35. Cybercrime Newsletter

30.05.2023

1) Dahinter stecken oft Betrüger – Verbraucherzentrale warnt vor Investment-Angeboten in sozialen Medien

In den sozialen Medien tummeln sich Betrüger, die das große Geld mit einfachen Investitionen versprechen. Doch die Verbraucherzentrale warnt.

Wenn jemand einem das schnelle Geld verspricht, sollte man immer vorsichtig sein. Denn solche Angebote sind meistens zu gut, um wahr zu sein. Die Verbraucherzentrale Nordrhein-Westfalen warnt aktuell vor sogenannten Trading-Gruppen in den sozialen Netzwerken.

Dabei sehen es Betrüger gezielt auf Personen ab, die finanziell unerfahren sind. Sie versprechen das große Geld innerhalb einer kurzen Zeit. Und das geht den "Anbietern" zufolge auch ganz einfach: Man schickt einem "Experten" eine kurze WhatsApp-Nachricht und wird in eine Gruppe eingeladen, in der Finanztipps gegeben werden.

Angeblich ist der finanzielle Aufwand bei den angebotenen Investitionen gering, diese haben aber eine sehr hohe Gewinnmarge. Beispiel: Die Betrüger versprechen, dass aus einem kleinen Beitrag von 250 Euro innerhalb von wenigen Monaten eine Viertelmillion wird. Dabei soll man sich entspannt zurücklehnen können, denn das Geld vervielfache sich von selbst.

Betroffene sehen ihr Geld meistens nie wieder

Und so funktioniert der Betrug: Wenn man angebissen hat, weisen die Kriminellen einen an, eine Investition auf einem Portal zu tätigen. Diese sehen meistens auch sehr professionell und authentisch aus – sie sind aber gefälscht. Die Kurse und Gewinne sind nur simuliert. Wer Geld auf die Fake-Portale einzahlt, sieht dieses meist nie wieder.

Das Problem: Viele Betroffene merken den Betrug erst, wenn sie sich ihr Geld auszahlen lassen wollen. Bis dahin kann es sein, dass sie schon viel Geld investiert haben. Und bei dem Versuch der Auszahlung kann es noch zu einem weiteren Betrugsversuch kommen.

Denn wie die Verbraucherzentrale erklärt, verlangen die Portale zur "Auszahlung" häufig Unterlagen wie Ausweiskopien, Kopien der Kreditkarte oder Meldebescheinigungen. Oft werden die eingereichten Unterlagen aber nicht anerkannt. Die Betrüger wollen der Verbraucherzentrale zufolge entweder Zeit gewinnen – oder gar Identitätsdiebstahl betreiben.

Was tun, wenn Betrüger mit Angeboten locken?

Wer – in welcher Art und Weise auch immer – von vermeintlichen Finanzexperten solche Angebote bekommt, sollte diese sofort abwehren. Die Verbraucherzentrale NRW warnt: "Auf keinen Fall sollte man sich drängen lassen, einen Vertrag möglichst schnell zu unterzeichnen". Im besten Falle sollte man die Polizei kontaktiert und den versuchten Betrug melden. Hat man bereits Geld überwiesen, sollte man sich an seine Bank wenden.

Allerdings bekommen die meisten Opfer solcher Betrüger ihr Geld nicht zurück. Oft sitzen die Kriminellen im außereuropäischen Ausland, was es schwierig macht, rechtliche Schritte einzuleiten.

Quelle: https://www.t-online.de/digital/aktuelles/id_100180516/betrug-in-sozialen-medien-verbraucherzentrale-warnt-vor-investment-angeboten.html

2) Warnung von Scotland Yard – Simple Betrugsmasche kann Sie Ihr Erspartes kosten

Betrug durch "Shoulder Surfing" – diese Masche ist einfach, aber effektiv. Jetzt kommt eine neue Warnung vom Londoner Scotland Yard.

Betrüger bedienen sich heutzutage oft ausgeklügelter Techniken und hacken sich über digitale Schwachstellen online zu ihrer Beute. Manchmal geschieht die Abzocke aber auch auf ganz einfache Art und Weise – und schmerzt umso mehr.

Das sogenannte Shoulder Surfing (Englisch für: jemandem über die Schulter schauen) ist so eine Masche. Nun warnt Scotland Yard in London vor dieser Form des Betruges.

"Es ist nur ein Telefon, aber wenn man die Sicherheitsmaßnahmen außer Acht lässt, läuft man im Grunde mit einer Tasche voller Bargeld herum", sagt John Roch, Leiter der Abteilung Wirtschaftskriminalität der Metropolitan Police in London, der BBC. Der Kriminalkommissar weiter: "Die möglichen Folgen des 'Shoulder Surfing' sind für die Opfer verheerend. Denn wenn es dem Kriminellen gelingt, das Smartphone zu erbeuten und sich Zugang zu den Banking-Apps zu verschaffen, kann das Ersparte ganz schnell weg sein."

So gehen die Betrüger beim "Shoulder Surfing" vor

Stellen Sie sich vor, Sie stehen in einer Warteschlange am Ticketschalter eines Bahnhofes oder in einer Bar am Tresen. Wenn Sie in dieser beengten Situation das Smartphone hervorziehen und Ihre PIN zum Entsperren über die Tastatur eingeben, kann das leicht von jemandem hinter Ihnen mit angesehen werden. Ist Ihr Telefon wenig später nicht mehr auffindbar, hat womöglich ein Betrüger die Hand im Spiel.

Jake Moore vom Cybersicherheitsunternehmen ESET erklärt: "Hat ein Betrüger gesehen, welche PIN benutzt wurde, holen sich Taschendiebe das Telefon. Eine andere Methode ist, Getränke in einem Pub mit K.o.-Tropfen zu versetzen und dem Opfer das Telefon einfach abzunehmen." Besonders leicht mache man es den Betrügern, wenn man die PIN zum Entsperren des Telefons auch für die Banking-Apps nutze, so Moore.

Ein großes Problem sind laut Scotland Yard zudem im Smartphone abgespeicherte Zugangscodes – selbst wenn diese versteckt abgelegt werden. "Betrüger wissen genau, wo sie suchen müssen", warnt Roch.

Dieser aktuelle Fall ist eine Warnung

Ein Opfer des "Shoulder Surfing" hat jetzt mit der BBC gesprochen. Jacopo de Simone wurde letztes Jahr in einem Pub das Telefon entwendet. Der große Schock kam, als er sich am nächsten Morgen in seine Banking-App einloggte und feststellte, dass sein gesamtes Geld (mehr als 22.000 Pfund, etwa 25.000 Euro) gestohlen worden war.

Nach einem zehnmonatigen Streit mit seiner Bank und dem Versuch, seine Unschuld zu beweisen, bekam er das Geld schließlich zurückerstattet. "Ich bin sehr vorsichtig mit der Benutzung des Smartphones geworden und habe keinerlei Banking-Apps mehr auf dem

Telefon", erzählte de Simone der BBC.

Keine Finanz-Apps auf dem Mobiltelefon – das ist auch einer der Ratschläge von Scotland Yard. Hier finden Sie eine Übersicht über weitere Sicherheitsmaßnahmen.

So schützen Sie sich

- Verwenden Sie nach Möglichkeit biometrische Daten (Face-ID oder Fingerabdruck) zur Identifizierung.
- Entfernen Sie Banking-Apps von Ihrem Telefon und benutzen Sie diese nur auf Geräten zu Hause.
- Verwenden Sie unterschiedliche PIN-Nummern zum Entsperren Ihres Telefons und Ihrer Banking-Apps.
- Speichern Sie keine Passwörter oder PINs auf Ihrem Telefon.
- Achten Sie immer auf Ihre Umgebung, wenn Sie auf Ihr Smartphone beziehungsweise Finanz-Apps auf Ihrem Telefon zugreifen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100179728/scotland-yard-warnt-vor-betrugsmasche-shoulder-surfing-.html

3) Whatsapp-Falle: Hacker locken mit Gratis-Bier – so erkennen Sie den Betrug

Passend zum Vatertag geht derzeit eine Whatsapp-Nachricht mit einem Gewinnspiel um, die 2000 Kühlschränke voll mit Gratis-Bier verspricht. Vorsicht: ein Betrug. Eine bekannte Brauerei warnt davor.

Morgen ist Vatertag. Traditionell ein Tag, an dem Bier – mitunter „verdünnt“ durch Hochprozentiges – eine besonders große Rolle spielt. Hacker nutzen das jetzt aus und verschicken Whatsapp-Nachrichten mit einem dazu passenden Gewinnspiel. Davor **warnt** das österreichische Sicherheitsportal Mimikama.at.

Der Betrug geht folgendermaßen: Die Hacker verschicken Whatsapp-Nachrichten, in denen von einer „Krombacher Vatertag 2023 Aktion“ die Rede ist. Die Whatsapp-Nachricht enthält ein Foto, das einen Krombacher-Getränke-Kühlschrank zeigt, randvoll mit dem leckeren Durstlöscher gefüllt. Darunter steht, dass es 2.000 Kühlschränke mit kostenlosem Bier zu gewinnen gäbe. Und darunter folgt ein Link (mit der Top-Level-Domain .ru für Russland), der angeblich zu dem Gewinnspiel führt.

