbst überprüfen.

Schon Anfang April 2025 wurde ein Cyberangriff auf Spectos bekannt, bei dem Hacker:innen personenbezogene Daten von Samsung-Kund:innen entwenden konnten. Spectos stellt eine Software für das Kundenmanagement bereit, über die beispielsweise Support-Tickets bearbeitet werden können. Von dem Angriff waren insgesamt mehr als 216.000 Kundendaten betroffen.

Samsung-Datenleck: So könnt ihr überprüfen, ob ihr betroffen seid

Wie Heise berichtet, konnte der Betreiber der Website Have I Been Pwned eine Kopie der gestohlenen Daten erwerben. Demnach befanden sich unter den Daten unter anderem E-Mail-Adressen, Klarnamen und Adressen sowie Support-Anfragen von Samsung-Kund:innen. Zudem beinhalten die Daten auch abgeschlossene Käufe und Sendungsverfolgungsnummern. Diese Daten reichen zwar nicht aus, damit Cyberkriminelle sich Zugriff auf eure Konten verschaffen können, doch bergen sie ein anderes Risiko. Sie können für eine Reihe von verschiedenen Phishing-Angriffen genutzt werden, um euch Malware unterzujubeln oder euch weitere sensible Daten zu entlocken. Dementsprechend sollten Samsung-Kund:innen prüfen, ob sie von dem Datenleck betroffen sind.

Das ist dank des Projekts Have I Been Pwned denkbar einfach. Ihr müsst lediglich die Datenbank aufrufen und die E-Mail-Adresse in das Suchfeld eingeben, die ihr für euren Samsung-Account nutzt. Im Anschluss wird die Adresse mit den vorhandenen Daten aus einer Reihe von Leaks und Cyberangriffen abgeglichen. Taucht sie in einem Datenpaket auf, müsst ihr handeln.

Wurde eure E-Mail-Adresse im Netz geleakt, solltet ihr schnellstmöglich eine neue Adresse einrichten und anschließend alle eure Logins darauf ummelden. Lasst ihr die E-Mail-Adresse verfallen, nützt sie den Angreifer:innen auch nichts mehr. Euch vor der Nutzung der anderen Daten aus dem Leak abzusichern, ist deutlich schwerer. Aber in der Regel können die Angreifer:innen mit den anderen Daten weniger anstellen.

Quelle: https://t3n.de/news/216000-samsung-kundendaten-im-netz-1683273/

5) YouTube-Videos liken für 1.000 Euro am Tag? So läuft der WhatsApp-Betrug

Heute wurde ich über Whatsapp angeschrieben. Bis zu 1.000 Euro könnte ich am Tag mit dem Anschauen von Youtube-Videos verdienen. Hier das Protokoll des Gesprächs mit einem Online-Betrüger.

„Hallo , Kann ich mit dir reden?“

Diese Nachricht erhielt ich heute Morgen über Whatsapp. Von einer mir unbekannten Telefonnummer versendet. Immer wieder hört man von Betrügern, die über Whatsapp die Nutzer hereinlegen wollen. Die Nummern beschaffen sich solche Betrüger aus dubiosen Quellen. Da scheint wohl auch meine Nummer dabei gewesen zu sein. Mist.

„Mal sehen, wie so ein Gespräch verläuft“, dachte ich mir also und nahm mir die Zeit für ein Gespräch mit der mir unbekannten Person.

Ich: *„Wer bist Du denn?“*

Fragte ich also zurück. Wenige Sekunden später kam dann die Antwort des vermutlichen **Betrügers**:

> *Ich habe gute Neuigkeiten für Sie. Können Sie sich ein paar MinutenZeit nehmen?*
>
> *Ich arbeite für eine Werbeagentur in Großbritannien. Wir stellen derzeit Teilzeitkräfte ein, um YouTube-Videos zu bewerben.*
>
> *Sie können 500–1000 EUR pro Tag verdienen, indem Sie sich kurze Videos von YouTubern ansehen.*
>
> *Bei Interesse können Sie jetzt am Aufgabentest teilnehmen.*

Ah, die gute alte **Sie-können-unheimlich-viel-Geld-mit-wenig-Arbeit-verdienen-Masche.** Mal schauen, wie die abläuft.

Ich: „Wie sieht der Aufgabentest aus?“

Der Gesprächspartner antwortete mit einem Screenshot …

… und der Anleitung:

> *Die Aufgabe ist ganz einfach: Ich werde Ihnen einen YouTube-Videolink oder den Benutzernamen des YouTubers zur Verfügung stellen.*
>
> *Du musst dich nicht registrieren oder einloggen, einfach liken und mir einen Screenshot schicken und du erhältst 10Eur*
>
> *Durch weitere Kooperationen können Sie zwischen 500 und 1000 Euro pro Tag verdienen.*

Wir sind also wieder beim „Du“, ich blieb trotzdem beim „Sie“.

> **Ich**: „Haben Sie ein Beispiel für so einen Youtube-Videolink?“

Betrüger:

Ja. Ich werde einen YouTube-Link und einen Kanalnamen angeben.

YouTuber-Benutzername: @ansleytaylor

Sie müssen das Video nicht bis zum Ende ansehen. Klicken Sie auf „Gefällt mir “ und schicken Sie mir einen Screenshot. Sie können 10 Provisionen abheben.

Ich:

„Und was muss ich tun, um das Geld dann zu erhalten von Ihnen?“

Betrüger:

„Like und abonniere unseren YouTube-Kanal und schicke mir einen Screenshot. Sobald du den Screenshot absendest, erhältst du die Provision.“

Ich legte also einen Fake-Account bei Youtube an und antwortete mit einem Screenshot, der belegte, dass ich den Kanal abonniert und das Video gelikt hatte.

Betrüger:

„Ok“

„Ihr Screenshot ist korrekt. Um den 10 Eur Bonus zu erhalten, teilen Sie mir bitte Ihr tatsächliches Alter mit.“

Ich: *38*

(Wer mich kennt, weiß, dass ich gelogen habe. Aber einen Betrüger anzulügen ist ja nicht schlimm, oder?)

Betrüger:

OK.

Die Person, die Sie bezahlt, ist in Telegram. Sie müssen also die Telegram -Anwendung auf Ihrem Telefon haben, um ihn zu kontaktieren. Hast du Telegram?

Ich: *Nein*

Betrüger:

Gemäß den Regeln des Unternehmens müssen Sie nur ein Telekonto haben, da das Gehalt per Telegramm ausgezahlt wird. Es ist kein Betrug. Ihre Verantwortung ist es, vertrauensvoll Geld abzuheben. Es dauert nur 2 Minuten, um Ihr Geld abzuheben

An dieser Stelle wollte ich das Gespräch schon beenden. Aber der Betrüger ließ nicht mehr locker. In den nächsten Minuten hakte er noch mehrmals nach:

Betrüger:

Wenn Sie kein Telegram haben, können Sie Ihre Provision bei Ihrem Freund oder im Telegram Ihres Freundes anfordern.

Und 15 Minuten später

Betrüger:

> *WhatsApp dient nur der Rekrutierung, YouTube dient den Moderatoren. Um die wirtschaftliche Sicherheit der Teilzeitbeschäftigten zu gewährleisten, wird das Unternehmen über Telegram kommunizieren und Belohnungen verteilen.*
>
> *Sie benötigen ein Telegram-Konto, um Ihr Gehalt abzurufen.*

Ich blockierte schließlich den Kontakt.

Nicht nachmachen: So schützen Sie sich

Machen Sie es nicht wie ich und reagieren Sie erst gar nicht auf solche Anfragen. Die beste Reaktion ist es, sofort die Nachricht zu löschen und den Whatsapp-Kontakt zu blockieren.

Früher oder später wollen die Online-Betrüger nämlich persönliche Daten von Ihnen. Etwa Bankkontonummern, Anschriften, etc. Über diese Daten sind dann weitere Angriffe möglich. Sollten Sie Opfer eines solchen Betrugs geworden sein, sollten Sie unbedingt bei der Polizei eine Anzeige erstatten (das geht auch online), Hilfe bei Verbraucherzentralen suchen und natürlich Ihre Bank informieren. Für mehr Informationen dazu empfehle ich Ihnen die Lektüre dieses Artikels.

Tipp: Die o.g. Schreenshots können unter dem u.g. Link abgerufen werden.

Quelle: https://www.pcwelt.de/article/2762543/youtube-videos-liken-fur-1-000-euro-am-tag-so-lauft-der-whatsapp-betrug.html?utm_date=20250427145347&utm_campaign=Security&utm_content=slotno1-pushheadline-YouTube-Videos%20liken%20f%C3%BCr%201.000%20Euro%20am%20Tag%3F%20So%20l%C3%A4uft%20der%20WhatsApp-Betrug&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) Verbraucher fühlen sich abgezockt – Vorsicht: Service-Seiten verlangen Geld für kostenlose Leistungen

Die Ummeldung für den Rundfunkbeitrag ist ein kostenloser Service. Es gibt aber Websites, die für diese und ähnliche Leistungen Geld kassieren.

Nach seinem Umzug im Mai vergangenen Jahres will ein Marktcheck-Zuschauer seine neue Adresse beim Beitragsservice melden. Er tippt „Rundfunkbeitrag“ in die Suchmaschine ein und klickt auf den ersten Treffer: „Service-Rundfunkbeitrag.de“. Er geht davon aus, auf der Seite des Beitragsservice zu sein.

Kaum erkennbar: Seiten von Drittanbietern

Die Seite sieht für ihn seriös aus. Der Betroffene gibt seine neue Adresse ein und zahlt 29,99 € für die Ummeldung. „Das hat mich natürlich gewundert, weil ich in Erinnerung hatte, dass es eigentlich kostenlos sein müsste“, sagt er.

Er schaut sich die Seite nochmal ganz genau an. Ganz unten entdeckt er einen unauffälligen Hinweis, dass der Service in keiner Verbindung zu den öffentlich-rechtlichen Rundfunkanstalten steht. Die richtige Seite heißt „Rundfunkbeitrag.de“. Dort hätte er seine Adressdaten kostenlos ändern können.

Widerruf nicht möglich

„Nachdem ich das gemerkt hatte, dass dort eine Privatfirma dahintersteckt, habe ich gleich auf deren Seite auf den Widerrufsbutton geklickt“, so der Betroffene. Doch es heißt, das

Widerrufsrecht sei erloschen – die Dienstleistung sei mit der Weiterleitung des Auftrags an den öffentlich-rechtlichen Rundfunk bereits erfüllt.

Verzweigtes Netzwerk: Eine Firma betreibt viele Service-Seiten

Laut Impressum steckt die SSS Software Special Service GmbH mit Sitz in Horhausen im Westerwald hinter der Seite. Dieses Unternehmen betreibt noch weitere Seiten - etwa Wohngeldanträge oder Nachsendeaufträge. Dienstleistungen, die auf den Originalseiten günstiger oder sogar kostenlos wären.

Zum Zeitpunkt unserer Recherche bietet das Unternehmen zum Beispiel einen Grundbuchauszug für knapp 30 Euro – statt den behördlichen 10 Euro. Den eigentlich kostenlosen Wohngeldantrag ebenfalls für knapp 30 Euro. Der Nachsendeauftrag der Post kostet statt rund 38 Euro stolze 180 Euro, also mehr als das Vierfache.

Sind solche Service-Seiten legal?

Bei den Verbraucherzentralen sind allein über die Seite „service-rundfunkbeitrag.de“ mehr als 90.000 Beschwerden von Nutzern eingegangen. Sie fühlen sich abgezockt. Oliver Buttler von der Verbraucherzentrale Baden-Württemberg sagt dazu: „Prinzipiell ist es zulässig, dass man einen Dienstleister beauftragt für Tätigkeiten, die man eigentlich selbst machen könnte. Der Vorwurf an dieser Stelle ist aber nur, dass suggeriert wird, man wäre der Originalanbieter und die Kosten werden hier im Kleingedruckten versteckt“.

Auch, dass Betroffene ihr Widerrufsrecht zum Teil nicht ausüben können, sieht der Verbraucherrechtsexperte Oliver Buttler kritisch: „Wir haben hier eine gesetzliche Grundlage, die besagt, dass man bei Vertragsabschlüssen im Fernabsatzgeschäft, also im Internet, jederzeit ein Widerrufsrecht ausüben kann. Voraussetzung ist allerdings, dass diese Dienstleistung dann noch nicht abgeschlossen ist“. Der Kritikpunkt an diesen Dienstleistungen sei, dass für den Verbraucher nicht nachvollziehbar sei, was mit den eigenen Daten passiere.

Fragen an das abgemahnte Service-Netzwerk

Ende vergangenen Jahres hat der Bundesverband der Verbraucherzentrale die SSS Software Special Service GmbH abgemahnt. Daraufhin hat das Unternehmen angekündigt, Widerrufe der bisherigen Kunden in vielen Fällen zu akzeptieren. Zwar haben einige Betroffene ihr Geld zurückbekommen, andere aber nicht.

Die SWR Marktcheck-Redaktion bittet die SSS-Software Special Service GmbH um ein Gespräch, denn die Redaktion will wissen, was von der Ankündigung zu halten ist. Die Anfrage bleibt jedoch für mehrere Wochen unbeantwortet. Daraufhin probiert die Redaktion es mehrfach erfolglos per Telefon.

Wochen später meldet sich das Unternehmen doch noch und bittet um die schriftliche Zusendung der Fragen. Eine Antwort auf diese Fragen erhält die Redaktion bis Redaktionsschluss nicht.

Service-Seiten mit Sitz in Dubai

Mittlerweile hat die Seite eine neue Adresse. Sie sieht fast genauso aus, nur steht jetzt im Impressum ein neuer Name und eine Anschrift in Dubai. Die SWR Marktcheck-Redaktion bittet einen Kollegen vor Ort dorthin zu fahren: eine große Freihandelszone am Rande von Dubai. Mehr als 20.000 Unternehmen sind hier offiziell registriert. In zahlreichen Gebäuden entdeckt der Marktcheck-Kollege sogenannte Co-Working Spaces. Die kann man für unter 8.000 Euro im Jahr mieten und die Freihandelszone dann rechtmäßig im Impressum verwenden.

In welchem der zahlreichen Bürogebäude das Unternehmen sitzen soll, kann der Reporter nicht herausfinden. Doch auch „Digitaler Post Service“ ist nun beim Wirtschaftsministerium Dubai registriert - in der Freihandelszone.

Wie hängen die Service-Unternehmen zusammen?

In Deutschland wird im Westerwald weiter recherchiert: Unter der Adresse, die zuvor im Impressum stand. Denn auf unsere Frage, wie die Unternehmen zusammenhängen, hat die Marktcheck-Redaktion keine Antwort erhalten.

An der angegebenen Adresse befindet sich ein Wohnhaus. Doch die Frau, die dort die Tür öffnet, gibt an den Geschäftsführer nicht zu kennen und hat angeblich auch noch nie von ihm gehört.

Mehrere Anwohner erzählen der Reporterin vor Ort, dass der im Impressum genannte Geschäftsführer mit seiner Partnerin in dem Haus leben würde. Doch offen vor der Kamera will das niemand äußern. Immer wieder würden Leute nach ihm fragen, weil sie ihr Geld zurückwollen.