Wer auf den Link klickt, kommt auf eine Seite, auf der es vier Fragen zu beantworten gibt. Gleich zum Start heißt es, dass nur noch 250 Geschenke übrig sind. Damit soll der Benutzer unter Druck gesetzt werden, sodass er sofort an dem Gewinnspiel teilnimmt, anstatt erst einmal in Ruhe zu überlegen.

Im Rahmen des Gewinnspiels muss man eben nicht nur die vier Fragen beantworten (wodurch die Betrüger einiges über die Teilnehmer erfahren und von diesen Daten erhalten), sondern soll das Gewinnspiel auch mit den eigenen Kontakten teilen. Damit wollen die Hacker erreichen, dass sich die Nachricht weiter verbreitet.

Mit den derart eingesammelten Daten können die Gangster dann Phishingattacken starten oder diese für Identitätsdiebstahl missbrauchen. Theoretisch ist auch denkbar, dass über solche Links Malware verbreitet wird. Ebenso ist es möglich, dass die Teilnehmer für das Gewinnspiel in eine Abo-Falle gelockt werden, wie Mimikama.at betont.

Krombacher warnt bereits vor diesem Gewinnspielbetrug auf Twitter:

> Aus aktuellem Anlass! pic.twitter.com/8Bml5JKyvt
>
> — Krombacher (@krombacher) May 16, 2023

Seien Sie grundsätzlich immer misstrauisch bei Gewinnspielen, die per Mail oder Whatsapp kommen. Gehen Sie auf die Webseiten der Unternehmen (nutzen Sie dafür die Google-Suche oder geben Sie die Webadresse des Unternehmens direkt in die Adresszeile des Browsers ein), die angeblich das Gewinnspiel durchführen und prüfen Sie, ob dort von dem Gewinnspiel die Rede ist.

Quelle: https://www.pcwelt.de/article/1919816/whatsapp-falle-krombacher-gratis-bier.html?utm_date=20230524120058&utm_campaign=Security&utm_content=Title%3A%20Whatsapp-Falle%3A%20Hacker%20locken%20mit%20Gratis-Bier%20%E2%80%93%20so%20erkennen%20Sie%20den%20Betrug&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Gehackt trotz 2-Faktor-Login: Wie man sich dagegen schützt

Im Podcast sprechen wir über 2FA, die Zweifaktor-Authentifizierung: Wie richtet man sie ein, wie funktionieren Phishing-Angriffe darauf, was bringt FIDO2.

Die sogenannte Zweifaktor-Authentifizierung gilt im Allgemeinen als sicher. Wir geben einen Überblick der wichtigsten Methoden: per SMS, per Hardware – vor allem FIDO2-kompatiblen USB-Sticks wie dem YubiKey – oder per TOTP. Letzteres sind diese sechsstelligen PINs, die eine spezielle App erzeugt, die sogenannten Einmalpasswörter (Time Based One Time Password). Google hatte dazu vorige Tage eine Änderung der Authenticator-App angekündigt, was wir kurz (als noch nicht gut genug) einsortieren.

Wie das SMS-Verfahren knackbar ist, ist schon länger bekannt – neuerdings aber lassen sich auch die TOTP-Logins abgreifen, und zwar mit einem aufwändigen Phishing-Verfahren, das wir erklären. Dagegen hilft vor allem die übliche Vorsicht beim Anklicken von Links in zwielichtigen Mails, die allerdings auch immer weniger zwielichtig aussehen. Noch besser schützen die FIDO2-Keys, da sie die URL mitcodieren und daher bei einer falschen URL gar kein Passwort liefern.

Heute im Studio: Pina Merkert (KI-Expertin), Lutz-Labs (SSDs) und Niklas Dierking (2-Faktor-Login), Moderation Jörg Wirtgen. Wir sprechen über SSDs mit SATA-Anschluss zum Nachrüsten für alte PCs und Notebooks – auf YouTube ab Freitag zu sehen. Danach erklären wir, wie 2-Faktor-Authentifizierungen gehackt werden können und warum sie trotzdem sinnvoll sind – auf YouTube ab Samstag zu sehen. Schließlich diskutieren wir, wie sich künstliche Intelligenz auf die Medien und auf einige Jobs auswirken könnte – auf YouTube ab Donnerstag. Auf den anderen Podcast-Kanälen erscheint die gesamte Folge am Samstag.

Anmerkung der Redaktion: Unter dem u.g Link kann ein Filmbeitrag zum o.g. Thema abgerufen werden.

Quelle: https://www.heise.de/news/Gehackt-trotz-2-Faktor-Login-Wie-man-sich-dagegen-schuetzt-c-t-uplink-48-2c-8970929.html

5) Gefahr für schlüssellose Fahrzeuge – Autodiebstahl: Hacker schließen Wagen mit Nokia 3310 kurz

Moderne Autos lassen sich schlüssellos öffnen und starten, etwa über das Smartphone. Das birgt Gefahren! Diebe können diese Wagen spielend knacken – ausgerechnet mit einem alten Nokia-Handy.

Es ist ungemein komfortabel: Sie näheren sich Ihrem Auto, es klackt – und der Wagen ist aufgeschlossen, ohne dass Sie den Schlüssel aus der Hosentasche fischen müssen. Einmal eingestiegen, geht es schlüssellos weiter. Ein einfacher Druck auf den Startknopf und der Motor läuft. Möglich machen diesen Luxus sogenannte Smart-Key-Systeme, die immer häufiger in modernen und eher hochpreisigen Autos zum Einsatz kommen. Nutzerinnen und Nutzer speichern dabei einen digitalen Schlüssel auf ihrem Smartphone oder haben einen entsprechenden Sender in der Tasche. Der kommuniziert mit dem Auto via Funk und entsperrt den Wagen, sobald Sie sich in der Nähe befinden. Dieses Prinzip hat allerdings auch eine Schattenseite.

Nicht nur für die Besitzerinnen und Besitzer der Autos ist das Öffnen der Türen und das Starten des Motors ein Kinderspiel, auch Diebe können die Fahrzeuge ohne viel Aufwand knacken. Das berichtet das Magazin Motherboard unter Berufung auf das Cybersecurity-Unternehmen Canis Automotive Labs. Demnach nutzen gut organisierte Autodiebe unter anderem modifizierte Uralt-Handys wie das Nokia 3310 oder auch harmlos anmutende Bluetooth-Lautsprecher, mit denen sie das System der Smart-Key-Fahrzeuge überlisten. Im Darknet wechseln entsprechend präparierte Geräte laut Bericht für Preise zwischen 3.500 und 18.000 Euro die Besitzer. Dabei kosten die Bauteile für ein manipuliertes Nokia 3310 nicht einmal 10 Euro und der Aufwand für den Umbau soll vergleichsweise gering sein.

Keine einfache Lösung in Sicht

Die Diebe verbinden das 2000 erschienene Handy über einen nachträglich eingebauten USB-Anschluss mit dem Bordsystem des Autos und schleusen darüber Entsperrbefehle ein. Das geht natürlich nur, wenn sie bereits im Fahrzeug sitzen. Ist der Wagen noch verschlossen, ist der Einsatz etwas aufwendiger. Dann müssen die Kriminellen zunächst einen Scheinwerfer ausbauen, um an die Fahrzeugelektronik zu kommen. Ist das geschehen, lässt sich das Nokia-Handy wiederum über das USB-Kabel mit zwei Kontakten am Fahrzeug verbinden und kann so die Türen entsperren. Die modifizierten Nokia-Handys und Bluetooth-Speaker gibt es im Darknet für diverse Automarken wie BMW, VW, Renault, Toyota und Maserati.

Besonders bitter: Einen sicheren und allgemeingültigen Schutz gegen diese Masche gibt es laut Canis Automotive Labs nicht. Die einzige Lösung sei eine kryptografische Verschlüsselung der Smart Keys. Die müssten die Autohersteller per Update vornehmen. Bislang zeigen die laut Bericht aber wenig Interesse an dem Thema. BMW etwa soll auf eine Anfrage von Motherboard gar nicht reagiert haben. Bei Toyota erklärte man immerhin, man wolle das Thema mit Experten für Diebstahlprävention und Strafverfolgungsbehörden weiter verfolgen. Wie ein Diebstahl mit einem Nokia 3310 ablaufen kann, zeigt ein kurzes YouTube-Video. https://www.youtube.com/watch?v=oeJumGZ56CY

Quelle: https://www.computerbild.de/artikel/cb-News-Sicherheit-Autodiebstahl-Hacker-schliessen-Wagen-Nokia-3310-kurz-35658787.html

6) Telefonbetrug: Hüte dich vor 015214434794

Aktuell häufen sich die Beschwerden über die unbekannte Telefonnummer 015214434794. Offenbar handelt es sich bei ihr um Betrugsversuch.

Kriminelle versuchen immer wieder auf verschiedenen Wegen, ihre Opfer hinters Licht zu führen und so an sensible Daten oder an Geld zu kommen. Eine der häufigsten Vorgehensweisen ist dabei der **Telefonbetrug**, bei dem Ahnungslose von unbekannten Nummern angerufen werden. Aktuell macht diese Masche wieder die Runde.