Sammelklage der Verbraucherzentrale

Inzwischen hat der Verbraucherzentrale Bundesverband eine Sammelklage gegen die SSS-Software Special Service GmbH eingereicht. Betroffene können sich mit einem Formular in wenigen Minuten dieser Klage anschließen.

Tipp: Der Fernsehbeitrag kann unter dem u.g. Link abgerufen werden.

Quelle: https://www.swr.de/verbraucher/ard-marktcheck/vorsicht-abzocke-service-seiten-verlangen-geld-fuer-kostenlose-leistungen-100.html

7) Millionen Telekom-Kunden sollten „Rechnung“ bloß nicht bezahlen

Cyberkriminelle verschicken aktuell gefälschte Telekom-Rechnungen.
Die Verbraucherzentrale verrät, wie sich betroffene Kunden schützen können.

Telekom-Kunden aufgepasst: Aktuell versuchen Betrüger mit gefälschten Rechnungen sensible Daten zu ergaunern. Vor kurzem wurden bereits AOK-Kunden vor Phishing-Mails mit angeblichen Rückerstattungen gewarnt. Bei der aktuellen Masche setzen die Betrüger ahnungslose Kunden unter Zahlungsdruck.

Millionen Telekom-Kunden sollten „Rechnung“ bloß nicht bezahlen

Die Verbraucherzentrale warnt in ihrem aktuellen Phishing-Radar vor der Betrugsmasche. Kriminelle verschicken seit dem 15. April E-Mails mit gefälschten Festnetz-Rechnungen im Namen der Telekom. Die angebliche Rechnung beläuft sich auf 168,73 Euro und enthält eine zufällig generierte zehnstellige Buchungskontonummer.

Die betrügerische E-Mail beginnt mit der unpersönlichen Anrede „Guten Tag“ und informiert den Empfänger über eine angebliche Festnetz-Rechnung. Besonders auffällig gestaltet sich ein blaues Feld in der Mitte der Nachricht: Es hebt den Betrag von 168,73 Euro für April 2025 hervor und enthält einen Button mit der fehlerhaften Aufschrift „RechnungOnline ansehen“.

Im unteren Teil der Nachricht kündigen die Betrüger die Abbuchung des Betrags zum 15. April 2025 an. Sie verweisen zudem auf ein angebliches Rechnungsarchiv im Kundencenter, um ihrer Fälschung einen legitimen Anstrich zu verleihen.

Warnung vor gefälschter Telekom-Rechnung: Diese Anzeichen entlarven den Betrug

Die Verbraucherzentrale identifiziert mehrere verräterische Merkmale, die auf einen Phishing-Versuch hindeuten:

- Die unpersönliche Anrede „Guten Tag“ statt einer individualisierten Kundenansprache
- Eine grammatikalisch fehlerhafte Satzstruktur zu Beginn der Nachricht
- Die verdächtige Formulierung „RechnungOnline ansehen“ ohne Leerzeichen
- Eine fehlende öffnende Klammer im Betreff der E-Mail
- Die Absenderadresse stammt nicht von offiziellen Telekom-Servern

Warnung vor Phishing-Mails und Online-Betrug: Empfänger können sich schützen

Zum Umgang mit Phishing-Versuchen gibt es klare Empfehlungen von der Verbraucherzentrale:

- Phishing-Mails unbeantwortet in den Spam-Ordner verschieben
- Niemals auf Links in verdächtigen E-Mails klicken
- Bei Unsicherheit die offizielle Website oder App der Telekom nutzen
- Dort nach tatsächlichen Rechnungen oder Mitteilungen suchen
- Im Zweifelsfall den offiziellen Kundenservice der Telekom kontaktieren

Wer unsicher ist, ob eine Rechnung echt oder gefälscht ist, sollte sich direkt bei der Telekom informieren. Echte Rechnungen finden Kunden immer in ihrem persönlichen Kundenkonto auf der offiziellen Webseite oder in der Telekom-App.

Quelle: https://www.ruhr24.de/service/telekom-warnung-rechnung-finanzen-kunden-verbraucherzentrale-nicht-bezahlen-betrug-phishing-mail-93690200.html

8) Reisen nach Großbritannien – Polizei warnt Flugreisende vor neuer Betrugsmasche

Wer ins Vereinigte Königreich reist, braucht seit April eine elektronische Reisegenehmigung. Ein Verfahren, das sich Betrüger zunutze machen.

Flugreisende aufgepasst: Die Polizei warnt in Hessen vor einer neuen Betrugsmasche im Zusammenhang mit der sogenannten "Electronic Travel Authorisation" (ETA). Die elektronische Reisegenehmigung muss seit Anfang April vor Reisen nach Großbritannien online beantragt werden.

Dieses Verfahren nutzen offenbar Betrüger aus, um Touristen das Geld aus der Tasche zu ziehen oder sensible und persönliche Daten abzugreifen. Eine Erfahrung, die laut dem Polizeipräsidium Mittelhessen zuletzt auch eine Frau aus dem Landkreis Gießen machen musste.

Frau aus Gießen fiel auf Betrugsmasche herein

Die 42-Jährige hatte demnach auf einer "täuschend echt" gestalteten Website ihre Einreisegenehmigung beantragt. Für dieses bezahlte sie 99 US-Dollar mit ihrer Kreditkarte und lud zudem ein Foto von sich sowie eine Kopie ihres Reisepasses hoch. Daraufhin erhielt sie tags darauf ihr Visum.

Weil ihr dieses allerdings auffällig erschienen sei, rief die Frau noch einmal die Website auf. Als ihr Virusprogramm anzeigte, dass es sich um eine sogenannte Phishingseite handelt, ließ sie ihre Kreditkarte umgehend sperren und erstattete Anzeige.

Stündliche Verbindungen von Frankfurt nach London

Die Polizei mahnt im Zusammenhang mit der Beantragung der ETA zur Vorsicht. Reisende sollten nur die offiziellen Wege nutzen, die auf der Website des britischen Ministeriums beschrieben sind und keine Zahlungen an Dritte zu leisten. Der ETA-Antrag kostet 16 britische Pfund (knapp 20 Euro).

Allein vom Flughafen in Frankfurt am Main gehen pro Tag etliche Flüge nach Großbritannien. Nach London etwa gibt es zeitweise stündliche Verbindungen, auch in Richtung Manchester und Glasgow heben täglich Flieger ab.

Quelle: https://frankfurt.t-online.de/region/frankfurt-am-main/id_100685036/hessen-polizei-warnt-vor-neuer-betrugsmasche-bei-reisen-nach-england.html

9) Digitale Bedrohung – Betrug im Internet: Microsoft warnt vor neuen Tricks

Internetbetrug wird immer raffinierter. Microsoft erklärt, wie Verbraucher sich schützen können – und warnt vor neuen Maschen, die besonders Deutschland betreffen.

Microsoft hat vor einer besorgniserregenden Entwicklung im Internet gewarnt: Betrüger nutzen zunehmend Künstliche Intelligenz, um ihre Betrugsmaschen überzeugender zu gestalten. Wie aus dem aktuellen "Cyber Signals"-Bericht hervorgeht, verhinderte der Konzern zwischen April 2024 und April 2025 Betrugsversuche im Wert von vier Milliarden US-Dollar. Erschreckend dabei ist, dass die neuen Betrugsmaschen oft kaum von seriösen Angeboten zu unterscheiden sind.

Die Zeiten, in der gefälschte Online-Shops auf den ersten Blick an schlechter Aufmachung und Rechtschreibfehlern zu erkennen waren, sind vorbei. Dank Künstlicher Intelligenz können Betrüger inzwischen binnen Minuten täuschend echte Websites erstellen, die von legitimen Online-Shops kaum zu unterscheiden sind. Früher brauchten sie dafür Tage oder sogar Wochen.

"Die heutigen Betrugsseiten sehen professionell aus, haben überzeugende Produktbeschreibungen und glaubwürdige Kundenbewertungen – all das wird mithilfe von KI erstellt", warnt Microsoft. Selbst die Kundendienst-Chatbots auf diesen Websites werden durch Künstliche Intelligenz gesteuert und können auf Nachfragen und Beschwerden reagieren. Dadurch wirke alles täuschend echt.

Deutschland im Visier der Betrüger

Laut dem Microsoft-Bericht konzentrieren sich die Betrüger besonders auf große Online-Märkte. Deutschland wird ausdrücklich als Zielregion genannt, da es einer der größten E-Commerce-Märkte in der Europäischen Union ist. Die Betrüger gehen nach dem Prinzip vor: "Je größer der digitale Marktplatz in einer Region, desto größer die mögliche Beute."

Die Verbreitung der betrügerischen Angebote erfolgt vor allem über Anzeigen in sozialen Medien. Die Betrüger setzen KI ein, um ihre Anzeigen zu optimieren und möglichst viele Menschen anzulocken. Was früher ein handwerklich aufwendiger Prozess war, geht heute automatisiert.

Auch Arbeitssuchende sind betroffen

Darüber hinaus zeigt der Microsoft-Bericht, dass auch Arbeitssuchende zunehmend im Visier von Betrügern stehen. Die Kriminellen erstellen gefälschte Firmenprofile und Stellenanzeigen, die kaum von echten zu unterscheiden sind.

"Bei Jobbetrügereien werden nicht nur falsche Stellen angeboten, sondern die Betrüger führen sogar KI-gestützte Vorstellungsgespräche durch", erklärt Microsoft. Dabei werden Bewerber oft nach persönlichen Informationen wie Lebenslauf oder sogar Bankverbindungen gefragt – angeblich zur Überprüfung der Bewerberinformationen.

Ein besonderes Warnsignal sind unaufgeforderte SMS und E-Mails mit Stellenangeboten, die hohe Bezahlung für minimale Qualifikationen versprechen. "Wenn ein Jobangebot zu gut klingt, um wahr zu sein, ist es das wahrscheinlich auch", warnt Microsoft.

Der gefälschte Computer-Support

Bei einer weiteren Masche, die durch KI noch gefährlicher wird, geben sich Betrüger als Microsoft-Mitarbeiter oder IT-Experten aus und behaupten, auf dem Computer des Opfers Probleme entdeckt zu haben. Dem "Cyber Signals"-Bericht zufolge missbraucht zum Beispiel die Cyberkriminellen-Gruppe Storm-1811 verstärkt den Microsoft-Dienst "Quick Assist", um sich als IT-Support auszugeben.

Über Telefonate überzeugen sie ihre Opfer, ihnen Zugriff auf den Computer zu gewähren. Sobald die Betrüger Zugang haben, können sie auf alle gespeicherten Informationen zugreifen oder Schadsoftware installieren, die ihnen auch später noch Zugriff ermöglicht.

Wie Microsoft gegen die Betrüger vorgeht

Um seine Nutzer zu schützen, hat Microsoft zahlreiche Sicherheitsmaßnahmen eingeführt. Der Edge-Browser erkennt nun verdächtige Webseiten und warnt vor Tippfehlern in der Webadresse, die zu betrügerischen Seiten führen könnten. Außerdem werden betrügerische Pop-up-Fenster blockiert, die angebliche Computerprobleme melden und eine Telefonnummer für "Hilfe" anzeigen.

Außerdem blockiert Microsoft nach eigenen Angaben täglich bereits über 4.400 verdächtige Verbindungsversuche über den Quick-Assist-Dienst. Das Unternehmen hat das Programm zudem mit Warnhinweisen ausgestattet, die Nutzer vor möglichen Betrugsversuchen warnen, bevor sie jemandem Zugriff auf ihren Computer gewähren.

So können Sie sich schützen

Microsoft gibt Verbrauchern konkrete Tipps zum Schutz vor KI-gestütztem Betrug:

1. Lassen Sie sich nicht unter Druck setzen: Betrüger erzeugen absichtlich Zeitdruck mit "zeitlich begrenzten" Angeboten und ablaufenden Countdowns. Nehmen Sie sich immer Zeit für eine Überprüfung.
2. Nutzen Sie sichere Zahlungsmethoden: Vermeiden Sie direkte Banküberweisungen oder Zahlungen mit Kryptowährungen. Diese bieten keinen oder nur sehr geringen Schutz bei Betrug. Bevorzugen Sie PayPal, Kreditkarten oder Käuferschutz-Optionen.
3. Überprüfen Sie bei Stellenangeboten den Arbeitgeber: Schauen Sie auf LinkedIn, Glassdoor und der offiziellen Firmenwebsite nach, ob das Unternehmen wirklich existiert und die Stelle tatsächlich ausgeschrieben ist.
4. Wenn für eine Stelle vorab Zahlungen für Schulungsmaterialien, Zertifizierungen oder Hintergrundchecks verlangt werden, ist das ein deutliches Warnsignal. Auch unrealistisch hohe Gehälter für wenig qualifizierte Tätigkeiten sollten misstrauisch machen.
5. Seien Sie misstrauisch bei unaufgeforderten Anrufen: Microsoft und andere Tech-Unternehmen rufen nicht unaufgefordert an, um technische Probleme zu beheben. Wenn Sie einen solchen Anruf erhalten, legen Sie auf.
6. Geben Sie niemals Fernzugriff: Gewähren Sie niemandem Fernzugriff auf Ihren Computer, es sei denn, Sie haben den Support selbst kontaktiert und sind sich der

Echtheit absolut sicher.

Microsoft arbeitet nach eigenen Angaben mit Strafverfolgungsbehörden weltweit zusammen, um gegen Betrug vorzugehen. Wenn Sie Opfer eines Betrugs geworden sind oder verdächtige Aktivitäten bemerken, bei denen sich jemand als Microsoft-Mitarbeiter ausgibt, können Sie sich direkt unter www.microsoft.com/reportascam melden.

Quelle: https://www.t-online.de/digital/aktuelles/id_100681704/ki-betrug-microsoft-warnt-vor-neuen-maschen-in-deutschland.html

10) Betrüger setzen auf Drohung – Phishing-Attacke auf Kunden der Deutschen Bank

Eine gefälschte E-Mail fordert Kunden der Deutschen Bank zu einer Verifizierung auf. Die Verbraucherzentrale warnt.

Betrüger versuchen aktuell erneut, Kunden der Deutschen Bank mit einer täuschend echten E-Mail in die Falle zu locken. Unter der Betreffzeile "Telefonnummern-Verifizierung erforderlich" fordern sie dazu auf, die eigene Telefonnummer "so schnell wie möglich" zu bestätigen. Wer der Aufforderung nicht folgt, müsse mit einer vorübergehenden Kontosperrung rechnen – so zumindest die Drohung in der Nachricht. Ziel der Kriminellen ist es, an sensible Kundendaten zu gelangen, warnt die Verbraucherzentrale.

Die E-Mail wirkt auf den ersten Blick offiziell, weist jedoch deutliche Warnzeichen für einen Phishing-Versuch auf. Dazu zählen eine unpersönliche Anrede, ein unseriöser Absender und ein eingebetteter Button, über den die vermeintliche Verifizierung vorgenommen werden soll. Aber gerade die Kombination aus Zeitdruck und der drohenden Kontosperrung könnte potenzielle Opfer zu unüberlegtem Handeln verleiten.

Telefonnummern-Verifizierung erforderlich

Sehr geehrter Kunde,

Wir haben festgestellt, dass Ihre Telefonnummer noch nicht verifiziert wurde.
Um Ihr Konto aktiv zu halten, bitten wir Sie,
Ihre Telefonnummer so schnell wie möglich zu bestätigen.

Telefonnummer verifizieren

Wenn Ihre Telefonnummer nicht bis zum 21/04/2025 verifiziert wird,
kann Ihr Konto vorübergehend gesperrt werden.

Mit freundlichen Grüßen,
Deutsche Bank

So sieht die betrügerische E-Mail aus. (Quelle: Verbraucherzentrale/Phishing-Radar)

Die Deutsche Bank warnt eindringlich vor solchen E-Mails und empfiehlt, verdächtige Nachrichten konsequent zu ignorieren. Wer Zweifel hat, ob es sich um eine echte Mitteilung handelt, sollte sich direkt über die offiziellen Kanäle der Bank informieren und keinesfalls auf Links in der Nachricht klicken.

So schützen Sie sich vor Phishing-Angriffen

- Öffnen Sie keine Anhänge und klicken Sie niemals auf Links in verdächtigen E-Mails.
- Geben Sie keine Login-Daten oder persönlichen Informationen preis.
- Lassen Sie sich nicht unter Druck setzen – Eile ist ein typisches Druckmittel von Betrügern.
- Achten Sie auf Warnsignale wie: fehlende persönliche Anrede, Rechtschreibfehler oder schlechten Stil, dringliche Fristen und Drohungen.

Die Deutsche Bank rät: Im Zweifel lieber einmal zu viel bei der Bank nachfragen, als auf die Tricks der Täter hereinzufallen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100676806/deutsche-bank-verbraucherzentrale-warnt-kunden-vor-phishing-angriff.html

11) Nummer 017658612759: Anruf von Anwaltskanzlei?

Unter der Handynummer 017658612759 meldet sich eine Rechtsanwaltskanzlei bei euch und will mit euch Vertragsdaten besprechen. Allerdings solltet ihr große Zweifel an der Geschichte haben und das fängt bereits bei der Telefonnummer an. Was steckt dahinter?

Man kann die Nummer 017658612759 zurückrufen, aber dann wird die Verbindung sofort unterbrochen. Eine Beschwerde bei der Bundesnetzagentur ist in so einem Fall aber sinnlos, weil die Nummer sowieso eine Fälschung ist: Im Hintergrund der Gespräche sind nämlich Callcenter-Geräusche zu hören. Die Fake-Nummer wird also durch Call-ID-Spoofing erzeugt. Dadurch versteckt ein Telefoncomputer seine richtige Nummer, die sich oftmals in solchen Fällen sogar im Ausland befindet. Darauf deuten auch die Sprachkenntnisse der Anruferinnen hin.

Um was geht es bei den Anrufen der Nummer 017658612759?

- Gebrochen Deutsch sprechende Callcenter-Mitarbeiterinnen geben sich als Angestellte einer Anwaltskanzlei aus.
- Sie sprechen euch mit eurem Namen an und behaupten, dass eure Daten für ein Gewinnspiel- oder Lotto-Abo eingetragen wurden, das sich nach einer kostenlosen Periode in einen kostenpflichtigen Vertrag umgewandelt hat.
- Vermutlich, so legen sie euch nahe, habt ihr vergessen zu kündigen. Um nun nicht ein Jahr lang monatlich hohe Kosten zahlen zu müssen, bieten sie euch als Alternative ein selbst kündigendes Kurz-Abo an. Ihr sollt ein Vierteljahr monatlich um die 69 Euro zahlen, um aus dem Jahresvertrag herauszukommen.
- Ziel des Anrufes ist, an eure IBAN zu kommen. Dazu versuchen sie es auch mit Druck, indem sie zum Beispiel behaupten, dass ihr andernfalls nicht aus dem Jahres-Abo kommt und fast 900 Euro Gebühren anfallen.
- Wenn ihr auf das „Angebot“ nicht einsteigen wollt, ihnen widersprecht oder schriftliche Beweise fordert, werden die Anruferinnen schnell unfreundlich bis beleidigend und behaupten, sie würden nun einfach die Abo-Gebühren einziehen lassen. Dann legen sie auf.

Diese Kriminellen haben zwar eure Daten gekauft, aber die Kontoverbindung fehlt ihnen offensichtlich. Außerdem können sie keinen schriftlichen Vertragsabschluss nachweisen. Ihr habt also trotz aller Drohungen nichts zu befürchten.

So wird diese Nummer blockiert

- Anrufe dieser Nummer auf dem Handy lassen sich einfach sperren. Sobald sie einmal in der Anrufliste auftauchen, könnt ihr sie bei Android und iPhone in wenigen Schritten blockieren und melden.
- Für solche Betrugsanrufe findet ihr im „Telefoniecenter“ der Telekom eine schwarze Liste, mit der ihr Telefonnummern im Festnetz abweisen könnt.
- Auch in Telefon-Routern ist so eine Funktion integriert. Ihr könnt Spam-Nummern in der Fritzbox blockieren, indem ihr sie dort in den Einstellungen auf die Sperrliste setzt.

Quelle: https://www.giga.de/tech/nummer-017658612759-anruf-von-anwaltskanzlei--01JQV4E158JW4XKV4KX0713WH2?utm_source=flipboard&utm_content=Gigade/magazine/Smarthome

12) Aufpassen: Diese gefälschten Captcha-Anfragen installieren Malware auf Ihrem PC

Falsche Captcha-Tests werden immer häufiger von Hackern genutzt, um Nutzerdaten zu stehlen und Malware zu verbreiten. So können Sie sich davor schützen.

Jeder kennt die klassischen Captcha-Tests auf Webseiten. Klicken Sie hier, um zu bestätigen, dass Sie kein Roboter sind. Wählen Sie alle Ampeln aus, alle Autos, alle Zebrastreifen und so weiter. Meistens sind diese Tests nur lästig, doch teilweise können sich dahinter auch Angriffsversuche von Hackern verbergen.

Davor warnen Sicherheitsexperten zumindest immer häufiger. Das Bundesamt Sicherheit in der Informationstechnik (kurz BSI) hatte bereits Anfang März vor gefährlichen Captcha-Anfragen gewarnt. Seit Neuestem gibt es auch Meldungen über eine Malware namens “Qakbot”, die eine noch gefährliche Variante des Captcha-Betrugs verwendet.

Wie funktioniert der Captcha-Betrug?

Hackangriffe mit Captchas sind deshalb so gefährlich, weil man sie als Nutzer aus reiner Gewohnheit erst einmal anklickt, wenn sie auf einer Webseite auftauchen. Von dieser intuitiven Reaktion machen Hacker jetzt auch Gebrauch und verwenden Pop-up-Meldungen, die einem echten Captcha-Test zum Verwechseln ähnlich sehen.

Nutzer werden auch hier aufgefordert, einen Kasten anzuklicken, um den Test zu lösen. Der Klick sorgt aber dafür, dass sie auf andere Seiten weitergeleitet werden. Weitere Handlungen sorgen dafür, dass gefährliche Protokolle in der Zwischenablage gespeichert werden. Das autorisiert die Angreifer dazu, Schadcode auszuführen.

In manchen Fällen fordern die Captchas sogar dazu auf, bestimmte Tastenkombinationen zu drücken, die direkt Windows Powershell aufrufen oder bestimmte Kommandos auf dem Gerät ausführen. Spätestens hier sollte aber jedem Nutzer auffallen, dass es sich nicht um eine normale Captcha-Anfrage handeln kann.

Angriff bleibt oft unbemerkt

Damit das Opfer den Angriff gar nicht bemerkt, wird jeder weitere Klick durch zusätzliche “Verifikationsanfragen” getarnt. Im schlimmsten Fall endet das mit der Ausführung eines Malware-Skripts, das den ganzen PC übernehmen kann.

Die Sicherheitsexperten von Dark Atlas bezeichnen den Angriff als “Clickfix Captcha” und warnen ausdrücklich davor. Captcha-Angriffe sollen eine höhere Erfolgsrate als andere Betrugsversuche aufweisen, da sie sich psychologischer Tricks bedienen. Der einzige Schutz davor ist es, aufmerksam zu bleiben, besonders wenn Sie unbekannte Webseiten besuchen. Und natürlich ein zuverlässiger Virenschutz, der im Ernstfall eingreifen kann.

Dass Captcha dazu genutzt werden, um Nutzerdaten abzugreifen, ist aber tatsächlich nichts Neues. Sogar offizielle Captcha-Anfragen, die von Unternehmen wie Google konzipiert werden, sammeln Informationen über Nutzer, ohne dass es ihnen direkt bewusst ist. Mehr dazu lesen Sie in unserer Meldung Captcha-Falle: Kein Schutz vor Bots, sondern versteckte Spyware.

Quelle: https://www.pcwelt.de/article/2655395?utm_source=flipboard&utm_content=topic/de-computer

13) Neue Betrüger-App nimmt heimlich Ihren Bildschirm auf: Darauf müssen Sie achten

Android-Nutzer aufgepasst: Der gefährliche Banking-Trojaner Vultur tarnt sich derzeit als legitime McAfee-Sicherheits-App und bedroht die Sicherheit Ihrer persönlichen Daten.

Die Sicherheitsforscher von Fox-it.com haben herausgefunden, dass diese Schadsoftware aktuell über gefälschte SMS-Nachrichten verbreitet wird, die vorgeben, unautorisierte Transaktionen zu melden.

Opfer werden dabei aufgefordert, eine Telefonnummer anzurufen, woraufhin sie von Betrügern dazu verleitet werden, eine vermeintliche McAfee-App herunterzuladen. Diese App enthält jedoch den Vultur-Trojaner, der es Angreifern ermöglicht, Bildschirminhalte aufzuzeichnen, Tastatureingaben zu protokollieren und sensible Informationen wie Passwörter und Bankdaten zu stehlen.

So schützen Sie sich:

- Installieren Sie Apps ausschließlich aus offiziellen Quellen: Laden Sie Anwendungen nur aus dem Google Play Store oder anderen vertrauenswürdigen App-Stores herunter.
- Seien Sie vorsichtig bei unerwarteten Nachrichten: Ignorieren Sie SMS oder E-Mails, die Sie auffordern, unbekannte Apps zu installieren oder verdächtige Links zu öffnen.
- Überprüfen Sie App-Berechtigungen: Achten Sie darauf, welche Zugriffsrechte eine App anfordert, und seien Sie skeptisch, wenn diese übermäßig erscheinen.
- Nutzen Sie eine zuverlässige Sicherheitslösung: Ein aktuelles Antivirenprogramm kann helfen, bekannte Bedrohungen zu erkennen und zu blockieren.

Sollten Sie bereits eine verdächtige App installiert haben, entfernen Sie diese umgehend und führen Sie einen vollständigen Scan Ihres Geräts durch. Im Zweifelsfall setzen Sie Ihr Smartphone auf die Werkseinstellungen zurück, um mögliche Schadsoftware vollständig zu entfernen.

Tipp: Virenscanner für Android: Testsieger gratis und werbefrei

Quelle: https://www.chip.de/news/Neue-Betrueger-App-nimmt-heimlich-Ihren-Bildschirm-auf-Darauf-muessen-Sie-achten_185906704.html?utm_source=flipboard&utm_content=topic%2Fde-digital

14) Unbekannter Anruf: Diese Telefonnummern sollten Sie momentan besser ignorieren

Anrufe von unbekannten Nummern entpuppen sich oft als Spam oder Werbung. Wir zeigen Ihnen, wie Sie in Sekundenschnelle erkennen, ob der Anruf vertrauenswürdig ist oder nicht.

Das Smartphone klingelt, eine unbekannte Nummer ruft an und der Mitarbeiter am Telefon will Sie überzeugen, in Aktien zu investieren oder Ihren Handyvertrag zu wechseln. In manchen Fällen wird auch gleich aufgelegt, sobald Sie den Anruf entgegennehmen.

Meist handelt es sich um unerwünschte Spamanrufe, bei denen Betrüger oder unseriöse Unternehmen Ihre Daten abgreifen wollen oder Sie bei einem Rückruf in eine Kostenfalle locken.

Viele neuere Handys erkennen Spamanrufe inzwischen automatisch und zeigen auf dem Display eine Warnung mit "potenzieller Spam" an. Werbeanrufe ohne explizite Erlaubnis sind in Deutschland rechtlich nicht erlaubt, weshalb die Betrüger häufig Ihre Nummern wechseln. Somit klappt es nicht immer, dass das Smartphone dubiose Anrufer erfasst.

Mit einem cleveren Tool finden Sie dennoch schnell heraus, ob die Nummer, die Sie anruft, echt ist.

Spam-Anrufe checken: Mit diesen Tools geht's

Sind Sie sich unsicher, ob eine Nummer aus einem Callcenter stammt, können Sie kostenfreie Webseiten nutzen. Zum Beispiel:

- Cleverdialer.de
- Tellows.de

Dort können Sie einfach die Daten eingeben und überprüfen, ob jemand anderes bereits angerufen wurde. Neben der Rufnummer können Sie zusätzlich auch die Art des Anrufes (Werbung, Umfrage, Gewinnspiel, etc.) einsehen und abwägen, ob sich ein Rückruf lohnt.

Top Telefonnummern der letzten 7 Tage

Meist anrufende Rufnummern	
Platz	Telefonnummer
1	015219466469
2	01637782275
3	03050931590
4	0031613839719
5	015226937332
6	015170294736
7	0031613515450
8	0031649035316
9	015258299923
10	015783748738

Meist bewertete Rufnummern	
Platz	Telefonnummer
1	0031613515450
2	0031649035316
3	015219466469
4	040655801110
5	040228994527
6	0031613839719
7	040228993182
8	004367762016936
9	040228992652
10	015170294736

Hier finden Sie die aktuellen Spamnummern der letzten 7 Tage. Bild: Cleverdialer.de

Laut Datenbank von tellows.de wird unter anderem vor folgenden Nummern und ihren Betrugsmaschen gewarnt:

- **03080098648**
  Anrufername: Apotherkerbund
  Betrugsmasche: Vermeintliche Umfrage zur Gesundheit mit angeblichem kostenlosen Zeitungsabos als Aufwandsentschädigung.
- **+16465535819**
  Anrufername: Immobilien Anruf New York
  Betrugsmasche: Call-Center, das mit veralteten Immobilien-Scout-Anzeigen Wohnungen vermarktet.
- **022166951483**
  Anrufername: EWE Energiezentrale
  Betrugsmasche: Vermeintlicher Energieanbieter aus Köln, der versucht, unseriöse Stromtarife zu verkaufen.
- **01637875622**
  Anrufername: Gewinnspiel
  Betrugsmasche: Die Anruferinnen und Anrufer täuschen ein Gewinnspiel-Abo vor, das sofort bezahlt werden muss oder sonst für 12 weitere Monate kostenpflichtig verlängert wird.
- **069222224635**
  Anrufername: Energieportal
  Betrugsmasche: Angebliches Energieunternehmen, das mit Kaltakquise versucht, alternative Energiequellen zu bewerben.
- **017688854744**
  Anrufername: O2
  Betrugsmasche: Datenbetrug und Ja-Masche, bei der nach gesprochenem "Ja" Scheinverträge geschlossen werden. Die Betrüger geben sich als Mitarbeitende von O2 aus und fragen Sie zu Ihren Daten.
- **053120970053**
  Anrufername: Strafverfolgungsbehörde
  Betrugsmasche: Betroffene werden mit einer Computeransage getäuscht, die vorgibt von Europol (Europäisches Polizeiamt) zu sein. Die gleiche Nummer wird mitunter für andere Betrugsversuche, z. B. angeblichen Finanz- und Krypto-Beratungen verwendet.