Telefonbetrug mit 015214434794 und der Kassenärztlichen Vereinigung

Solltest du dieser Tage von der Handynummer 015214434794 angerufen werden, lege direkt

wieder auf oder blockiere sie direkt. Es handelt sich eindeutig um Telefonbetrug. Bei verschiedenen Seiten wie zum Beispiel Wemgehoert.de sind in den letzten Tagen mehrere Reaktionen dazu erschienen.

So heißt es unter anderem, dass die Verantwortlichen dahinter mehrmals am Tag anrufen würden. In einigen Fällen würde sich dann nach dem Abheben aber niemand oder nur kurz melden und das Gespräch direkt wieder beenden.

Eine andere Person berichtet aber davon, dass sich jemand als Kassenärztliche Vereinigung ausgeben würde. Man könne ab dem 1. Juli den Zahnersatz zu 100 Prozent ersetzt bekommen und auch Implantate erhalten. Man solle einfach nur eine monatliche Gebühr zahlen. Auch bei Clever Dialer gibt es mehrere diesbezügliche Meldungen. Dort heißt es, dass das Angebot angeblich nur noch für einen Tag gültig wäre.

Das kannst du dagegen tun

In Wahrheit würde dich die Kassenärztliche Vereinigung ganz sicher nicht einfach so wegen eines Sonderangebotes anrufen. Zudem ist es nicht glaubwürdig, dass sich dort jemand nur mittels einer Handynummer bei dir meldet.

Damit du allerhöchstens nur ein einziges Mal Ziel eines Telefonbetrugs wirst, solltest du den Kontakt direkt sperren. Wir sagen dir, wie du Nummern bei Android und iPhone blockierst.

Quelle: https://www.futurezone.de/digital-life/article455895/telefonbetrug-huete-dich-vor-015214434794.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

7) Keine Lieferung – Heizöl: Fake-Shops nehmen zu

Immer häufiger fallen Heizölkunden auf Fake-Shops im Internet rein. Verbraucherschützer erklären, wie Sie sich davor schützen können.

Viele Verbraucher nutzen die günstigen Heizölpreise, um jetzt schon ihre Heizöltanks zu füllen. Die erhöhte Nachfrage nutzen Betrüger aus. So kommt es vermehrt vor, dass zahlreiche Heizöl-Kunden bei Fake-Shops Öl für viel Geld einkaufen, aber nie eine Lieferung erhalten. Aber auch während der Lieferung können die Kunden abgezockt werden.

Verbraucherschützer geben daher den Tipp, auf diese Warnzeichen zu achten:

Fake-Shop erkennen

Folgende Punkte können laut Verbraucherzentrale NRW e.V. auf einen betrügerischen Händler im Internet hindeuten:

- **Auffällige Internetadresse**
  Achten Sie vor allem auf die Endungen ".de" und ".com", sie deuten auf Seriosität hin.
- **Zahlungsweise**
  Es sollten mehrere Zahlungsmethoden zur Auswahl stehen. Vermeiden Sie in jedem Fall Vorkasse. Nutzen Sie kundenfreundliche Zahlungsmethoden, bei denen Sie auch eine Absicherung erhalten.
- **Preise**
  Der Preis sollte nicht zu günstig sein. Zudem sollten die zusätzlichen Kosten nicht zu hoch sein.
- **Gütesiegel**
  Kontrollieren Sie, ob die Gütesiegel verifiziert und echt sind. Teilweise klappt das mit einem Klick auf das Gütesiegel. Sie sollten dann zur entsprechenden Seite weitergeleitet werden.

- **Kundenbewertungen**
  Suchen Sie nach weiteren Kundenmeinungen zu dem Onlinehändler.
- **AGB**
  Lesen Sie sich die AGB durch.

Zusätzlich sollten Sie vor dem Heizölkauf auf der Internetseite der Verbraucherzentrale suchen, ob Sie den Onlineshop in der Liste der Fake-Shops finden.

Betrug bei der Heizöllieferung

Doch auch, wenn die Lieferung kommt, ist der Kunde nicht vor Betrug geschützt. Denn einige Lieferdienste haben die Tankwagen manipuliert. So kann es vorkommen, dass laut Anzeige am Lieferwagen mehr Heizöl oder Diesel geliefert wurde, als eigentlich geflossen ist. Auslöser kann einerseits die Zumischung von Luft sein, so der Bund der Energieverbraucher e. V., oder eine manipulierte Tankanzeige.

Schützen Sie sich vor der Betrugsmasche, indem Sie

- sich vor der Öllieferung einen Betankungswächter oder/und eine digitale Füllstandsanzeige einbauen lassen;
- während des Tankvorgangs vor Ort sind und bleiben;
- den Tankvorgang genau protokollieren (Datum, Uhrzeit, Dauer des Tankvorgangs, Menge des Restöls im Lieferfahrzeug, Name des Fahrers, Kfz-Nummer des Wagens);
- die Prüfplakette vom Eichamt auf dem Tankwagen kontrollieren;
- das Zählerwerk im Blick behalten.

Stellen Sie Unklarheiten während oder unmittelbar nach der Bestellung fest, sollten Sie diese umgehend reklamieren, solange der Öltankwagen noch vor Ort ist. Vergleichen Sie die Werte Ihres Betankungswächters mit denen der Öltankanzeige am Lieferfahrzeug. Diese Zahlen müssen darüber hinaus mit den Angaben auf dem Lieferschein übereinstimmen. Rufen Sie notfalls die Polizei zu Hilfe.

Tipp:

- Die besten Alternativen: Werden Sie unabhängig von Gas und Öl
- Schwankender Preis: So sparen Sie beim Heizölkauf bares Geld
- Durchschnittswerte deutscher Haushalte: Darauf sollten Sie bei Ihrer Ölheizung achten

Quelle: https://www.t-online.de/heim-garten/aktuelles/id_100175298/heizoel-aus-dem-internet-so-schuetzen-sie-sich-vor-fake-shops-und-betruegern.html

8) Aktuelle Betrugsmaschen: Angebliche Kontosperrung bei Amazon

Sie gehen mit großer Raffinesse vor: Betrüger und Betrügerinnen, die ihre Opfer am Telefon, im Netz oder an der Haustür um ihr Geld bringen. Letztlich sind es aber immer ähnliche Tricks, nur in unterschiedlichen Varianten. Um gewarnt zu sein, sollte jeder von den folgenden Betrugsmaschen gehört haben.

Phishing bei Amazon: Vorsicht bei angeblicher Kontosperrung

Update vom 25. Mai: Amazon-Kunden erhalten derzeit vermehrt Phishing-Mails, in denen Betrüger vorgeben, das Konto sei wegen verdächtiger Aktivitäten gesperrt worden. Davor warnt aktuell die Verbraucherzentrale.

- Der Betreff einer solchen E-Mail sieht folgendermaßen aus: "Case -Informationen zu

Aktivitätszugriffen - Kontoauszugsstatus [Alert] - Es gibt einige verdächtige Aktivitäten. Ihr Konto wurde daher aus Sicherheitsgründen gesperrt. Bitte aktualisieren Sie Ihr Konto innerhalb von 24 Stunden."

Dazu erhalten Amazon-Kunden einen Link, den sie anklicken sollen, um das eigene Konto zu verifizieren und eine Kontosperrung zu vermeiden. Den Nutzern wird gedroht, dass die getätigte Bestellung sonst storniert und der Kontozugriff verwehrt werde.

Auffallend und besonders raffiniert: Die Adressaten der E-Mail werden mit Namen und Nennung der Mail-Adresse angesprochen, die für das Konto verwendet wird. Das verstärkt den Eindruck, die Mail stamme wirklich von Amazon. Die Verbraucherzentrale rät, auf keinen Fall dem Link zu folgen, sondern die E-Mail unbeantwortet in den Spam-Ordner zu verschieben.

Behörde warnt vor betrügerischer Zollgebühren-SMS

Update vom 22. Mai: Die Anzahl von betrügerischen SMS, in denen Verbraucher zur Zahlung von angeblichen Zollgebühren aufgefordert werden, hat stark zugenommen. Im Januar seien 65 Beschwerden zu dem Thema eingegangen, im Februar 91, im März 331 und im April 2.075, teilte die Bundesnetzagentur der Deutschen Presseagentur (dpa) mit.

Die Masche trat Mitte 2022 auf, danach meldeten sich immer mehr Bürger bei der Behörde. In den SMS wird ein Paket angekündigt, das im Zoll festhänge. Erst wenn Zollgebühren entrichtet werden, werde die Sendung weitergeschickt, heißt es in den Betrugs-SMS, in denen auch ein Link ist. Klickt man den an, wird man auf einer Webseite zur Angabe persönlicher Daten aufgefordert.

Die Behörde warnt davor, die Webseiten zu öffnen und Daten preiszugeben. Denn tatsächlich handelt es sich um kein echtes Paket, sondern um Datenphishing - also das illegale Abgreifen von Daten, etwa von Kreditkarteninfos.

Die Bundesnetzagentur hat deswegen bereits mehr als 200 Mobilfunknummern abschalten lassen, die für die Masche genutzt worden waren. Allerdings setzen die Kriminellen inzwischen verstärkt ausländische Rufnummern ein, die von der Bundesnetzagentur nicht gekappt werden können. Ein Sprecher der Deutschen Post DHL wies darauf hin, dass der Bonner Konzern nie per SMS nach persönlichen Daten frage oder zu Zahlungen auffordere.