Einige Userinnen und User geben an, von den Spam-Anrufern unter Druck gesetzt worden zu sein. Sollten Sie einen dubiosen Anruf erhalten und ebenfalls dazu gedrängt werden, einen Vertrag abzuschließen, können Sie auf Höflichkeiten verzichten. **Legen Sie einfach auf und blockieren die Nummer**. Um andere Menschen vor der Abzocke zu warnen, melden Sie die Daten bestenfalls noch bei Cleverdialer oder tellows.

Unser Rat: Werden Sie von einer unbekannten Rufnummer angerufen, gehen Sie am besten erst gar nicht dran. Seriöse Unternehmen hinterlassen meist eine Nachricht auf Ihrer Mailbox oder die Rufnummer lässt sich via Googlesuche leicht einem Unternehmen zuordnen.

Wie Sie Ihr Handy zusätzlich gegen unerwünschte Anrufe schützen können, lesen Sie in diesem Beitrag.

Tipp: Datenbank von Cleverdialer

Quelle: https://www.chip.de/news/Unbekannter-Anruf-Diese-Telefonnummern-sollten-Sie-momentan-besser-ignorieren_184116106.html

15) Verbraucherschützer warnen – Betrüger locken Menschen mit Diabetes in gefährliche Falle

Die Verbraucherzentrale NRW warnt vor einer Betrugsmasche: Diabetes-Patienten werden Nahrungsergänzungsmittel angeboten – mit gefährlichen Versprechungen.

Immer mehr Menschen mit Diabetes erhalten derzeit Anrufe oder stoßen online auf Angebote für vermeintlich wirksame Nahrungsergänzungsmittel, die als Ersatz für das Medikament Metformin angepriesen werden. Die Verbraucherzentrale NRW warnt: Diese betrügerische Verkaufsmasche kann schwerwiegende gesundheitliche Folgen haben.

Betrug mit Nahrungsergänzungsmitteln

Dubiose Anbieter behaupten demnach, ihr Nahrungsergänzungsmittel könne Insulinresistenz bekämpfen und den Blutzuckerspiegel innerhalb von zwei bis drei Wochen normalisieren. In Werbeanrufen werden Betroffene mit der Frage "Sie haben doch Diabetes?" konfrontiert und dann zum Kauf gedrängt. In manchen Fällen wird ein Abonnement abgeschlossen, ohne dass die Betroffenen es merken. "Wir raten dringend davon ab, auf solche Angebote einzugehen", sagt Angela Clausen, Expertin für Nahrungsergänzungsmittel bei der Verbraucherzentrale NRW laut Pressemitteilung. Besonders kritisch sei, dass den Betroffenen geraten werde, ihre verordneten Medikamente abzusetzen. "Das kann zu erheblichen gesundheitlichen Risiken führen", so Clausen weiter.

Wichtig

Nahrungsergänzungsmittel sind kein Ersatz für verschriebene Medikamente. Diabetes ist eine ernste Erkrankung und sollte stets ärztlich begleitet und behandelt werden.

Kurzfristige Besserung täuscht – langfristige Gefahr

Einige Betroffene berichten, dass sie sich nach dem Absetzen ihrer Diabetesmedikamente kurzfristig besser gefühlt hätten. Die Expertin erklärt, dass dies daran liegen könnte, dass unangenehme Nebenwirkungen von Metformin, wie Übelkeit oder Durchfall, ausbleiben. Doch das ist trügerisch: Langfristig steigt der Blutzuckerspiegel wieder stark an, das Risiko für Folgeerkrankungen wie Herz-Kreislauf-Probleme oder Demenz erhöht sich.Wer Nahrungsergänzungsmittel in Betracht zieht, sollte sich an die Dosierung auf der Packung halten und vorher mit seinem Arzt sprechen. "Nahrungsergänzungsmittel können in bestimmten Fällen sinnvoll sein, etwa bei einem nachgewiesenen Vitamin-B12- oder Vitamin-D-Mangel. Doch die Entscheidung darüber sollte immer medizinisch begleitet sein", betont Clausen.

Verträge können rückgängig gemacht werden

Viele Betroffene schließen unbewusst teure Abonnements für die Nahrungsergänzungsmittel ab. Doch hier gibt es eine gute Nachricht: Wer telefonisch oder online bestellt hat, kann den Vertrag innerhalb von 14 Tagen widerrufen. Fehlt eine ordnungsgemäße Belehrung zum Widerrufsrecht, verlängert sich die Frist sogar um ein Jahr. Wichtig: Das Produkt sollte nicht geöffnet werden, da sonst das Widerrufsrecht erlöschen kann.

Betroffene, die keine Kontaktdaten des Anbieters haben, können sich an die Verbraucherzentrale NRW wenden. Falls die Ware per Nachnahme geliefert wurde, empfiehlt es sich, die Annahme zu verweigern. Zudem sollte jegliche unaufgeforderte Telefonwerbung gemeldet werden, denn diese ist in Deutschland ohne vorherige Zustimmung illegal.

Quelle: https://www.t-online.de/gesundheit/aktuelles/id_100639734/diabetes-neue-betrugsmasche-mit-nahrungsergaenzungsmitteln.html

Anwenderinformationen:

1) Mobiles Internet – Hotspot auf dem iPhone funktioniert nicht – das können Sie tun

WLAN-Hotspots sind bei vielen Nutzern täglich im Einsatz. Hier erfahren Sie, was Sie machen können, wenn der Hotspot auf Ihrem iPhone nicht funktioniert.

Mobile Datenverbindungen sind nicht nur auf dem Smartphone praktisch. Per WLAN-Hotspot lässt sich die Internetverbindung auch mit anderen Geräten teilen. Doch was tun, wenn Sie gerade unterwegs sind und der Hotspot auf Ihrem iPhone einfach nicht funktionieren will? Wir haben für diesen Fall ein paar schnelle Tipps für Sie.

Tun Sie das, wenn Ihr iPhone-Hotspot nicht funktioniert

Wenn Sie mit Ihrem iPhone einen WLAN-Hotspot erstellt haben, dieser aber nicht funktioniert, setzen Sie die folgenden Maßnahmen um, um das Problem zu beheben. Testen Sie den Verbindungsaufbau nach jedem der genannten Punkte erneut.

- Stellen Sie zunächst sicher, dass der Hotspot in den iPhone-Einstellungen unter "Persönlicher Hotspot" aktiviert ist. Sofern sich der Hotspot dort nicht starten lässt, vergewissern Sie sich, dass Sie einen Mobilfunktarif verwenden, der den Einsatz von Hotspots zulässt. Setzen Sie sich dafür gegebenenfalls mit Ihrem Provider in Verbindung.
- Aktivieren Sie in den Hotspot-Einstellungen die Option "Zugriff für andere erlauben".
- Wenn Sie ein iPhone 12 oder neuer verwenden, aktivieren Sie die Option "Kompatibilität maximieren". Diese sorgt zwar für eine geringere Leistung und Sicherheit der WLAN-Verbindung, dafür unterstützt dieser Modus aber mehr und vor allem auch ältere Endgeräte.
- Starten Sie Ihr iPhone sowie das Gerät neu, mit dem Sie auf den Hotspot zugreifen möchten. Möglicherweise liegt lediglich ein temporäres Problem mit der Software vor, das sich durch einen Neustart beseitigen lässt.
- Prüfen Sie, ob auf dem iPhone, dessen Hotspot nicht funktioniert, die aktuelle Version von iOS installiert ist. Möglich ist das unter "Einstellungen > Allgemein > Softwareupdate". Sofern ein Update zur Verfügung steht, installieren Sie dieses. Installieren Sie auch auf dem anderen Endgerät alle verfügbaren Softwareupdates.
- Setzen Sie die Netzwerkeinstellungen von iOS zurück. Navigieren Sie dafür in den Systemeinstellungen zu "Allgemein > iPhone übertragen/zurücksetzen > Zurücksetzen" und wählen Sie dort die Option "Netzwerkeinstellungen". Beachten Sie, dass dabei auch alle gespeicherten VPN- und WLAN-Verbindungen verloren gehen. Diese müssen Sie im Anschluss neu einrichten, ebenso wie den Hotspot.

Sie haben alle genannten Maßnahmen umgesetzt, aber Ihr iPhone-Hotspot funktioniert noch immer nicht? Setzen Sie sich in diesem Fall mit dem Support von Apple in Verbindung, um weitere Unterstützung zu erhalten. Erreichbar ist dieser über die Webseite getsupport.apple.com.

Tipp: Apple: iPhone lässt sich nicht zurücksetzen – so klappt es doch

Handy: iPhone-Mailbox ausschalten: So geht's für alle Modelle

Apple: Das iPhone klingelt nicht: So beheben Sie den Fehler

Quelle: https://www.t-online.de/digital/smartphone/id_100482084/hotspot-bei-iphone-funktioniert-nicht-das-koennen-sie-tun.html

2) Erstellen von Anzeigen – Kleinanzeigen-Portal veröffentlicht neue Option für Verkäufer

Bislang galt bei "Kleinanzeigen" das Ganz-oder-gar-nicht-Prinzip: das Inserat gleich online stellen oder später von vorn anfangen. Das ändert sich jetzt.

Mitglieder vom Verkaufsportal "Kleinanzeigen" können das Erstellen ihrer Anzeigen ab sofort flexibler handhaben. Die Arbeit an einem Angebot muss nicht mehr zwingend zu Ende gebracht und das Inserat dann online gestellt werden, damit es nicht verloren geht.

Es kann nun gespeichert und später zur weiteren Bearbeitung wieder aufgerufen werden, wie das Unternehmen mitteilt. Bis zu fünf Inserate sollen sich so gleichzeitig bis zu 60 Tage lang sichern lassen, sowohl für Privatleute als auch für Geschäftskunden.

Am Rechner beginnen und später auf dem Telefon weitermachen

Die Anzeigen sind den Angaben zufolge auch dann noch gespeichert, wenn man sich von der Seite abmeldet. Anders als bisher können Anzeigen so auch auf mehreren Endgeräten bearbeitet werden.

Ein praktisches Beispiel: Man beginnt mit der Arbeit am Inserat im Browser am Rechner, wechselt dann aber zum Hinzufügen der Fotos aufs Smartphone, weil die Bilder eben oft mit dem Telefon aufgenommen werden und dann dort verfügbar sind.

Option bei anderen Portalen längst Standard

Bisher sei dieser Medienbruch nur über den Umweg der zwischenzeitlichen Veröffentlichung einer Anzeige zu überwinden gewesen, erklärt das Unternehmen. Die gespeicherten Entwürfe werden im Profil über den aktuell geschalteten Inseraten angezeigt, damit sie nicht in Vergessenheit geraten.

Andere Portale wie Ebay oder Vinted bieten ihren Nutzern längst an, Entwürfe für Anzeigen zu speichern und später weiterzubearbeiten. Bei "Kleinanzeigen" war das ein langersehnter Wunsch der Anwender. Warum der Dienst das lange Zeit nicht zugelassen hat, ist nicht bekannt.

Quelle: https://www.t-online.de/digital/aktuelles/id_100693514/kleinanzeigen-de-portal-veroeffentlicht-neue-option-fuer-verkaeufer.html

3) Volksbanken bringen Girocard aufs iPhone – abseits von Apple Pay

Die Volks- und Raiffeisenbanken nutzen die Apple abgerungene NFC-Öffnung, um die Girocard in die eigene Banking-App zu integrieren – abseits von Apple Pay.

Bislang führte für iPhone-Nutzer und Banken bei Mobile Payment kein Weg an Apple Pay vorbei. Das ändert sich bald: Die Volks- und Raiffeisenbanken wollen Kunden noch im laufenden Jahr die Option geben, mit dem iPhone kontaktlos in Ladengeschäften zu zahlen – außerhalb von Apples zentralem Bezahldienst. "Die erste girocard-Transaktion auf dem iPhone – ganz ohne Apple Pay – wurde erfolgreich in unseren Testsystemen durchgeführt", wie der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR) nun auf Linkedin mitteilte.

Die Genossenschaftsbanken kommen mit diesem Schritt einer "eigenen, unabhängigen Bezahllösung für Apple-Smartphones näher", betonte der BVR. Ab dem 5. September soll

die VR-Banking-App auf iOS die entsprechende Funktionalität bieten, wie der BVR auf Nachfrage erklärte. Auf Android ist das bereits integriert. "Im ersten Schritt wird unter iOS aber nur girocard integriert. Debit- und Kreditkarten werden von uns noch bewertet", erläuterte ein Sprecher des Verbands gegenüber Mac & i. Volks- und Raiffeisenbanken steht offen, weiterhin eine virtuelle Mastercard für Apple Pay anzubieten, so der BVR.

VR-Banking-App wird iPhone-Wallet

Die VR-Banking-App wird sich ab September auch als neues Standard-Wallet auf iPhones einrichten lassen. Das gewählte Standard-Wallet öffnet sich – so wie jetzt Apple Pay / Apple Wallet – durch Annäherung an ein NFC-Bezahlterminal oder durch zweifaches Drücken auf die iPhone-Standby-Taste.

Das Interesse des BVR, Girocard-Zahlungen auf dem iPhone selbst abzuwickeln, ist keine Überraschung: Schon Anfang 2024 kündigte der Verband an, dies ermöglichen zu wollen. Um Vorwürfe der Wettbewerbsverzerrung auszuräumen und einer Strafe zu entgehen, hat Apple sich im vergangenen Jahr gegenüber der EU-Kommission zur Öffnung der NFC-Schnittstelle des iPhones verpflichtet. Unter dem kurze Zeit später greifenden Digital Markets Act ist die ursprüngliche Verdongelung der iPhone-NFC-Schnittstelle mit Apple Pay ohnehin nicht mehr zulässig.

Apple öffnet iPhone-NFC auf Druck in vielen Regionen

Im Europäischen Wirtschaftsraum setzt Apple dafür auf "Host Card Emulation", das auch in Android zum Einsatz kommt. In weiteren Regionen öffnete Apple das iPhone im vergangenen Jahr ebenfalls für andere Payment-Dienste, dort können Bezahldienste auch auf das in iPhone-Chips integrierte "Secure Element" zurückgreifen.

Bislang nutzt diese neue Freiheit nur ein großer skandinavischer Mobile-Payment-Dienst. Apples Bezahldienst wird hierzulande inzwischen von praktisch allen größeren Banken mit Kredit- und Debitkarten unterstützt. Die Girocard (teils immer noch irrtümlich "EC-Karte" genannt) in Apple Pay ist aber eine Rarität geblieben und hauptsächlich bei Sparkassen und der Commerzbank zu finden. Nicht jede Bank ist rundum glücklich mit Apple Pay, dann bei jeder solchen Transaktion von Kunden fließt eine Provision an den US-Konzern. Wenig glücklich dürfte aber auch so mancher Kunde sein, wenn seine Bank plötzlich bei Apple Pay ausschert.

Quelle: https://www.heise.de/news/Volksbanken-bringen-Girocard-aufs-iPhone-abseits-von-Apple-Pay-10363174.html

4) Apps -- Sofort löschen: 13 Apps sind laut Experten „gefährlich“

Nicht alle Anwendungen, die ein App-Store zu bieten hat, sind harmlos. Die folgenden scheinen eher eine schlechte Idee zu sein.

Sowohl Android- als auch iOS-Nutzerinnen und -Nutzer sind einer aktuellen Untersuchung zufolge durch gleich mehrere Applikationen gefährdet. Die folgenden **Apps zu löschen**, wenn du sie verwendest, kann sich entsprechend lohnen.

13 Apps löschen: Sie erlauben Zugriff auf Daten

Symantec, ein auf die Entwicklung von Software für Cybersicherheit spezialisiertes US-Unternehmen, ist einem Bericht zufolge auf diverse Anwendungen im Google Play Store sowie im Apple App Store gestoßen, die „mit fest kodierten, unverschlüsselten Anmeldedaten für Cloud-Dienste wie Amazon Web Services (AWS) und Microsoft Azure Blob Storage

ausgeliefert“ werden. Wer sie nutzt, sollte die Apps löschen – und zwar aus verschiedenen Gründen.

Zum einen ermöglichen die betroffenen Anwendungen laut den Fachleuten leichten und unbefugten Zugriff auf Speicherbereiche und Datenbanken mit sensiblen Benutzerdaten. Zum anderen könnten Kriminelle sie nutzen, um Informationen zu manipulieren oder zu stehlen.

„Diese gefährliche Methode bedeutet, dass jeder, der Zugriff auf den Binär- oder Quellcode der App hat, diese Anmeldeinformationen extrahieren und zur Manipulation oder Exfiltration von Daten missbrauchen könnte, was zu schwerwiegenden Sicherheitsverletzungen führen würde“, so die Forschenden im Detail.

Diese Anwendungen sind betroffen

Laut Symantec habe man insgesamt 13 Exemplare identifiziert, die Zugangsdaten zu Cloud-Diensten in sich tragen. Die meisten davon stammen aus dem Play Store, aber auch im App-Store der Konkurrenz fanden sich einige Beispiele. Insgesamt wurde diese bereits millionenfach von Nutzer*innen heruntergeladen.

Identifizierte Android-Apps:

1. Pic Stitch: 5 Millionen+ Downloads
2. Meru Cabs: 5 Millionen+ Downloads
3. Sulekha Business: 500.000+ Downloads
4. ReSound Tinnitus Relief: 500.000+ Downloads
5. Saludsa: 100.000+ Downloads
6. Chola Ms Break In: 100.000+ Downloads
7. EatSleepRIDE Motorcycle GPS: 100.000+ Downloads
8. Beltone Tinnitus Calmer: 100.000+ Downloads

Identifizierte iOS-Apps:

1. Crumbl: 3,9 Millionen+ Bewertungen
2. Eureka: Verdiene Geld für Umfragen – 402.100+ Bewertungen
3. Videoshop – Video Editor – 357.900+ Bewertungen
4. Solitaire Clash: Gewinne echtes Geld – 244.800+ Bewertungen
5. Zap Surveys – Verdiene leicht Geld – 235.000+ Bewertungen

Zwar bedeutet das Vorhandensein einer der oben genannten Exemplare auf deinem Handy oder Tablet noch nicht, dass deine persönlichen Daten gestohlen wurden. Sie sind darüber allerdings zugänglich für Kriminelle, wenn von Entwicklerseite keine Maßnahmen ergriffen werden, die das Risiko beseitigen. Die Apps zu löschen, ist also die beste Option, sich kurzfristig zu schützen.

Es ist zudem nicht das erste Mal, dass Symantec auf dieses spezielle Risiko hingewiesen hat. Laut dem Unternehmensblog hatte man bereits im September 2022 Alarm geschlagen als über 1.800 iOS- und Android-Apps mit AWS-Anmeldeinformationen entdeckt wurden. Damals enthielten 77 Prozent davon gültige Zugriffstoken in ihrer Codebasis.

Tipp: So kannst du Apps löschen (Android & iOS)

Quelle: https://www.futurezone.de/digital-life/apps/article593111/13-apps-loeschen-experten-warnen-davor-untersuchung-aktuellen.html?utm_source=flipboard&utm_content=topic%2Fde-digital

5) Umstrittene KI-Suchfunktion – Windows 11 schaut jetzt mit

Microsoft verteilt die neue Recall-Funktion. Automatische Bildschirmfotos sollen die Suchfunktion erleichtern, bereiten aber auch Sorgen um den Datenschutz.

Bereits vor einigen Wochen hat Microsoft angekündigt, die umstrittene Funktion Recall für alle Copilot+-Computer freizuschalten. Nun hat das Unternehmen das neue Tool für aktuelle Windows-11-PCs ausgerollt, berichtet "Golem". In der aktuellen Version ist das Unternehmen auf Datenschutzbedenken eingegangen.

Wie funktioniert Recall?

Recall erstellt im Hintergrund in regelmäßigen Abständen Screenshots vom Desktop und speichert sie lokal auf dem PC in einer Datenbank. Mithilfe von Stichworten soll der Nutzer später leichter alte Webseiten, Dokumente oder Fotos wiederfinden können.

Das funktioniert mittels KI-gestützter Computer Vision, die auf dem Gerät selbst mittels NPU-Computerchip (englisch: Neural Processing Unit) berechnet wird. Ein NPU-Chip ist also Voraussetzung. Deshalb ist Recall auch nur auf aktuellen Copilot+-PCs nutzbar.

Datenschutzbedenken haben Start verschoben

Recall sollte eigentlich schon vor einem Jahr starten. Doch heftige Datenschutzbedenken der Nutzer bremsten Microsoft aus. Der Grund: Die Software könnte womöglich sämtliche Bildschirminhalte analysieren. Schon damals versprach das Unternehmen, dass alle Daten ausschließlich lokal verarbeitet werden.

So lässt sich Recall löschen

Aufgrund dieser Datenschutzbedenken wurde das Tool nun zu einem sogenannten Opt-in-Feature, dem Kunden selbst zustimmen müssen, wenn sie es nutzen möchten. Wer das Tool generell nicht nutzen möchte, kann Recall auch vollständig vom System entfernen. Microsoft hat die Funktion als optionale Komponente in Windows 11 integriert.

So geht's: In der Windows-Suche können Sie das Menü Windows-Features aktivieren oder deaktivieren. Mit einem gesetzten Häkchen werden die Recall-Dateien vom Computer entfernt. Aber: Einige Programmreste könnten laut Microsoft noch eine Weile auf dem PC verbleiben, bevor sie endgültig gelöscht werden.

Lesetipp:

- KI-Assistent: Meta AI in WhatsApp: Wie Sie die Funktion ausblenden
- Betriebssysteme: Windows 11 unnötige Dienste deaktivieren – so geht's

Quelle: https://www.t-online.de/digital/aktuelles/id_100695314/recall-fuer-windows-11-microsoft-fuehrt-neue-funktion-ein.html

6) Der Wahnsinn – Tausende Amiga-Spiele kostenlos im Browser

Der Amiga war für viele Menschen der erste Kontakt mit Videospielen. Dank des Internet-Archivs können Sie 13.000 Titel kostenlos online spielen.

Amiga-Games kostenlos spielen: Bubble Bobble, Double Dragon, Leisure Suit Larry

Unglaublich, welche Spiele-Hits bereits zu Amiga-Zeiten (Mitte 1980ger bis frühe 1990ger-Jahre) aufgefahren wurden. Viele Spiele gingen in Serie und sind bis heute bekannt:

- Bubble Bobble
- Double Dragon
- Project X
- Lemmings
- Emerald Mine
- Leisure Suit Larry
- King's Quest
- R Type
- Marble Madness

Das Internet-Archiv unter Archive.org stellt die Amiga-Software auf deren Webplattform kostenlos und legal zum Abruf bereit. Über 13.000 Titel sind verfügbar.

Amiga-Games steuern: Keyboard, Gamepad, Maus

Gesteuert werden die angebotenen Amiga-Programme in der Regel mit dem Keyboard, manchmal auch bereits mit der Maus. Oft funktionieren hier die Spiele besser, wenn man sie in den Vollbild-Modus schaltet.

Leider klappt die Steuerung per Gamepad teilweise nicht, deswegen empfehlen wir Ihnen für den vollen Spiele-Genuss das Tool JoyToKey. Damit können Sie Keyboard-Tasten auf den Controller umlegen und so viel entspannter daddeln.

Wenn Sie mit der Tastatur spielen wollen, aber die Tasten ungünstig belegt sind, können Sie diese mit SharpKeys umbelegen. Wir wünschen viel Spaß.

Amiga Games: Die besten Remakes zum Download

Viele der Spiele bei Archive.org funktionieren leider nicht wirklich gut und lassen sich nur sehr hakelig steuern. Komfortabler spielen Sie mit den herunterladbaren Versionen. Einige der Amiga Spiele stehen mittlerweile zum kostenlosen Download bereit.

Wer es etwas moderner mag, kann außerdem gleich zu Remakes der Spiele-Klassiker greifen. Die besten Amiga Remakes stellen wir Ihnen in unserer Fotostrecke vor. Dort finden Sie auch die passenden Download-Links, um die Spiele herunterzuladen und sofort in die Retro-Gaming-Welt einzutauchen.

Quelle: https://www.chip.de/news/Der-Wahnsinn-Tausende-Amiga-Spiele-kostenlos-im-Browser_98053263.html?utm_source=flipboard&utm_content=topic%2Fde-digital

7) Tipps für den Messenger – Acht WhatsApp-Tricks, die Sie kennen sollten

Chats zitieren, Standort teilen oder Benachrichtigungstöne ändern: WhatsApp bietet viele Funktionen, die nicht sofort ersichtlich sind. Diese sollten Sie kennen.

Millionen Menschen nutzen täglich WhatsApp. Der Messenger bietet viele Funktionen, um Nutzern die Kommunikation zu erleichtern. Wir zeigen Ihnen acht Tipps:

1. Standort teilen

Wenn Sie mit einem Nutzer schnell den Standort teilen wollen, klicken Sie im Chat unten auf das Büroklammer-Symbol, beim iPhone auf das "+"-Symbol. Im aufpoppenden Menü wählen Sie "**Standort**". Um den Standort teilen zu können, müssen Sie die GPS-Funktion Ihres Smartphones aktivieren.

2. Nachricht schnell zitieren

Nutzer können eigene Chatnachrichten und die von Kontakten zitieren. Drücken Sie dafür auf die gewünschte Nachricht, bis sie markiert ist. Im Menü oben wählen Sie nun den Pfeil, der nach links zeigt. So zitieren Sie die Nachricht im derzeitigen Chatverlauf. Schneller geht es, wenn Sie die gewünschte Chatnachricht nach rechts wischen.

Übrigens: Mit dem Pfeil nach rechts schicken Sie die Nachricht an einen anderen Kontakt oder eine Gruppe.

3. Benachrichtigungston für Kontakte bestimmen

Sie können jedem Kontakt einen individuellen Ton geben. Klicken Sie dafür im Chat mit einem Kontakt auf dessen Namen. Jetzt öffnet sich sein Profil. Wählen Sie hier "Eigene Benachrichtigungen" (Android) beziehungsweise "Eigene Töne" (iPhone). Hier können Sie verschiedene Einstellungen vornehmen.

4. Chatnachrichten als Favoriten speichern

Wenn Sie eine Chatnachricht für später speichern möchten, können Sie sie mit einem Stern markieren. Drücken Sie dafür auf die gewünschte Nachricht, bis sie markiert ist. Im Menü oben wählen Sie nun den Stern.

Um die gespeicherten Nachrichten aufzurufen, klicken Sie im Fenster mit den Kontakten auf die drei Punkte rechts oben. Unter dem Punkt "**Mit Stern markierte**" finden Sie die gespeicherten Nachrichten.

5. Hintergründe ändern

Die Hintergründe in den Chats lassen sich in den Einstellungen ändern. Klicken Sie im Fenster mit den Kontakten auf die drei Punkte rechts oben, dann auf "**Einstellungen**". Beim iPhone wählen Sie den "**Einstellungen**"-Reiter unten rechts. Als Nächstes wählen Sie "**Chats**". Hier findet sich die Option "**Hintergründe**". WhatsApp stellt verschiedene Quellen zur Auswahl, beispielsweise die Galerie.

6. Kontakte aktualisieren

Wenn Sie einen neuen Nutzer im Adressbuch haben, müssen Sie ihn aus der Kontaktliste wählen, um einen Chat zu starten. Manchmal kann es jedoch sein, dass der Kontakt da nicht auftaucht. In dem Fall kann es helfen, die Liste zu aktualisieren. Klicken Sie dafür im Fenster mit den Chats auf das grüne Symbol unten rechts. Jetzt erscheint eine Liste mit allen

Kontakten. Klicken Sie nun oben rechts auf die drei Punkte und als nächstes auf "**Aktualisieren**". Nun sollte der gewünschte Kontakt in der Liste erscheinen.

7. Gruppennachrichten ausschalten

Wen ständige Gruppenbenachrichtigungen nerven, der kann entweder die Gruppe verlassen oder den Gruppenchat stummschalten. Klicken Sie dafür auf den Chat, den Sie stummschalten wollen. iPhone-Nutzer tippen im Chatfenster oben auf den Namen der Gruppe, um das Einstellungsmenü zu öffnen. Als Nächstes wählen Sie die drei Punkte rechts oben und dann "**Benachr. stummschalten**."

Jetzt können Sie einstellen, ob die Nachrichten für acht Stunden, eine Woche oder ein Jahr stumm bleiben sollen. Das Gleiche funktioniert auch in Chats mit einzelnen Kontakten.

8. Gemeinsame Gruppen finden

Um zu prüfen, welche Gruppen Sie sich mit einem Kontakt teilen, klicken Sie im Chat mit einem Kontakt auf seinen Namen. Jetzt öffnet sich sein Profil. Scrollen Sie runter, bis Sie den Reiter "**Gemeinsame Gruppen**" sehen.

Quelle: https://www.t-online.de/digital/whatsapp/id_84903806/whatsapp-diese-acht-tricks-sollten-sie-kennen-chat-standort-und-mehr.html

8) Was kann ChatGPT eigentlich alles?

KI-Tools können im Alltag und bei der Arbeit durchaus nützlich sein. Die meisten großen Sprachmodelle gehen mittlerweile jedoch weit über die reine Textverarbeitung hinaus. Wir verraten dir, was ChatGPT aktuell alles kann.