Vorsicht bei der Urlaubsplanung: Fallen Sie nicht auf unseriöse Buchungsplattformen rein

Update vom 16. Mai: Die Buchung von Hotelzimmern oder anderen Unterkünften für die Ferien wird Urlaubern und Urlauberinnen über Buchungsplattformen erleichtert. Manchmal verstecken sich dahinter jedoch unseriöse Angebote. Wie die Verbraucherschutzbehörde "Watchlist Internet" warnt, melden sich vermehrt Unterkünfte, die keine Verträge mit manchen dieser Plattformen haben - sodass auch kein Zimmer gebucht werden kann.

Es kann also passieren, dass Sie ein Zimmer über eine unseriöse Plattform gebucht und bezahlt haben, vor Ort in dem Hotel oder Ferienwohnung jedoch niemand etwas davon weiß. Normalerweise wird die Kredit- oder Debitkarte bei einer Reservierung über die Seiten erst belastet, wenn Sie in dem Hotel ein- bzw. auschecken. In betrügerischen Fällen wird sie aber bereits bei der Reservierung belastet.

Vor dem Buchen sollten Sie die Plattform unbedingt prüfen:

- Lesen Sie Bewertungen und Erfahrungsberichte, diese können Sie einfach ergoogeln.
- Achten Sie auf die Preise. Wenn diese deutlich günstiger sind als bei anderen Anbietern, ist Vorsicht geboten.
- Testen Sie die Seitenfunktion. Klicken Sie möglichst viele Links an, wenn viele davon

nicht funktionieren, kann das ein Indiz sein.
- Checken Sie die Zahlungsmöglichkeiten. Manchmal ist angeblich sowohl eine Kreditkarten- als auch eine Paypal-Zahlung möglich. Bei der Buchung geht dann nur noch eine Kreditkartenzahlung. Derartige Widersprüche sind unseriös.
- Prüfen Sie das Impressum. Deutsche Unternehmen können Sie im Handelsregister überprüfen, österreichische bei der WKO. Bedenken Sie, dass die Durchsetzung Ihrer Rechte bei Nicht-EU-Unternehmen deutlich schwieriger ist.

Das können Sie tun, wenn Sie bereits über eine unseriöse Plattform gebucht haben:

- Kontaktieren Sie die gebuchte Unterkunft und fragen Sie nach, ob Ihre Buchung angekommen ist.
- Sollte die Unterkunft keine Buchung von Ihnen haben, kontaktieren Sie Ihr Kreditkarteninstitut und lassen Sie Ihre Karte sperren.
- Sollte bereits Geld abgebucht worden sein, fordern Sie eine Rückbuchung von Ihrem Kreditkartenunternehmen. Beträge, die ohne Ihre Zustimmung abgebucht wurden, müssen gemäß § 67 Zahlungsdienstleistungsgesetz 2018 von Ihrem Zahlungsdienstleister zurückerstattet werden.

Namensänderung bei Ebay-Kleinanzeigen: Vorsicht vor Betrugsmaschen

Update vom 2. Mai: Da ein norwegisches Unternehmen das Portal gekauft hat, heißt Ebay-Kleinanzeigen ab 16. Mai nur noch Kleinanzeigen. Diese Änderung bei dem Second-Hand-Portal könnte Betrügerinnen und Betrüger auf den Plan rufen, warnt nun mimikama, ein Verein, der sich mit Internetmissbrauch beschäftigt. Es sei gut möglich, dass Betrüger nun mit Phishing-SMS und -Emails versuchen, an Telefonnummern, Emails oder Kontodaten von Käuferinnen und Käufern zu gelangen oder versuchen, sie zu Registrationen und Überweisungen zu bewegen. Gerade in diesen Wochen ist besondere Vorsicht geboten.

Was jetzt wichtig ist, wenn Sie ein Konto bei Ebay-Kleinanzeigen haben:

- Zwar ändern sich Name und Farbgestaltung der Website, Passwörter, bestehende Nutzerkonten und Zahlungsmöglichkeiten bleiben aber gleich.
- Es ist außerdem nicht nötig, die App für Android oder IOS neu zu installieren.
- Wenn Sie etwa per Mail oder SMS dazu aufgefordert werden, im Zuge der Namensänderung Daten einzugeben, handelt es sich mit großer Wahrscheinlichkeit um eine Betrugsmasche. Reagieren Sie auf keinen Fall darauf und verschieben Sie die Mail ungelesen in den Papierkorb.

Phishing bei Netflix-Kunden

Update vom 27. April: Die Verbraucherzentrale warnt derzeit nahezu täglich vor Phishing-Versuchen, mit denen Betrüger im Namen von großen bekannten Banken Daten klauen. Aktuell kursieren laut den Verbraucherschützern auch vermehrt E-Mails, die angeblich von Netflix stammen sollen. Besonders auffällig bei dieser E-Mail seien Filmempfehlungen unterhalb des Textes, die den Eindruck verstärken, es handele sich wirklich um Post von Netflix. In Wahrheit stecken Betrüger dahinter.

Unter dem Betreff "Aktualisieren Sie Ihre Informationen" werden den Kunden Probleme bei der Rechnungsstellung vorgegaukelt. Wegen einer "technischen Störung" solle man über einen Button die eigenen Daten aktualisieren. Ansonsten könne man die Netflix-Dienste nicht mehr nutzen. Der Link führt wiederum auf eine Seite, die täuschend echt nach dem Streaming-Dienst aussieht.

Vorsicht! Geben Sie Ihre Daten auf keinen Fall ein, sondern verschieben Sie die E-Mail unbeantwortet in den Spam-Ordner.

Fake-Shop-Warnung: Autoreifen-Betrug weitet sich massiv aus

Update vom 25. April: Cyberkriminelle haben längst auch den Autozubehör-Markt für sich entdeckt. Insbesondere Reifen-Fake-Shops verbreiten sich zunehmend. Die Seiten machen einen guten Eindruck, alles sieht seriös aus und der Preis scheint unschlagbar.

Wer auf so einen Shop hereinfällt, merkt sehr schnell, wie solche Traumpreise möglich sind: durch Betrug. Wer in Fake-Shops bezahlt, bekommt niemals Ware geliefert und verliert sein Geld, warnt das Verbraucherschutzportal "Watchlist Internet". Die Experten pflegen dort eine Fake-Shop-Warnliste, die auch Dutzende falsche Reifenhändler im Netz enthält.

Daran erkennen Sie die Fake-Shops:

- Neben einem Preis, der zu gut ist, um wahr zu sein, ist Vorkasse als einzige verfügbare Zahlungsoption ein ziemlich sicheres Indiz für einen Fake-Shop. Oft werden anfangs noch verschiedene Zahlungswege angeboten. Das ist aber nur Schein. An der Kasse ist dann etwa überraschend von technischen Problemen die Rede, und es bleibt nur die riskante Überweisung, die kaum zurückgeholt werden kann.
- Bei unbekannten Shops lohnt es sich auch immer, das Impressum zu prüfen, etwa mit einem Anruf oder einer E-Mail-Anfrage. Denn bei Betrugs-Websites ist meist niemand zu erreichen oder es kommt nie eine Antwort.
- Zudem kann man die Adresse oder den Shop-Namen in eine Suchmaschine und bei einem Kartendienst eingeben. Oft wird dann schnell klar: Hier residiert ein ganz anderes Unternehmen oder es handelt sich um ein Wohnhaus. Oder man stößt direkt auf Warnungen von Betrugsopfern.

Das können Sie tun, wenn Sie Opfer geworden sind:

Wer auf einen Fake-Shop hereingefallen ist und vorab überwiesen hat, sollte nicht nur Anzeige bei der Polizei erstatten, sondern auf jeden Fall seine Bank kontaktieren, raten die Experten. Möglicherweise könne das Geld noch zurückgeholt werden. Wurde ein Bezahldienst oder eine Kreditkarte benutzt, aber nie Ware geliefert, kann man sich an den jeweiligen Bezahl-Dienstleister wenden.

Phishing-Alarm: Diese E-Mail stammt nicht vom Finanzministerium

Update vom 24. April: Momentan sind Phishing-Mails in Umlauf, die angeblich vom Finanzministerium stammen. In der Mail ist von einem 750 Milliarden Euro umfassenden Maßnahmenpaket namens "NextGenerationEU" die Rede. Man könne Geld in einen "digitalen Euro" umwandeln und erhalte dabei eine Förderung in Höhe von 29 Prozent der getätigten Einlage.

Hinter der Mail stecken Betrüger, die raffiniert zu Werke gehen: Denn tatsächlich gibt es das Wiederaufbauprogramm der EU - die in der Phishing-Mail beschriebenen Funktionen allerdings nicht.

Rechtschreibfehler in der Internetadresse

In der Phishing-Mail ist ein Link enthalten, der zum angeblichen "Pilotprogramm" führt, außerdem gibt es einen "persönlichen Zugangsschlüssel". Über den Link gelangt man auf eine Website, die so aussieht, als sei sie vom Finanzministerium. Ein Blick auf die URL zeigt allerdings, dass es sich um Betrug handelt: In der Internetadresse "bundesminsiterium-der-finanzen.com" ist ein Rechtschreibfehler.