ChatGPT hat das Thema Künstliche Intelligenz salonfähig gemacht. Nur zwei Monate nach der Veröffentlichung verzeichnete die KI über 100 Millionen Nutzer weltweit. Damit ist ChatGPT die am schnellsten wachsende Internet-Anwendung aller Zeiten. Mittlerweile zählt Entwicklerunternehmen OpenAI weltweit über 300 Millionen monatlich aktive Nutzer – und über eine Million zahlende Abonnenten.

Deutschland hat sich dabei zu einem der wichtigsten Märkte für das Unternehmen entwickelt. Laut einer Studie des TÜV-Verbands haben 91 Prozent der Deutschen schon einmal von KI-Tools wie ChatGPT gehört. Mehr als die Hälfte hat sie demnach bereits genutzt.

Was kann ChatGPT?

Rund um die besten KI-Modelle hat sich mittlerweile ein regelrechter Wettstreit entwickelt. Nach OpenAI haben große Tech-Konzerne wie Google, Microsoft und Facebook-Mutterkonzern Meta eigene KI-Systeme entwickelt. Aber auch Unternehmen wie Anthropic oder Perplexity mischen im KI-Wettstreit mit.

Sie alle vereint das Ziel, die besten KI-Modelle entwickeln zu wollen – mit teilweise unterschiedlichen Ansätzen. Neben der reinen Rechenleistung spielt dabei auch der Funktionsumfang eine entscheidende Rolle.

Aufgrund der rasanten technologischen Entwicklung im Bereich Künstliche Intelligenz gehen die meisten großen Sprach- und KI-Modelle bereits seit einiger Zeit über die reine Textverarbeitung hinaus. In der folgenden Übersicht verraten wir dir deshalb, was ChatGPT mittlerweile kann und welche Möglichkeiten dir die KI bietet. Einige Funktionen sind jedoch nur über ein Bezahl-Abo nutzbar.

1. Fragen beantworten (Suchmaschine)

ChatGPT funktioniert ähnlich wie klassische Suchmaschinen. Im Gegensatz zu Google und Co. kannst du der KI jedoch konkrete Fragen stellen, um konkrete Antworten auf eine Frage zu erhalten. ChatGPT fasst dir die wichtigsten Informationen dann in Form einer Antwort samt einigen Quellen zusammen. Eine herkömmliche Liste mit Links wie bei Google erhältst du jedoch nicht. Dafür hast du die Möglichkeit, Nach- und Rückfragen zu stellen. Solltest du mit einer Antwort etwa unzufrieden sein oder mehr Informationen benötigen, kannst du beispielsweise nach Gegenargumenten oder ausführlicheren Beschreibungen fragen.

2. Texterstellung

Ob Blogbeiträge, Social Media-Posts, Werbetexte oder Beschreibungen jeglicher Art: ChatGPT kann so ziemlich jede Form von Texten für dich erstellen. Die Qualität und den Umfang bestimmst du selbst über deine Prompts beziehungsweise Eingaben. Neben dem Thema und der Textform hast du beispielsweise die Möglichkeit, den Stil, Umfang und die Struktur festzulegen. Ein Beispiel: „Schreib mir einen kurzen Erklärtext dazu, was BASIC thinking ist. Er sollte maximal 200 Wörter lang sein. Aufbau: Einleitung, Erklärung, Fazit.“

3. Korrekturen

ChatGPT kann dir dabei helfen, Texte zu korrigieren und Fehler zu finden. Gib der KI einen entsprechenden Befehl und kopieren anschließend einen Link oder Text in das Aufforderungsfenster. Ein Beispiel: „Bitte lies den folgenden Text auf Rechtschreibung und Grammatik Korrektur und stelle mir die Fehler samt Verbesserungen heraus“. Dir sollte jedoch stets bewusst sein, dass KI-Modelle wie ChatGPT aufgrund ihrer Funktionsweise nicht alle Fehler finden können. Denn: Viele KI-Systeme speisen ihre Informationen aus dem Internet und können dadurch auch Falschinformationen enthalten.

4. Bildgenerierung

Du kannst dir mit ChatGPT Bilder in den verschiedensten Stilrichtungen generieren lassen. Format, Farben und Thema kannst du dabei selbst bestimmen. Ein Beispiel: „Generier mir ein abstraktes Bild zum Thema xyz im Format 16:9“. Sofern du KI-generierte Bilder veröffentlichen möchtest, solltest du jedoch darauf achten, diese entsprechend zu kennzeichnen („Mit KI generiert“) – und zwar ohne irreführende Dinge zu suggerieren.

5. Ideenfindung und kreative Arbeit

KI-Modelle wie ChatGPT können dir dabei helfen, Ideen zu bestimmten Themen zu finden. Ein Beispiel: „Ich möchte eine Geschichte über Tiere im Weltraum schreiben. Welche Ideen hast du für mich?“ Je nach deinen Anforderungen kann dir die KI auch dabei helfen, Produkte, Kampagnen oder Projekte zu beschreiben. Theoretisch hast du sogar die Möglichkeit, dir komplette Drehbücher, Liedtexte oder Gedichte schreiben zu lassen. In puncto Urheberrecht und Vermarktung gibt es diesbezüglich aber Unklarheiten.

6. Übersetzungen

Mit ChatGPT kannst du dir Texte in über 100 Sprachen übersetzen lassen. Ein Beispiel: “ Übersetze mir den folgenden Text ins Italienische: …“.

7. Programmierhilfe

Du kannst die OpenAI-KI auch nutzen, um Unterstützung bei Programmiersprachen zu erhalten. Beispiel: „Erstell mir den html-Code für eine Tabelle mit vier Zeilen und vier Spalten“. Außerdem hast du die Möglichkeit, bereits bestehende Codes auf Fehler hin überprüfen zu lassen. Im Gegensatz zu anderen KI-Modellen, die auf das Coden und

Programmieren ausgelegt sind, hat ChatGPT jedoch gewisse Grenzen und kann allenfalls als Assistent fungieren.

8. Mathematische Berechnungen

ChatGPT kann einfache und auch komplexere mathematische Aufgaben und Probleme lösen. Die KI fungiert also ebenfalls als eine Art Taschenrechner – nur deutlich umfangreicher. Du hast außerdem die Möglichkeit, dir Gleichungen umformen zu lassen.

9. Texte und Dokumente zusammenfassen

Du hast einen Artikel oder Text, der dir zu lang ist, um ihn komplett zu lesen? Dann kannst du ChatGPT darum bitten, ihn für dich zusammenzufassen. Die Länge der Zusammenfassung bestimmst du selbst. Außerdem kannst du dir sowohl Dokumente, Linkinhalte als auch Texkopien bündeln lassen.

10. Unterhaltung und Assistenz

ChatGPT kann dir beim Verfassen von E-Mails, der Organisation von Terminen und anderen alltäglichen Aufgaben helfen. Du kannst aber auch einfach nur mit der KI chatten und eine Konversation führen. Mittlerweile nutzen allerdings nur wenige Menschen KI-Modelle zur Unterhaltung. Denn: Für subjektive Ratschläge und Lebensweisheiten sind KI-Modelle definitiv die falsche Adresse.

Hinweis: Dir sollte stets bewusst sein, dass KI-Modelle nicht fehlerfrei sind, da sie zu sogenannten Halluzinationen neigen. Die Folge sind falsche oder erfundene Informationen, die entstehen können, weil Sprachmodelle anhand von Mustern und Wahrscheinlichkeiten antworten, anstatt anhand von echtem Wissen oder Verständnis. Da viele KI-Modelle mithilfe von Daten aus dem Internet trainiert werden, sind sich nicht fehlerfrei. Vor allem bei sensiblen Themen ist es deshalb ratsam, Informationen und Inhalte auf ihren Wahrheitsgehalt hin zu überprüfen.

Auch interessant:

- KI-Sprachmodelle: Was sind eigentlich Large Language Models?
- Copilot: Alles, was du über die Microsoft-KI wissen musst
- KI-Kontextfenster: Das „Sichtfenster“ von Künstlicher Intelligenz
- Künstliche Intelligenz: 7 KI-Podcasts, die du kennen solltest

Quelle: https://www.basicthinking.de/blog/2025/04/02/was-kann-chatgpt-eigentlich-alles/?utm_source=flipboard&utm_content=MobilityMag/magazine/Neu+bei+Mobility+Mag

9) WhatsApp – Sprachnachrichten aufnehmen wird einfacher

WhatsApp testet eine neue Funktion zum Aufnehmen von Sprachnachrichten. Für Nutzer bedeutet die Änderung eine deutliche Erleichterung.

Bisher müssen WhatsApp-Nutzer entweder das Mikrofonsymbol gedrückt halten, um eine Sprachnachricht aufzunehmen, oder den Button nach oben wischen, um eine Sperre zu aktivieren. In der neuen Version reicht es aus, das Mikrofonsymbol einmal kurz anzutippen, um den Aufnahmemodus zu starten, wie das Portal "WABetaInfo" schreibt.

Diese Neuerung kombiniert die beiden bisherigen Methoden und aktiviert automatisch den Sperrmodus, der bisher nur durch Wischen erreichbar war. Nach dem Antippen des Mikrofonsymbols sehen Nutzer die Dauer der Sprachnachricht, eine Audiowelle sowie Buttons zum Löschen, Pausieren oder zum Absenden der Nachricht.

Nutzer haben mehr Kontrolle

Ein weiterer Vorteil der neuen Funktion ist die Möglichkeit, vor dem Absenden zu entscheiden, ob die Sprachnachricht nur ein einziges Mal vom Empfänger angehört werden darf. Dies bietet den Nutzern mehr Kontrolle über ihre gesendeten Inhalte.

Die Änderung zielt darauf ab, die Kommunikation flüssiger zu gestalten und die Bedienung zu vereinfachen. Besonders bei längeren Sprachnachrichten könnte die neue Funktion hilfreich sein.

Neue Funktion aktuell nur für ausgewählte Nutzer

Allerdings gibt es auch potenzielle Nachteile. So könnte es häufiger zu versehentlichen Aktivierungen der Sprachaufnahme kommen, wenn ein einfaches Antippen des Mikrofonsymbols ausreicht.

Aktuell ist die neue Funktion nur für ausgewählte Nutzer der iOS-Beta-Version 25.13.10.70 verfügbar, die die Beta-Version von WhatsApp über Testflight installiert haben. Wie bei neuen Funktionen üblich, testet WhatsApp diese mehrere Wochen oder sogar Monate, um Feedback zu sammeln und mögliche Fehler zu beheben, bevor sie für alle Nutzer freigeschaltet wird.

Tipp:

- KI-Assistent: Meta AI in WhatsApp: Wie Sie die Funktion ausblenden
- Messenger-Tipp: WhatsApp-Sprachnachrichten abhören: So klappt's
- Tipps zur Chat-Anwendung: WhatsApp: Blaue Haken verraten nicht nur die Zustellzeit

Quelle: https://www.t-online.de/digital/aktuelles/id_100696892/whatsapp-sprachnachrichten-neue-funktion-erleichtert-aufnahme.html

10) Ab heute: Bis zu 100 Prozent mehr Datenvolumen bei Magenta Mobil Prepaid

Die Telekom erhöht heute deutlich das monatliche Datenvolumen bei den meisten Magenta-Mobil-Prepaid-Tarifen. Das sind die neuen Tarife ab dem 29.4.2025.

Alle Jahre wieder … erhöht die Deutsche Telekom das Datenvolumen in den Magenta-Mobil-Prepaid-Tarifen. So auch 2025, und zwar ab dem 29. April, also ab heute. Die Preise bleiben unverändert.

Das sind alle Magenta-Mobil-Prepaid-Tarife ab dem 29.4.2025:

- MagentaMobil Prepaid S: 1 GB für 4,95 Euro / 28 Tage **(unverändert)**
- MagentaMobil Prepaid M: 13 GB für 9,95 Euro / 28 Tage (bisher: 8 GB)
- MagentaMobil Prepaid L: 25 GB für 14,95 Euro / 28 Tage (bisher: 15 GB)
- MagentaMobil Prepaid XL: 50 GB für 19,95 Euro / 28 Tage (bisher: 25 GB)
- MagentaMobil Prepaid Max: unlimited GB für 99,95 Euro / 28 Tage **(unverändert)**
- MagentaMobil Prepaid Jahrestarif: 156 GB für 12 Monate (13 GB / mtl.) für 99,95 Euro (bisher: 96 GB für ein Jahr)

Unverändert bleiben also die Tarife MagentaMobil Prepaid S und Max. Die 5G-Nutzung ist immer enthalten. Telefon- und SMS-Flatrates in alle deutschen Netze sind in fast allen Tarifen immer enthalten, ausgenommen beim Tarif S: dort gelten die Flatrates nur innerhalb des Telekom-Mobilfunknetzes. Außerdem gibt es bei Prepaid S noch 50 Minuten für Anrufe in alle anderen deutschen Netze.

Alle Preise beziehen sich auf einen Abrechnungszeitraum von 28 Tagen. Nicht verbrauchtes Inklusiv-Datenvolumen kann in den meisten Tarifen weiterhin im folgenden Abrechnungszeitraum genutzt werden – das führte die Telekom im August 2024 für die Prepaid-Tarife ein. Dort wird es vorrangig verbraucht, bevor das neue Datenvolumen angebrochen wird. Möglich ist das in den MagentaMobil-Prepaid-Tarifen M, L, XL sowie im Jahrestarif.

Die Schweiz wird in allen Magenta-Mobil-Prepaid-Tarifen wie die EU behandelt – das zog die Telekom 2024 glatt. Es fallen fürs Surfen, Telefonieren oder Simsen also keine Extra-Kosten an.

Unverändert bleibt bei allen Tarifen der individuelle Datenbonus in der MeinMagenta-App.

Die neuen monatlichen Datenvolumen gelten sowohl für Neu- als auch Bestandskunden. Die neuen Prepaid-Tarife sind ab dem 29. April 2025 im Telekom-Shop, online auf telekom.de, im Kundenservice sowie im Handel buchbar.

Quelle: https://www.pcwelt.de/article/2762354/deutsche-telekom-ab-heute-mehr-datenvolumen-magenta-mobil-prepaid.html?utm_date=20250429095809&utm_campaign=Best-of%20PC-WELT&utm_content=slotno1-pushheadline-Ab%20heute%3A%20Bis%20zu%20100%20Prozent%20mehr%20Datenvolumen%20bei%20Magenta%20Mobil%20Prepaid&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

11) YouTube ganz ohne Werbung und Tracking: Dieses Kostenlos-Tool macht's möglich

Die offizielle YouTube-App ist voller Werbeunterbrechungen und sammelt zudem Nutzungsdaten. Wer genug davon hat, ist mit FreeTube besser bedient.

YouTube ist nicht nur in der Gratis-Version mit Werbung übersät, sondern speichert zudem die Daten der Nutzer über die angesehenen Videos. Das mag hilfreich für Videovorschläge sein, um noch passendere Empfehlungen für Ihre Clips zu erhalten. Allerdings lässt sich das Tracking nur durch **Löschen des Wiedergabeverlaufes** etwas eingrenzen.

Doch die kostenlose Software FreeTube will das ändern. Sie verspricht nicht nur eine private Nutzung ohne das Tracking der Daten. Sie lässt sich zudem auch wie das bekannte Videoportal bedienen – und macht dabei mit vielen nützlichen Funktionen auf sich aufmerksam.