Das Landeskriminalamt Niedersachsen geht davon aus, dass sich die Kriminellen später telefonisch oder per Mail bei den Interessentinnen und Interessenten melden, um an sensible Daten zu gelangen. Die Verbraucherzentrale NRW empfiehlt, die E-Mail nicht zu öffnen und

den Link nicht anzuklicken.

Täuschend echt: Kriminelle bringen Anleger mit guten Zinsangeboten um ihr Geld

Update vom 20. April: Festgeldangebote gelten als eine sichere Anlageform, momentan gibt es bei vielen Banken auch wieder gute Zinsangebote. Doch wenn es um gute Zinsangebote von Webportalen und Beratungsfirmen geht, ist höchste Vorsicht geboten. Die Verbraucherzentrale warnt vor Betrügern, die sich als Finanzexperten ausgeben und Festgeldangebote auf Webportalen oder über Beratungsfirmen vermitteln. Dabei gehen die Kriminellen so vor:

- Wer das Angebot wahrnehmen möchte, erhält ein Antragsformular einer Partnerbank, zu der man auch weitergeleitet wird.
- Hier erscheint ein gefälschter Eröffnungsantrag für ein neues Konto.
- Nun soll man den gewünschten Betrag auf dieses Konto mit ausländischer IBAN überweisen. Dieses Konto existiert wirklich, tatsächlich handelt es sich hierbei aber um eine Kontoverbindung der Kriminellen. Das überwiesene Geld sehen Anlegerinnen und Anleger nicht wieder.
- In manchen Fällen gibt es nach der Transaktion einen angeblichen Kontoauszug, meist melden sich die Betrüger aber nicht mehr oder schieben bei Nachfragen Ausreden vor.

Besonders perfide am Vorgehen der Kriminellen ist, dass es nicht leicht als Betrug zu erkennen ist: Nicht nur die Fake-Webportale sehen täuschend echt aus, auch die Zinsangebote sind gut, aber nicht unrealistisch hoch. Die Verbraucherzentrale gibt deshalb mehrere Tipps, wie man unseriöse Finanzberatungsangebote erkennen kann:

- Checken Sie in der BaFin-Unternehmensliste, ob die Vermittler hier auftauchen und somit für Finanzdienstleistungen in Deutschland zugelassen sind.
- Stutzig sollten Sie bei einem unvollständigen Impressum oder einer Geschäftsadresse im Ausland werden.
- Bei einer Kontoeröffnung gibt es normalerweise Legitimationsverfahren mit Identitätsnachweis. Findet das nicht statt, ist es ein klares Warnzeichen.
- Lassen Sie sich hingegen nicht von Siegeln und Auszeichnungen blenden: Betrügerische Webseiten wirken in vielen Fällen sehr professionell.
- Orientieren an Aufmachung und Zinssätzen seriöser Angebote, dabei kann etwa die Stiftung Warentest einen Überblick geben.
- Wenden Sie sich im Zweifelsfall an die Verbraucherzentrale oder holen Sie einen rechtlichen Rat ein.

Amazon-Konto angeblich gesperrt

Update vom 18. April: Wieder ist eine E-Mail im Umlauf, die angeblich von Amazon stammen soll. Tatsächlich handelt es sich erneut um eine Betrugsmasche, genauer gesagt um eine Phishing-Mail. Das meldet aktuell die Verbraucherzentrale.

- **Der Betreff:** "[Sicherheitswarnung] Ihr Konto wurde aufgrund einer nicht autorisierten Anmeldeaktivität gesperrt! - Aktion erforderlich".

"Unser Service hat ihr Konto vor jemandem geschützt, der auf Ihr Konto zugegriffen hat", heißt es dann in der E-Mail. Der User wird aufgefordert, seine Kontodaten über einen Link einzugeben. Ansonsten werde das Konto innerhalb von 48 Stunden nach Erhalt der Mail gelöscht. Die Folge, wenn User hier tatsächlich ihre Daten eingeben: Die Betrüger kennen diese nun und können sich problemlos in Konten ihrer Opfer einloggen.

Erst wenige Wochen zuvor hatten die Verbraucherschützer über eine betrügerische E-Mail im Namen von Amazon gewarnt. Der Inhalt der E-Mail wich nur leicht ab: Kunden wurden

aufgerufen, ihre Daten innerhalb von 24 Stunden zu aktualisieren. Sonst drohe die Sperrung des Kontos. Auch hier handelt es sich um Phishing. "Die Kriminellen versuchen Sie so unter Druck zu setzten und zu unüberlegtem Handeln zu bringen. Sie sollten die Aufforderung ignorieren und Phishing-Mails immer unbeantwortet in den Spam-Ordner verschieben", warnt die Verbraucherzentrale.

Diese Mail von Disney+ ist nicht echt!

Update vom 15. April: Wie die Verbraucherzentrale warnt, sind derzeit wieder Nutzerinnen und Nutzer von Disney+ im Fokus von Betrügerinnen und Betrügern. Vorsicht ist bei Emails geboten, in denen Sie dazu aufgerufen werden, Ihre Daten über einen Link einzugeben. Der Grund: Angeblich gebe es Probleme mit der Zahlungsmethode und Ihr Monatsabo könne daher nicht verlängert werden. Hierbei handelt es sich um eine Phishing-Mail, die Sie am besten ungeöffnet in den Papierkorb schieben.

Betrug mit QR-Code: Bei dieser Email handelt es sich um "Quishing"

Update vom 6. April: Die Verbraucherzentrale warnt, dass gerade viele Postbank-Kunden Phishing-Emails erhalten, in denen sie auf ungewöhnliche Aktivitäten in ihren Konten hingewiesen werden. Diese angeblich ausgeführten Aktivitäten werden in der Nachricht im Detail aufgelistet. Wenn man sie selbst nicht ausgeführt hat, so heißt es weiter, soll man einen in der Mail abgebildeten QR-Code mit dem Smartphone einscannen. Auf diese Weise bleibe das Konto weiter nutzbar.

Wer den Code scannt, landet auf einer Seite, auf der man Daten eingeben soll. Achtung: Hierbei handelt es sich um "Quishing" (Wortkombination aus "QR-Code" und "Phishing") - eine relativ neue Betrugsmethode mit falschem QR-Code. Mit diesem QR-Code versuchen Betrüger, an sensible Daten zu kommen. Die Verbraucherzentrale empfiehlt, die Email ungeöffnet in den Spam-Ordner zu schieben.

Woran Sie "Quishing" erkennen:

- Die E-Mails unterscheiden sich kaum von Phishing-Mails – der Aufbau und die Absicht gleich.
- In der Betreffzeile wird in der Regel auf ein Sicherheitsproblem hingewiesen. Manchmal heißt es auch, der Nutzer benötige ein Dokument, an das sie durch das Einscannen des QR-Codes auf ihrem Smartphone gelangen könnten - auf jeden Fall wird dazu aufgefordert, den QR-Code einzuscannen.

Die Cyberkriminellen können mit den erbeuteten Zugangsdaten etwa Einkäufe im Internet tätigen oder Zugang zu geschützten Firmennetzwerken erlangen.

Vier praktische Tipps gegen "Quishing":

- Mails sorgfältig prüfen, keine verdächtigen Anhänge oder Links öffnen, keine QR-Codes einscannen.
- Handelt es sich wirklich um den angeblichen Absender? Prüfen Sie dies über offizielle Kanäle und nehmen Sie im Zweifel Kontakt auf.
- Multi-Faktor-Authentifizierung nutzen: Selbst wenn Ihre Daten Kriminellen in die Hände fallen, fehlt ihnen der zweite oder dritte Faktor zum erfolgreichen Einloggen unter Ihrem Namen.
- Für Unternehmen gilt: Deren Sicherheitsrichtlinie sollte zwingend auch Smartphones einschließen. Oftmals existieren für Computer strenge Sicherheitsvorkehrungen, aber nicht für Firmenhandys. Zudem müssten Mitarbeitende unbedingt laufend über entsprechende Gefahren informiert werden.

Facebook-Betrug: Verschicken Sie niemals eine Kopie Ihres Ausweises

Update vom 6. März: Seien Sie vorsichtig bei Verkaufsangeboten jeder Art auf Facebook: Bei den Profilen der Anbieter kann es sich um Fake-Profile handeln, hinter denen Betrüger stecken. Typisch ist, dass sie im Zuge der Verhandlungen Ausweiskopien an ihre Opfer schicken und im Gegenzug ebenso eingescannte Ausweise verlangen. Höchste Vorsicht!

Bei den geschickten Ausweisen handelt es sich um gestohlene Kopien von Ausweisen Dritter - genau hierfür missbrauchen die Betrüger auch wiederum Ihren Ausweis. Die Folge kann etwa sein, dass Opfer an Ihrer Haustür klingeln und von Ihnen Ware abholen möchten, für die sie den Betrügern bereits Geld gezahlt haben.

Das Portal "Watchlist Internet" schildert diese Masche aktuell am Beispiel von Konzertkarten. Die Bereitschaft vieler Fans, hohe Preise für rare Karten zu bezahlen, ruft die Kriminellen hier verstärkt auf den Plan. Die Betrüger seien mit ihren Fake-Profilen überall, wo man bei Facebook nach Karten suchen würde: im Diskussionsforum der Veranstaltung, bei den Kommentaren darunter, auf dem Marketplace oder auch in speziellen Gruppen für Konzertkarten.