FreeTube: Kostenlos und voller Funktionen

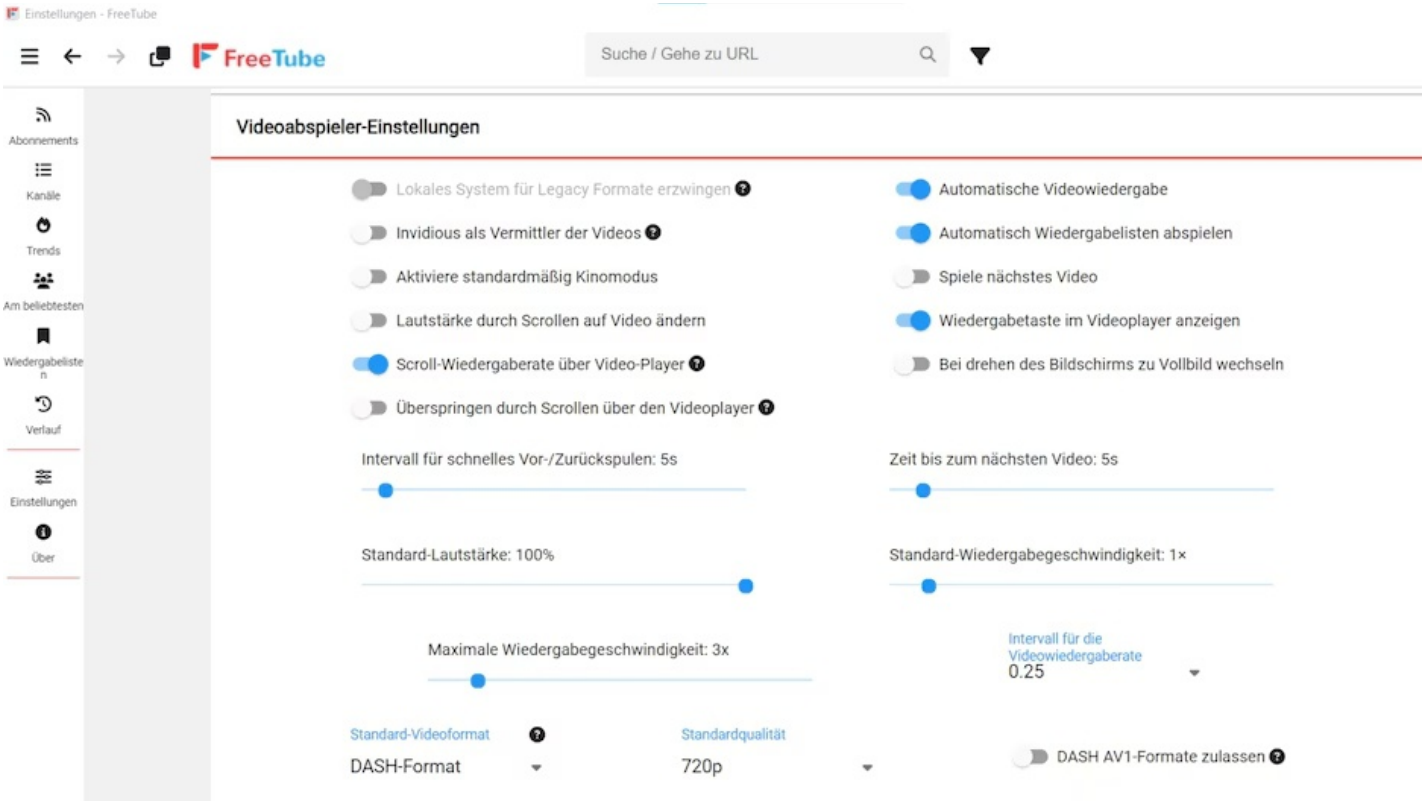
Vom generellen Aufbau und Layout erinnert FreeTube stark an die bekannte Videoplattform. Auf der linken Seite finden sich dort die wichtigsten Menüpunkte wie die Abonnements oder die aktuellen Trendvideos wieder.

Anders als bei YouTube benötigen Sie hier **allerdings keinen Account**, um den einzelnen Kanälen zu folgen. Sie haben jedoch trotzdem die Wahl, Ihre Abonnements direkt in die Anwendung zu importieren.

Über die Lupe können Sie das Video Ihrer Wahl suchen und filtern lassen. Wenn Sie den passenden Clip gefunden haben, können Sie sich dieses ohne Werbeunterbrechung in dem Programm ansehen.

Außerdem lässt sich das Video **direkt in der Anwendung speichern** oder auf Ihrem Rechner herunterladen. Für den Download stehen Ihnen daraufhin die verschiedensten Auflösungen zur Verfügung.

Weitere Features des Media-Players



Die Einstellungsmöglichkeiten der Software sind enorm. Foto: FreeTube

Das Besondere an FreeTube ist hierbei, dass die Software die Aktivitäten nicht in eine Cloud oder ähnliches weiterleitet, sondern lokal abspeichert. Somit werden **Ihre Suchverläufe nicht an YouTube weitergegeben**, bleiben aber trotzdem in der Anwendung enthalten.

Zudem ist die Software Open Source und kann dadurch stetig von Entwicklern und Nutzern verbessert werden. Ein weiterer Unterschied zu YouTube sind vor allem die umfangreichen Einstellungen der Software. Hier können Sie nach Belieben die verschiedensten Einstellungen zu den einzelnen Bereichen treffen, um das Ansehen der YouTube-Inhalte noch individueller zu gestalten.

Anmerkung der Redaktion: Free Tube kann unter dem u.g. Link downgeloaded werden

Quelle: https://www.chip.de/news/YouTube-ganz-ohne-Werbung-und-Tracking-Dieses-Kostenlos-Tool-machts-moeglich_185121774.html?utm_source=chip_1001310&utm_medium=email&utm_campaign=1018832&utm_content=29.04.2025

12) Diese praktische Webseite besuche ich einmal im Monat – und ihr solltet es auch!

Einmal im Monat tippe ich meine Mail-Adressen in den Online-Dienst von „Have I Been Pwned“ ein, um zu prüfen, ob meine Daten Opfer eines Datenlecks geworden sind. Denn dieser simple Check kann mich vor bösen Überraschungen bewahren.

„Have I Been Pwned“ schenkt mir reinen Datenschutz-Wein ein

Ich mache es seit Jahren: Am ersten Sonntag im Monat checke ich auf haveibeenpwned.com, ob Account-Daten, die ich mit meiner Mail-Adresse angelegt habe, in neuen Datenlecks aufgetaucht sind. **Und leider werde ich regelmäßig fündig**. Mal sind es Gaming-Publisher von alten Browser- und Online-Spielen wie etwa Gamigo oder Zynga, die

gehackt wurden, manchmal trifft es aber auch größere Social-Media-Plattformen wie Twitter oder Konzernriesen wie Adobe. Auf der Webseite könnt ihr einfach eure Mail-Adresse eingeben und der Service verrät euch dann, ob und in welchen Datenlecks eure Account-Daten aufgetaucht sind. Und nicht nur das – „Have I Been Pwned“ gibt auch an, was für Daten kompromittiert wurden. Konnten die Angreifer nur Mail-Adressen erbeuten? Oder wurden auch weitere sensible Daten wie Telefonnummern und Passwörter ergaunert? Hier ein Beispiel, wie das im Ernstfall auf der Webseite aussehen kann:

Ein paar Accounts, die ich mit meiner ganz alten Mail-Adresse erstellt habe, waren anscheinend Teil von Datenlecks. (© GIGA)

Die unangenehme Wahrheit ist: **Niemand ist sicher vor Datenlecks**. Besonders gefährlich wird es, wenn ihr – wie früher auch ich – überall das gleiche Passwort verwendet. Dann reicht ein einziges Leak, um theoretisch alle eure Accounts zu gefährden. Die Folgen können dann von peinlichen Fake-Posts in eurem Namen bis hin zu leergeräumten PayPal-Konten reichen, wenn ihr keine Zwei-Faktor-Authentifizierung eingerichtet habt. **Kleiner Zusatz-Tipp:** Wer nicht wie ich jeden Monat die Webseite selbst ansteuern will, kann sich über „Notify me“ ganz oben auf der Webseite für den Alert-Service von „Have I Been Pwned“ registrieren. Dann **bekommt ihr automatisch eine Warnung per Mail**, wenn eure Adresse in einem neuen Leak auftaucht.

Integrierte Passwort-Manager in Browsern bieten oft ähnliche Funktion

Wem selbst das zu aufwendig ist: Es gibt noch eine Alternative. Browser wie Google Chrome, Microsoft Edge, Mozilla Firefox und Safari bieten einen **Passwort-Check** an, der euch mitunter nicht nur über Datenlecks informiert, sondern euch auch auf schwache oder doppelte Passwörter hinweist – vorausgesetzt ihr nutzt den integrierten Passwort-Manager des jeweiligen Browsers. Klar, auch diese Tools bieten keine hundertprozentige Sicherheit. Manche Leaks bleiben unentdeckt oder werden erst Monate später gemeldet. Dennoch: Diese simplen Vorsichtsmaßnahmen können euch viel Ärger ersparen. Euer digitales Ich wird es euch danken.

Quelle: https://www.giga.de/tech/diese-praktische-webseite-besuche-ich-einmal-im-monat-und-ihr-solltet-es-auch--01JP85YTXKVC7DR3JSR5J9K2RV?utm_source=flipboard&utm_content=topic%2Fde-digital

Allgemeines:

1) Auto & Mobilität --Urteil: Nicht alle Marderbiss-Schäden werden erstattet

Beißt ein Marder am Auto Kabel kaputt, springt meist die Kaskoversicherung ein. Doch hat das Tier Isoliermaterial beschädigt, bleibt man auf den Reparaturkosten dafür womöglich sitzen. Das zeigt ein Urteil des Amtsgerichts Frankfurt am Main (Az.: 29046 C 103/24), auf das das Rechtsportal "anwaltsauskunft.de" verweist.

Im konkreten Fall hat die Versicherung Schäden durch Tierbisse an Kabeln, Schläuchen, Leitungen und deren "unmittelbare Folgeschäden" abgedeckt. Die Reparaturkosten für die Schläuche übernahm der Kaskoversicherer, doch nicht die Summe von etwa 1.200 Euro für die Beseitigung der Schäden am Dämmmaterial. Dagegen klagte der betroffene Autobesitzer.

Nur bestimmte Teile sind versichert

Ohne Erfolg. Das Amtsgericht wies die Klage ab, da das Isoliermaterial nicht zu den in der Klausel des Versicherungsvertrages genannten Teilen und auch nicht zu deren Folgeschäden zählt - also Schäden, die in dem Fall durch zerbissene Kabel, Schläuche oder Leitungen verursacht werden können. Defekte an der Lenkung oder am Motor, zum Beispiel.

Der Schaden am Dämmmaterial indes ist laut Gericht als eigener und direkt vom Marder verursachter Schaden zu werten - und sei als solcher nicht versichert.

Auch das Argument des Klägers, dass die einschränkende Auslegung der Klausel überraschend sei, ließ das Gericht nicht gelten. Es sei nachvollziehbar, dass Versicherer ihre Prämien nur für klar definierte Risiken kalkulieren könnten und aus dem Grund nicht "alle Schäden" abdecken müssten. © Deutsche Presse-Agentur

Quelle: https://www.gmx.net/magazine/auto/urteil-marderbiss-schaeden-erstattet-40914204

2) Nur mit den richtigen Reifen – Italien führt im Sommer neue Auto-Regel ein – was ab Mai gilt

Nicht selten führt das bei Deutschen beliebte Urlaubsland vor der Sommersaison neue Regeln ein – so auch 2025. Auf was Autofahrer achten sollten.

Die aus Deutschland verhältnismäßig günstige Bußgelder gewohnten Autofahrer stoßen in Italien gern auf harte Realitäten. Denn nicht selten stehen hinter der **Brenner-Mautstelle** Carabinieri oder die Polizia di Stato. Die italienischen Ordnungskräfte ziehen auch gut und gern die fahrbaren Untersätze mit deutschen Kennzeichen auf den Standstreifen, die sich in den Sommermonaten zuhauf über den Grenzpass schieben.

Vom Glauben fällt dann der eine oder andere Urlauber ab, wenn ihm Ordnungswidrigkeiten in Rechnung gestellt werden, die ihm bis dato völlig unbekannt waren. Denn Italien ändert vor der Sommersaison beizeiten die Verkehrsregeln, etwa die Pflicht zum Einschalten der **Beleuchtung** – auch am helllichten Tag. Im Jahr 2025 müssen Urlauber nun darauf achten, vor dem Grenzübertritt die richtige Bereifung aufzuziehen.

Italien: Keine Winterreifen im Sommer - diese Regelung muss beachtet werden

Denn zwischen dem **16. Mai bis 15. Oktober** dürfen in Italien keine Fahrzeuge mit

Winterreifen geführt werden, was auch für ausländische PKW gilt. Die Neuregelung betrifft sowohl Autos als auch Anhänger, schreibt der ADAC. Nur **Motorräder** seien ausgenommen. Bis 15. April galt in Italien hingegen die Pflicht, mit Winterreifen zu fahren – bis einschließlich 15. Mai muss also umgerüstet werden. Wer sich nicht daran hält, riskiert eine Strafe. Die soll laut der „Gazzetta Motori“ bei 422 bis 1695 Euro liegen**.** Allerdings gilt für bestimmte Bereifungen eine Ausnahme. Vor der Fahrt nach Italien sollten Fahrzeugführer unbedingt prüfen, ob ihre Bereifung darunter fällt.

Denn der Grenzübertritt ist mit Winter- und **Ganzjahresreifen** (M&S) erlaubt, wenn sie einen „Speedindex“ haben, der mit dem im Fahrzeugschein identisch oder höher ist, heißt es unter anderem vom ADAC. Der Geschwindigkeitsindex gibt an, welche Höchstgeschwindigkeit mit dem verbauten Reifen gefahren werden darf – ist also unabhängig von der eingetragenen Höchstgeschwindigkeit des Fahrzeugs. Wer also herausfinden möchte, ob die Ganzjahresreifen auch im Sommer in Italien gefahren werden dürfen, muss die entsprechende Position im Fahrzeugschein mit der Nummer auf dem Reifen vergleichen.