Um Vertrauen zu stiften, senden die Betrüger dann häufig die - gestohlene - Ausweiskopie. Im Gegenzug fordern sie ebenfalls eine Ausweiskopie. Hier gilt: Niemals eine Kopie des eigenen Ausweises schicken! Diese wird von Kriminellen für die nächsten Betrügereien missbraucht. Teils wird laut "Watchlist Internet" auch nur der halbe Ticketpreis verlangt plus die Ausweiskopie als Sicherheit. Hier gilt: Niemals Geld überweisen oder mit der PayPal-Funktion "Geld an Freunde & Familie senden" zahlen. In beiden Fällen ist das Geld weg, wenn sich der Verkäufer als Betrüger entpuppt.

Wie geht es besser? Am sichersten seien eine persönliche Übergabe und Bezahlung, raten die Verbraucherschützer. Geht das nicht, sollte man sich das Facebook-Profil des Verkäufers ganz genau anschauen und etwa über die PayPal-Funktion "Geld senden für Waren und Dienstleistungen" bezahlen, weil hier bei Problemen ein Käuferschutz greift.

Und auch dem Ticket selbst sollte man Beachtung schenken: E-Tickets, die selbst ausgedruckt werden, kauft man von Dritten am besten gar nicht. Hier besteht die Gefahr, dass sie mehrfach ausgedruckt worden sind.

Quelle: https://web.de/magazine/ratgeber/finanzen-verbraucher/aktuelle-betrugsmaschen-angebliche-kontosperrung-amazon-34288658

9) SMS-Angriff auf O2-Kunden – so reagieren Sie richtig

Derzeit schicken Betrüger wieder verstärkt SMS-Nachrichten im Namen von O2 an Handybesitzer. Die SMS haben das Ziel, die Nutzer in eine Falle zu locken. Darum geht es und so schützen Sie sich.

In den letzten Stunden haben wir die folgende SMS gleich doppelt erhalten, die angeblich vom Mobilfunkbetreiber O2 stammt. Der Wortlaut: “O2 INFO: Für Ihren Anschluss wurde eine E-SIM bestellt. Wenn es nicht um Sie geht, gehen Sie bitte zu O2esimcancel.com”.

Sie ahnen es: Die SMS stammt natürlich nicht von O2 und sollten Sie einen O2-Anschluss besitzen und diese SMS ebenfalls erhalten haben, dann ist das nur Zufall. Ihre Rufnummer und damit die Kontaktdaten sind also nicht zwingend in die falschen Hände geraten. Die Betrüger versenden die SMS nämlich wahllos an unzählige Rufnummern. Die dabei verwendeten Absender-Rufnummern sind natürlich auch gefälscht. Ebenso kann auch die Website variieren, die die Empfänger aufrufen sollen, um die angebliche E-SIM-Bestellung zu stornieren.

Das steckt hinter der Masche und so schützen Sie sich und andere Handybesitzer

Ein Blick ins Internet zeigt, dass die Masche nicht neu ist und in den vergangenen Stunden und Tagen vermehrt eine massive Anzahl neuer Betrugsversuche registriert werden. Einige Meldungen besorgter O2-Kunden finden sich hier im O2-Community-Forum.

Das Ziel der Betrüger ist es, die Empfänger zunächst in Sorge zu versetzen und sie dann dazu zu bringen, die in der SMS angegebene URL aufzurufen. Über diese Seiten wollen die Betrüger dann an die O2-Zugangsdaten der Nutzer gelangen. Zusätzlich besteht auch die Gefahr, dass mit dem Aufruf der Seite Schadsoftware auf das mobile Gerät gelangt.

Wer auf die Masche hereingefallen ist, sollte sofort sein Passwort auf “Mein O2” ändern. Es empfiehlt sich ebenfalls, das Smartphone auf Schadsoftware hin zu überprüfen, wobei etwa diese Apps helfen.

Im oben erwähnten O2-Community-Forum gibt ein O2-Moderator übrigens noch folgenden Tipp, woran man echte O2-Websites erkennt:

“Die einzigen von uns genutzten Adressen enden entweder auf -o2.de oder auf .o2online.de, SMS, die versuchen, euch zu einem Besuch anderer Seiten zu bewegen sind sehr wahrscheinlich immer Phishing-Versuche, um an eure Daten heran zu kommen. Hier eine gesunde Skepsis an den Tag zu legen und nicht drauf zu klicken ist absolut richtig und wichtig.“

Unsere Empfehlung lautet: Klicken Sie auf keinen Fall den in der SMS angegebenen Link an. Am besten löschen Sie die SMS sofort.

Alternativ können Sie die SMS als Spam bei Google melden und die Rufnummer dauerhaft blockieren. Dazu tippen Sie auf die SMS und wählen dann “Blockieren” aus. Im folgenden Fenster wählen Sie “Spam melden” aus. Dies sorgt dafür, dass sowohl der Inhalt der SMS als auch die Rufnummer bei Google und/oder dem Mobilfunkanbieter als Spam gemeldet werden. Dadurch können andere Handybesitzer schneller beim Empfang dieser oder einer ähnlichen SMS davor gewarnt werden, dass es sich um eine Betrugs-SMS handelt. Abschließend wird dann die SMS in den Bereich “Spam” in der Messages-App von Android verschoben.

Quelle: https://www.pcwelt.de/article/1930629/sms-angriff-auf-o2-kunden.html?utm_date=20230525144637&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20SMS-Angriff%20auf%20O2-Kunden%20%E2%80%93%20so%20reagieren%20Sie%20richtig&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

10) Warnung an o2-Kunden: Etliche Nutzer berichten über neue Betrugswelle

Neue Gefahr für o2-Kunden: Aktuell mehren sich Berichte über eine perfide neue Betrugsmasche, mit der Kriminelle Ihre Daten abgreifen wollen.

Neue Gefahr für o2-Kunden: Wie "PC-Welt" entdeckt hat, kursieren aktuell vermehrt SMS, in denen der Nutzer darüber informiert wird, dass er angeblich eine E-SIM bestellt hätte. In den Nachrichten ist auch ein Link hinterlegt, über den der Nutzer die angebliche Bestellung stornieren sollen kann.

Hierbei handelt es sich allerdings nicht um eine offizielle Benachrichtigung von o2, sondern um einen Betrugsversuch. Der hinterlegte Link führt nicht auf den offiziellen Webauftritt des Providers, sondern auf einen nachgebauten Fake. Werden hier die Daten des o2-Kontos eingetragen, landen diese direkt in den Händen der Kriminellen. Auch die Installation von

Malware über die Links ist nicht auszuschließen.

Betrüger nehmen o2-Kunden ins Visier: So reagieren Sie richtig

Ein Blick in das Community-Forum von o2 zeigt, dass die Masche aktuell weit verbreitet ist und viele Kunden die SMS ebenfalls erhalten haben, zum Teil sogar mehrfach.
Haben Sie eine derartige Nachricht erhalten, sollten Sie auf keinen Fall den hinterlegten Link anklicken und Ihre Daten angeben. Bevor Sie die Nachricht unbeantwortet löschen, sollten Sie einen Screenshot machen und Anzeige bei der Polizei erstatten.

Haben Sie Ihre Daten bereits hinterlegt, sollten Sie möglichst bald Ihr Passwort auf "Mein o2" ändern. Auch ein Check des Smartphones auf Schadsoftware ist in diesem Fall empfehlenswert. Das geht beispielsweise mit der Software von Malwarebytes.

Quelle: https://www.chip.de/news/Gefahr-fuer-o2-Nutzer-Betrueger-versuchen-es-mit-neuer-perfider-Masche_184808980.html

11) Neue Gefahr im Netz: Auf diesen Internetseiten sind Ihre Daten unsicher

Kriminelle versuchen aktuell, eine neue Art von Internetseiten für ihre Machenschaften zu nutzen. Wo Vorsicht gilt, erfahren Sie hier.

Seit kurzem können Seiten unter Googles Top-Level-Domain (TLD) .zip registriert werden. Cyber-Kriminelle nutzen diese schon jetzt für ihre Machenschaften, wie "Heise" berichtet.

Bei .zip handelt es sich nämlich auch um eine gängige Dateiendung. Die Betrüger erstellen nun echt aussehende Links, die angeblich zum Download von beliebten Programmen führen sollen. Tatsächlich werden die Seiten aber für Phishing oder das Verbreiten von Schadsoftware genutzt.

Kriminelle nutzen neue Domain für ihre Zwecke

Möglich ist beispielsweise, dass eine Domain mit dem Namen microsoft-office.zip erstellt wird. Unaufmerksame Nutzer könnten das für einen echten Download-Link halten. Tatsächlich werden dabei aber nur persönliche Daten der Opfer abgegriffen.

Nutzer sollten auf jeden Fall vorsichtig sein, wenn Sie auf eine Seite mit der TLD .zip stoßen. Bislang gibt es noch relativ wenige .zip-Seiten. IT-Administratoren sollten deshalb in Erwägung ziehen, den Zugriff auf .zip-Domains vorerst komplett zu blockieren.