Reifen: Wo der Speedindex zu finden ist

Im Fahrzeugschein ist der Speedindex auf der letzten Seite im Feld 15.1. bis 15.3. abzulesen. Dort findet sich die zulässige Reifendimension, wobei der letzte Buchstabe den Speedindex angibt. Auf dem Reifen findet sich die entsprechende Nummer auf der Seitenfläche. Nur wenn der Index auf dem Reifen (also der letzte Buchstabe der Abfolge) identisch oder höher als der im **Fahrzeugschein** ist, ist eine Fahrt in Italien erlaubt. Zur besseren Übersicht, welche Geschwindigkeitsgrenzen die einzelnen Buchstaben bedeuten, hier eine Übersicht, wie sie unter anderem Reifenhersteller Continental veröffentlicht:

Letzter Buchstabe auf dem Reifen/unter 15.1. bis 15.3.	Zulässige Höchstgeschwindigkeit in km/h
B	50
J	100
K	110
L	120
M	130
N	140
P	150
Q	160
R	170
S	180
T	190
U	200
H	210
V	240
Z	>240

Italien: Diese Strafen drohen

Ein Rechenbeispiel: Die Abfolge eines Renault R4 schließt im Fahrzeugschein unter 15.1. & 15.2. mit dem Buchstaben „M“. Das heißt, das Auto darf mit der im Fahrzeugschein eingetragenen Bereifung nicht schneller als 130 km/h fahren. Dass es technisch bedingt nicht schneller fahren kann, spielt hierbei keine Rolle. Auf der **Allwetterbereifung** steht allerdings ein „T“, was sich nicht mit den Angaben im Fahrzeugschein deckt. Eine Einreise ist

dennoch erlaubt, da der Speedindex auf dem Reifen mit „T“ (zugelassen bis zu 190 km/h) deutlich höher ist als im Fahrzeugschein mit M (bis zu 130 km/h). Wären die Angaben auf der Bereifung niedriger, könnte ein Bußgeld verhängt werden.

Und das nicht zu knapp: Laut ADAC droht bei Verstößen ein Bußgeld zwischen 431 und 1734 Euro. Im Zweifel könnte eine Beschlagnahmung und eine Nachbesichtigung erfolgen, bei der die **Zulässigkeit** geprüft werde, heißt es vom Automobilclub. Andre Medien berichten allerdings von einer Übergangszeit, in der Zuwiderhandeln zunächst noch toleriert werde.

Quelle: https://www.morgenpost.de/ratgeber-wissen/article408800560/italien-fuehrt-im-sommer-neue-auto-regel-ein-was-ab-mai-gilt.html?utm_source=flipboard&utm_content=morgenpost/magazine/Berliner+Morgenpost

3) Achtung Mallorca-Urlauber – Fake-Knöllchen für Mietwagen-Kunden

Auf Mallorca sorgt derzeit eine neue Betrugsmasche für Verunsicherung unter Mietwagenkunden. Mehrere Urlauber aus Deutschland berichten nach Angaben der Mallorca-Zeitung über gefälschte Bußgeldbescheide, die angeblich von der spanischen Verkehrsbehörde Dirección General de Tráfico (DGT) stammen sollen.

Die Schreiben beziehen sich auf Geschwindigkeitsverstöße auf einer Straße, die auf der Baleareninsel jedoch nicht existiert. Die Zeitung zitiert ein Ehepaar aus Trier, das im Februar 2025 einen Mietwagen der Firma Goldcar genutzt hatte. Kurz darauf flatterte ein Bußgeldbescheid über 200 Euro wegen eines angeblichen Tempoverstoßes ins Haus. Die Geschwindigkeit soll dabei 76 km/h auf einer auf 50 km/h begrenzten Straße betragen haben. Auffällig: Der Vorfall soll sich auf der Straße M-404 ereignet haben – einer Strecke, die es auf Mallorca gar nicht gibt.

"Wir haben uns sehr gewundert, weil wir an diesem Tag das Auto gar nicht benutzt hatten", so das Ehepaar gegenpber der Mallorca Zeitung. Der Bescheid enthielt jedoch sämtliche korrekten Daten: von der Ausweis- und Führerscheinnummer bis zur Adresse in Deutschland und den Angaben zum Mietwagen inklusive Kennzeichen. Erst ein Gespräch mit Freunden auf Mallorca brachte den entscheidenden Hinweis. "Uns wurde gesagt, dass bei echten Bescheiden aus Spanien immer ein Hinweis auf den Rabattsatz bei schneller Zahlung enthalten ist. Der fehlte hier", so die Betroffenen.

Straße M-404 existiert nicht auf Mallorca

Zudem war das beigefügte Blitzerfoto von schlechter Qualität – das Kennzeichen war darauf nicht zu erkennen. Entscheidend war letztlich die Recherche zur angegebenen Straße. Die Bezeichnung M-404 verweist auf eine Strecke im Süden der Autonomen Gemeinschaft Madrid. Straßen auf Mallorca beginnen dagegen mit "Ma" (für "Mallorca") oder seltener mit "PM" (für "Palma de Mallorca").

Das Ehepaar aus Trier waren wohl nicht die einzigen Urlauber, die angeschrieben wurden. In einem Forum fanden sich zahlreiche ähnliche Erfahrungsberichte, ebenfalls in Zusammenhang mit dem Mietwagenanbieter. Auch bei der Mallorca Zeitung meldete sich ein weiterer deutscher Kunde mit fast identischem Vorfall.

Nach Rücksprache mit der spanischen Verkehrsbehörde DGT erhielten die Urlauber eine eindeutige Antwort: "Es handelt sich um Betrug, nicht zahlen!" Auch der Mietwagenanbieter Goldcar riet nach interner Prüfung davon ab, den Betrag zu überweisen. Die örtliche Polizei in Palma verwies auf die Zuständigkeit der deutschen Polizei.

Goldcar bestätigt Problem – Ermittlungen laufen

Ein Sprecher von Goldcar bestätigte gegenüber der Mallorca Zeitung: "Wir sind uns des Problems bewusst, das lediglich eine sehr kleine Zahl von Kunden auf Mallorca betroffen hat." Das Unternehmen stehe in Kontakt mit den Behörden und kooperiere mit den laufenden polizeilichen Ermittlungen. Weitere Details nannte Goldcar nicht, um den Fortgang der Untersuchungen nicht zu gefährden.

Gleichzeitig betonte der Autovermieter, dass keine internen Daten weitergegeben worden seien. Kunden, die bereits Zahlungen geleistet haben, hätten den Betrag von Goldcar vollständig zurückerstattet bekommen.

Vorsicht bei Bußgeldbescheiden aus dem Ausland

Der Vorfall zeigt, dass auch im Ausland erhaltene Bußgeldbescheide genau geprüft werden sollten. Grundsätzlich ist es nicht ungewöhnlich, nach einem Aufenthalt in einem EU-Land einen Strafzettel per Post zu erhalten. Seit 2013 können Verstöße wie zu schnelles Fahren oder Falschparken innerhalb der EU grenzüberschreitend geahndet werden.

Allerdings müssen bestimmte Kriterien erfüllt sein: Echtheit der Absenderadresse, klare Identifizierung des Verstoßes, einwandfreies Beweisfoto – und bei Bußgeldern aus Spanien üblicherweise ein Hinweis auf die Möglichkeit zur reduzierten Zahlung innerhalb von 20 Tagen.

Fazit

Die aktuellen Fälle auf Mallorca zeigen, wie professionell gefälschte Bußgeldbescheide mittlerweile gestaltet sein können. Urlauber sollten daher genau prüfen, ob das Schreiben echt ist – insbesondere dann, wenn Auffälligkeiten wie unklare Ortsangaben, fehlende Rabatthinweise oder schlechte Bildqualität vorliegen. Im Zweifel ist eine direkte Rücksprache mit der zuständigen Behörde – in diesem Fall der DGT – empfehlenswert.

Quelle:https://www.auto-motor-und-sport.de/verkehr/achtung-mallorca-urlauber-fake-knoellchen-fuer-mietwagen-kunden/?utm_source=newsletter&utm_campaign=daily-newsletter&utm_content=outro-inline

4) Aldi, Edeka & Co. – Preistricks bei Lebensmitteln: Wie günstig sind “Knüller-Preise” oder “Super-Spar-Angebote" wirklich?

Warum “reduzierte” Spar-Preise manchmal sogar teurer sind und was es mit "Beispiel-Preisen" auf sich hat.

Super-Knüller, Top-Angebot, Spar-Preis – was nach richtig **Geldsparen** klingt, dient häufig allein dem **Handel**. Nämlich dazu, uns in die Filialen zu locken. Ob wir dabei etwas **sparen**, ist oft **schwer ersichtlich** oder **fraglich**.

Der Beispiel-Preis

Er zählt zu den **neuesten Handelstricks**. Beispiel-Preise finden sich insbesondere auf Preisschildern an der **Fisch- oder Fleischtheke**, aber inzwischen auch in der **Obst- und Gemüseabteilung** . Angegeben wird ein – **vermeintlich günstiger – Preis**. Er ist allerdings kein Stückpreis, sondern bezieht sich – und das ist für viele Kunden und Kundinnen nicht klar ersichtlich – auf ein ganz **bestimmtes Beispiel-Gewicht der Ware.**

Entdeckt bei: Aldi Süd

Eine MARKTCHECK-Zuschauerin entdeckt den Beispiel-Preis bei Aldi Süd in der Gemüseabteilung: 88 Cent kostet ein **Fenchel** – allerdings nur dann, wenn er **exakt 260 Gramm** wiegt. Häufig sind die Knollen aber größer und können also auch mal das doppelte oder mehr kosten. In unserem Beispiel wiegt die Knolle 458 Gramm, kostet mit 1,55 Euro also **deutlich mehr als die 88 Cent**.

Der Haken

Nur die wenigsten Kundinnen und Kunden können das genaue Gewicht schätzen oder verwenden beim Einkauf einen Taschenrechner. **Beispiel-Preise bei Lebensmitteln** findet der Handelsexperte Andreas Kaapke von der Dualen Hochschule Baden-Württemberg ein Unding. Kaapke beschäftigt sich seit Jahren mit der Preisgestaltung von Händlern: „Der Kunde erwartet einen Kilo-, Hundert-Gramm-Preis oder einen Stückpreis. Nicht jeder ist ein Mathe-Genie und nicht jeder hat die Zeit und die Lust, irgendwas umzurechnen."

Beim alltäglichen Kauf von Lebensmitteln wollen wir **schnelle Entscheidungen treffen** können, so Kaapke, da seien Beispiel-Preise **nicht sinnvol**l.

Klage gegen Aldi Süd

Die **Verbraucherzentrale Baden-Württemberg** hat gegen diese Art der Preisauszeichnung von **Aldi geklagt**. Preise müssten klar erkennbar sein, sagt Sabine Holzäpfel von Verbraucherzentrale Baden-Württemberg: „Es gibt das Gebot der Preisklarheit und Wahrheit. Und deshalb ist es aus unserer Sicht nicht zulässig, wenn ich einen Beispiel-Preis habe, aber es auch Stücke gibt, die mehr wiegen, also ich am Ende mehr bezahle." Eine **gerichtliche Entscheidung steht** in der Sache **noch aus**.

Das sagt Aldi Süd dazu

Aldi Süd schreibt uns: „Bei ihrer genannten Abbildung handelt es sich um einen bedauerlichen Einzelfall." Und weiter: „Bei ALDI SÜD werden unverpackte Obst- und Gemüseartikel grundsätzlich mit Stück- oder Kilopreisen angeboten. Beispielpreise werden nur bei losen Artikeln eingesetzt, die in offenen Schalen angeboten werden - beispielsweise bei Sonnentomaten in einer offenen Schale mit einem ungefähren Packgewicht von 500g. Auch der Artikel Fenchel wird in allen Filialen mit einem Kilopreis ausgezeichnet."

Der Super-Knüller-Preis

Beispiel-Preise sind nicht der einzige Weg, wie Lebensmittelhändler ihre Kunden mit schön klingenden Preisangaben locken. Es gibt auch die **Knüller-Preise, Mega-XXL-Angebote, Super-Knüller, Super-Spar-Angebote, Tiefpreis-Highlights**...

Der Haken

Damit **verbänden** Kunden einen **reduzierten Preis**, sagt Handelsexperte Kaapke: "Aber es sind **keine geschützten Begriffe**. Man kann nicht einklagen, dass ein Begriff wie „Aktion" oder „Knüller" oder „Superspar" automatisch eine Reduktion von so und so viel Prozent hat."

Der Reduziert-Preis: "Um 15 %, 20 %, 30 % reduziert"

Wenn beim Preisabschlag eine **konkrete Prozentzahl** steht, gibt es seit knapp drei Jahren eigentlich eine gesetzliche Vorgabe: „Immer, wenn eine Preis-Reduzierung angegeben oder beworben wird, also zum Beispiel minus 30 Prozent, muss ich die Info bekommen: was hat das denn innerhalb der letzten 30 Tage gekostet? Das dient dazu, dass man diesen Preisvorteil tatsächlich einordnen kann", erläutert Verbraucherschützerin Holzäpfel.

Der Haken

Die Preis-Reduktion ist oft nicht wirklich ein Spar-Preis. Denn **Händler erhöhen manchmal für kurze Zeit die Preise**, um sie dann **optisch umso deutlicher senken** zu können.

Beispiel: Der Normalpreis einer Tafel Schokolade beträgt 1 Euro. Wenn der Händler sie im Angebot für 80 Cent verkauft, kann er also schreiben „-20%“. Erhöht der Händler den Preis aber für kurze Zeit auf 1 Euro 20 und reduziert dann auf 80 Cent, steht im Angebot „-33%“. Das **sieht dann wesentlich verlockender aus**.

Der niedrigste Gesamt-Preis

Edeka gibt in seinen Prospekten bei Sonderangeboten eine Prozentzahl an, daneben ein **Sternchen**: Ein Hinweis auf den Text, der sehr klein am **Rand des Prospekts** steht: Der **niedrigste Gesamtpreis der letzten 30 Tage**.

Der Haken

Die **Schrift** am Rand ist **winzig klein** – dass der “niedrigste Gesamtpreis der letzten 30 Tage” hier kommuniziert wird, ist **vielen nicht bekannt**. Verbraucherinnen und Verbraucher nehmen den klein gedruckten Text am Rand häufig gar nicht wahr.

Entdeckt bei: Edeka

Der Super-Knüller ist in unserem Beispiel **identisch** mit dem niedrigsten Preis der letzten 30 Tage. Die Preis-Ersparnis im Vergleich zu einem Preis aus den Vorwochen ist **also gleich 0**.

Weiteres Beispiel: MARKTCHECK entdeckt ein Lachsfilet-Angebot bei Edeka. Der “**Super-Knüller-Preis**”: 2 Euro 79 – und damit **teurer als der günstigste Preis der vergangenen 30 Tage**. Da waren es nämlich schon mal nur 2 Euro 49!

“**Dreiste Irreführung**”, findet das **Verbraucherschützerin** Holzäpfel. “Mit einem Preisvorteil zu werben, wenn ich im Kleingedruckten – wenn ich es lesen kann – erfahre, dass das innerhalb der letzten dreißig Tage **schonmal günstiger** war. Dieser angebliche **Knüllerpreis ist ja tatsächlich keiner**“, so Holzäpfel.

Das sagt Edeka dazu

Auf Nachfrage teilt **Edeka** mit: „Wie bei anderen Artikeln auch, variiert bei Fisch und Meeresfrüchten die am Markt verfügbare Menge, weshalb die Einkaufskonditionen sowie die Verkaufspreise permanenten Schwankungen unterliegen. Der damals niedrige Preis war damit begründet, dass dieser nur drei Tage (von Donnerstag bis Samstag) gültig war.“

Tipp: Der Fernsehbeitrag kann unter dem u.g Link abgerufen werden.

Quelle: https://www.swr.de/verbraucher/ard-marktcheck/preistricks-bei-lebensmitteln-reduzierte-preise-sparangebote-preisknueller-wirklich-guenstiger-100.html