Quelle: https://www.chip.de/news/Neue-Webseiten-Hier-drohen-fuer-Nutzer-haeufig-Gefahren_184795269.html

12) Betrüger mit neuer Masche bringen zwei Northeimer um Tausende von Euro

Zwei Northeimer Online-Verkäufer auf einem Kleinanzeigenportal Opfer von Betrügern.

Northeim – Gleich zwei Northeimer sind in den vergangenen Tagen Opfer einer neuen Betrugsmasche auf dem Portal Kleinanzeigen, ehemals ebay-Kleinanzeigen, geworden. Darauf weist die Polizeiinspektion Northeim in einer dringenden Warnmeldung hin. Den beiden Geschädigten sei ein Schaden in Höhe von mehreren 1000 Euro entstanden.

Was war geschehen? In beiden Fällen hätten sich die Täter als Kaufinteressenten für die von den Northeimern in dem Onlineportal angebotenen Waren ausgegeben, heißt es von einem Sprecher der Polizei.

Ohne groß über den Preis zu verhandeln, hätten die Täter schnell angeboten, den Kaufpreis über die neue Bezahlmethode von Kleinanzeigen „Sicheres Bezahlen“ zu überweisen. Hierzu sei ein Link an die Geschädigten, in einem Fall per E-Mail, in dem anderen Fall per SMS, geschickt worden, unter dem sich die Verkäufer für die neue Bezahlmethode registrieren sollten. Lediglich der Name und die Kreditkartendaten sollten hierfür eingetragen werden.

In dem Glauben, der Kaufpreis würde auf dem jeweiligen Kreditkartenkonto der Northeimer gutgeschrieben werden, hinterlegten die Geschädigten Vor- und Nachname, Kreditkartennummer, Kartenprüfnummer sowie die Gültigkeitsdauer der Kreditkarte. In einem Fall sei die vermeintliche Registrierung sogar durch ein Chatfenster begleitet worden.

Nachdem sich die angeblichen Kaufinteressenten noch einmal vergewissert hatten, dass auch tatsächlich die richtigen Kreditkartendaten eingegeben wurden, sei der Kontakt hinsichtlich des Kaufinteresses abrupt abgebrochen, heißt es von der Polizei. Zu einem Verkauf der angebotenen Waren sei es dann zwar nicht mehr gekommen. Wozu es allerdings kam, waren mehrere Abbuchungen über das Kreditkartenkonto der Geschädigten, die diese beide natürlich nicht veranlasst hatten.

Insgesamt entstand den Northeimern ein finanzieller Schaden von mehreren Tausend Euro, der nach Recherchen der Geschädigten und der Polizei nicht durch die Kreditkartengesellschaften erstattet werde.

Über den versandten Link war es den Tätern nämlich gelungen, die Geschädigten auf eine sogenannte „Phishing-Seite“ zu locken, die einer Webseite von Kleinanzeigen zum Verwechseln ähnlich aussieht. Mit den dort erlangten Daten konnten die Täter die Geld-Abbuchungen ausführen.

Warnung der Polizei

Die Polizei Northeim rät in diesem Zusammenhang mit der neuen Betrugsmasche eindringlich, niemals überhastet die gesamten Kreditkartendaten im Internet preiszugeben. Besser die bekannten Zahlungsmethoden nutzen. Man sollte keinen Links folgen, die von Dritten zugesandt werden und man sollte stets die Adress-Details zu den Absendern der E-Mails prüfen. In den oben beschriebenen Fällen sei der Link von einer iCloud-E-Mail-Adresse und nicht von Kleinanzeigen gekommen.

Quelle: https://www.hna.de/lokales/northeim/northeim-ort47320/betrueger-mit-neuer-masche-92302673.html

Anwenderinformationen:

1) Netflix startet Konto-Sharing in Deutschland: Das kostet es und das sollten Sie wissen

Netflix hat das Konto-Sharing in Deutschland gestartet. Das Konto-Sharing ist aber nicht bei allen Netflix-Konten erlaubt. So viel kostet ein Zusatzmitglied und das sollten Sie wissen.

Netflix kassiert ab sofort auch in Deutschland für das Teilen von Netflix-Konten. 4,99 Euro muss man pro zusätzlichem Nutzer (von Netflix als “Zusatzmitglieder” bezeichnet) eines

Netflix-Kontos zahlen. Allerdings steht diese Option nur bei den beiden teuersten Netflix-Abonnements zur Verfügung.

So identifiziert Netflix den Haushalt, für den ein Konto gilt

Das Netflix-Konto-Sharing gilt für Nutzer, deren IP-Adresse nicht zu dem Haushalt gehört, für den das Netflix-Hauptkonto angemeldet ist. Via GPS führt Netflix also keine Überprüfung durch, sondern maßgeblich sind die **IP-Adresse des Haushalt**s, die **Geräte-IDs**, sowie die **Auswertung der Konto-Aktivität von Geräten**, die sich mit dem Netflix-Konto anmelden. Aus all diesen Informationen bestimmt Netflix, ob ein Netflix-Konto innerhalb des Haushalts genutzt wird, für das das Netflix-Konto gilt.

Zusätzlich kann Netflix noch die Eingabe eines vierstelligen Ziffern-Codes verlangen. Diesen Code verschickt Netflix an den Inhaber des Netflix-Kontos, wie die Kollegen unserer Schwesterpublikation Techhive erklären.

Von unterwegs, also beispielsweise im Urlaub, sollen die Nutzer des Haushalts auch weiterhin problemlos auf Netflix zugreifen können. Dafür fallen keine Extra-Kosten an. Das zusätzliche Konto wird nur für solche Nutzer fällig, die dauerhaft von einer anderen IP-Adresse als von der IP-Adresse, die der für das Netflix-Konto angemeldete Haushalt nutzt, zugreifen.

Für diese Abonnements ist Konto-Sharing offiziell möglich

Beim Premium-Konto für 17,99 Euro pro Monat dürfen bis zu zwei Extra-Mitglieder hinzugefügt werden. Pro Extra-Mitglied werden 4,99 Euro fällig. Zusatzmitglieder können über ihr Konto Netflix auf beliebigen Geräten wiedergeben, jedoch nur ein Gerät gleichzeitig nutzen.

Beim Standard-Konto für 12,99 Euro darf ein Extra-Mitglied für 4,99 Euro pro Monat hinzugefügt werden. Beim Basis-Konto für 7,99 Euro ist das Konto-Sharing **nicht** möglich.

Das günstigste Netflix-Konto mit Werbung kostet übrigens ebenfalls 4,99 Euro. Auch hier ist das Konto-Sharing nicht möglich.

Das Zusatz-Konto kann nur im Land des zahlenden Account-Nutzers aktiviert werden.

Alle Kosten und Details zu den unterschiedlichen Netflix-Abonnements lesen Sie auf dieser Hilfeseite von Netflix nach. Die “Spielregeln” für Zusatzmitglieder erklärt Netflix wiederum hier.

Preise in den USA

In den USA startet Netflix das Konto-Sharing ebenfalls. Dort kostet ein Extra-Nutzer 7,99 Dollar, das sind umgerechnet 7,41 Euro.

In einigen europäischen Ländern führte Netflix das kostenpflichtige Konto-Sharing bereits ein: 3,99 Euro müssen Nutzer zusätzlich pro Person und Monat in Portugal zahlen und sogar 5,99 Euro sind es zusätzlich in Spanien. In Deutschland ist das Konto-Sharing also günstiger als in Spanien und in den USA.

So geht Netflix gegen “Schwarzseher” vor

Entdeckt Netflix Nutzer, die ein Konto von einer anderen IP-Adresse nutzen, dann will Netflix diese zunächst warnen und auf die Möglichkeit des kostenpflichtigen Kontoteilens hinweisen. Diese Warnung ist verbunden mit dem Hinweis, dass Netflix diesen Zugang bald sperren würde.

Netflix zielt mit dieser Regelung beispielsweise auf Kinder, die aus dem Elternhaus ausgezogen sind, aber weiterhin mit dem Netflix-Konto der Eltern Netflix schauen. Oder auf

Freunde, denen der Netflix-Kunde seine Zugangsdaten gegeben hat. Dadurch, dass für diese Nutzer nun bezahlt werden muss, erhofft sich Netflix Zusatzeinnahmen.

Quelle: https://www.pcwelt.de/article/1928517/netflix-startet-konto-sharing-kosten.html?utm_date=20230524103911&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Netflix%20startet%20Konto-Sharing%20in%20Deutschland%3A%20Das%20kostet%20es%20und%20das%20sollten%20Sie%20wissen&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

2) Whatsapp-Nachrichten nachträglich bearbeiten – darauf haben wir lange gewartet

Die Whatsapp-Nutzer dürfen sich auf eine neue Funktion freuen, auf die sie lange Zeit gewartet haben. Und so funktioniert das nachträgliche bearbeiten von versendeten Whatsapp-Nachrichten.

Whatsapp hat die Verfügbarkeit der neuen Editier-Funktion **offiziell angekündigt** und sie stehe über die nächsten Wochen allen Nutzern weltweit zur Verfügung. Mit der Funktion erfüllen die Entwickler den Wunsch vieler Nutzer, die sich schon seit langer Zeit eine Möglichkeit wünschen, den Inhalt einer versendeten Whatsapp-Nachricht nachträglich zu ändern.

“Für den Fall, dass du einen Fehler gemacht hast oder einfach deine Meinung änderst, kannst du jetzt deine gesendeten Nachrichten bearbeiten”, heißt es in der Mitteilung von Whatsapp. Diese Bearbeiten-Funktion steht nur 15 Minuten nach dem Versenden zur Verfügung und nachträglich geänderte Nachrichten werden als “bearbeitet” gekennzeichnet.

Konkreter heißt es seitens Whatsapp: “Die Empfänger*innen der Nachricht sind damit über die Korrektur informiert, nicht aber über den Änderungsverlauf. Wie alle persönlichen Nachrichten, Medien und Anrufe sind deine Nachrichten inklusive deiner vorgenommenen Änderungen Ende-zu-Ende-verschlüsselt.”

Damit erhält Whatsapp eine spektakuläre Neuerung. Bisher war es nämlich nicht möglich, den Inhalt einer bereits versendeten Whatsapp-Nachricht zu verändern (außer man löscht die Nachricht und versendet sie korrigiert erneut). Da kann es also schon mal peinlich werden, wenn eine Nachricht zu viele Rechtschreibfehler und / oder Vertipper enthält. Mit der neuen Editier-Funktion können die Fehler schnell korrigiert werden.

So funktioniert die neue Editier-Funktion für Whatsapp-Nachrichten

Wenn Sie ein Nachricht versendet haben, die Sie nachträglich korrigieren wollen, dann gehen Sie wie folgt vor: Tippen oder klicken Sie auf die Nachricht innerhalb der ersten 15 Minuten nach dem Versand und wählen Sie dann im Kontextmenü “Bearbeiten” aus. Korrigieren Sie die Nachricht. Der Empfänger erhält den Hinweis, dass die empfange Nachricht nachträglich “bearbeitet” wurde. Nach Ablauf der 15 Minuten Frist ist eine weitere Änderung des Inhalts der Nachricht nicht mehr möglich.

Quelle: https://www.pcwelt.de/article/1924518/whatsapp-nachrichten-nachtraglich-bearbeiten.html?utm_date=20230524104505&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Whatsapp-Nachrichten%20nachtr%C3%A4glich%20bearbeiten%20%E2%80%93%20darauf%20haben%20wir%20lange%20gewartet&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Tip – Whatsapp-Gruppe komplett löschen – so geht's auf Ihrem iPhone

Will man aus einer geschwätzigen Whatsapp-Gruppe austreten und diese löschen, gibt es dazu am iPhone keine offensichtliche Option. Wir zeigen Ihnen, wie es trotzdem geht.

Möchte man aus einer Whatsapp-Gruppe austreten und diese aus der Chatliste löschen, gibt es in der Whatsapp-App auf dem iPhone keine offensichtliche Option dazu. Weder in den Gruppeneinstellungen in der jeweiligen Gruppe noch im Kontextmenü beim Wisch ist etwas von "Gruppe löschen" zu sehen.

Der Hintergrund dabei ist: Whatsapp lässt die jeweiligen Gruppen-Chats aus Chatliste erst dann löschen, wenn man diese Gruppe verlassen hat.

So löschen Sie eine Gruppe auf dem iPhone

1. Wischen Sie in der Chatliste von Whatsapp bei der zu löschenden Gruppe nach links
2. Bei dem erscheinenden Kontextmenü tippen Sie auf das Symbol mit den drei Punkten
3. Wählen Sie daraus die Option "Gruppe verlassen" und bestätigen Sie anschließend die Eingabe
4. Nun sind Sie aus der Gruppe ausgetreten und können nicht mehr im Gruppen-Chat schreiben
5. Wischen Sie erneut in der Chatliste bei der gerade verlassenen Gruppe nach links
6. Bei dem erscheinenden Kontextmenü tippen Sie auf das Symbol mit den drei Punkten
7. Wählen Sie hier die Option "Gruppe löschen" und bestätigen Sie die Eingabe

Sie nehmen somit nicht mehr an der Konversation in der Gruppe teil, der komplette Chatverläufe samt aller Medien aus der Gruppe wird gelöscht.

Eine Whatsapp-Gruppe komplett für alle Teilnehmer sperren

Wenn Sie eine Gruppe für alle anderen Teilnehmer löschen wollen, wird das nur mit Admin-Rechten für diese Gruppe funktionieren. Davor müssen Sie jeden Teilnehmer aus der Gruppe entfernen, dies geht nur in den Gruppeneinstellungen und nicht mehr aus dem Kontextmenü heraus, indem Sie jeden Teilnehmer antippen und dabei "Aus Gruppe entfernen" wählen.

Anschließend verlassen Sie selbst die Gruppe und löschen diese. Bei den entfernten Teilnehmern bleibt die Gruppe noch in der Chatliste, diese können aber nichts mehr schreiben und nicht neu beitreten.

Quelle: https://www.macwelt.de/article/1920374/whatsapp-gruppe-loeschen-iphone.html?utm_date=20230524110620&utm_campaign=Macwelt%20Daily&utm_content=Title%3A%20Whatsapp-Gruppe%20komplett%20l%C3%B6schen%20%E2%80%93%20so%20geht%27s%20auf%20Ihrem%20iPhone&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Dieses kostenlose Microsoft-Tool reinigt und optimiert Windows

Systemreiniger und -optimierer gibt es wie Sand am Meer. Am beliebtesten, wenn auch nicht unumstritten ist CCleaner. Nun macht Microsoft selbst dem CCleaner und ähnlichen Tools Konkurrenz: mit einer ersten öffentlichen Beta-Version des PC Manager, der Entmüllung, Virenscan und Updates in einer einfachen Oberfläche vereint.

16 Jahre nach der ersten Veröffentlichung ist **CCleaner** immer noch ein beliebter Systemreiniger für Windows-PCs. Damit kann man seinen Windows-PC mit wenigen Klicks in einer (halbwegs) übersichtlichen Oberfläche von Datenmüll befreien und andere Optimierungen vornehmen. **CCleaner ist aber nicht frei Kritik**: Unnötige Pseudo-Optimierungen wie die Registry-Defragmentierung, ein immer stärkerer Fokus auf Monetarisierung, Bündelung mit anderer Software und ressourcenfressende Hintergrund-Dienste sind nur einige der Kritikpunkte.

CCleaner ist allerdings noch eines der seriösen Produkte inmitten einer gigantischen Menge an betrügerischen Säuberungs- und Optimierungs-Tools für Windows-PCs. Viele dieser Produkte arbeiten lediglich mit Placebo-Effekten, nehmen gefährliche Änderungen am System vor oder installieren gar Malware. Gerade unbedarfte User installieren diese häufig aus Versehen.

CCleaner-Konkurrenz von Microsoft

Microsoft hat nun seinen **eigenen Systemreiniger** in einer ersten öffentlichen Beta-Version unter dem Namen **PC Manager zum Download** freigegeben (bei Microsoft ansehen). Das Tool erfindet nicht das Rad neu, aber es bündelt, wie auch CCleaner, einige sinnvolle Funktionen unter einer Oberfläche:

- Löschen temporärer Daten und anderen Datenmülls,
- Windows-Programme aus dem Autostart entfernen,
- Windows-Updates anstoßen,
- Virenscan starten,
- Prozesse beenden und
- Standard-Browser ändern.

Zum letzten Punkt: Microsoft versucht bereits an zahlreichen anderen Stellen in Windows mit zahlreichen „Dark Pattern“ Kunden dazu zu bringen, **Microsoft Edge als Standardbrowser einzustellen**. Das spiegelt sich auch in diesem Tool, indem es Edge als „recommended“, also empfohlen, darstellt.

Was taugt Microsofts PC Manager?

Abgesehen davon scheint der PC Manager aber in Ordnung. Vorteil gegenüber CCleaner ist, dass nach dem Deaktivieren von Autostart-Anwendungen direkt der Einfluss auf die Startzeit gemessen wird. CCleaner hat hingegen einige Optionen mehr, was die Löschung von Daten aus Anwendungen angeht. Die meisten Funktionen beider Tools kann man freilich auch mit Windows-Bordmitteln erreichen (Autostart-Management: Strg + Shift + Esc → Tab „Autostart“; Datenreiniger: Win + R → cleanmgr).

Größtes Verdienst des PC Manager ist entsprechend, **dass Microsoft ihn überhaupt anbietet** und damit eine **Alternative zu den etlichen schädlichen Tools** bringt, die bestenfalls keinen Vorteil bringen und schlimmstenfalls die Systemsicherheit gefährden. Auch wenn der PC Manager für versierte Nutzer nicht notwendig sein mag – jede verhinderte Installation eines dieser schädlichen Tools ist trotzdem ein Gewinn.

PC Manager downloaden

Den PC Manager kann man auf dieser Seite bei Microsoft downloaden. Er läuft unter Windows 10 und 11. Die erste Beta-Version ist ausschließlich auf Englisch verfügbar.

Quelle: https://www.giga.de/news/dieses-kostenlose-microsoft-tool-reinigt-und-optimiert-windows/

5) Windows 10: Vorsicht vor Update KB5026361

Auch für Windows 10 erscheinen noch regelmäßig Updates. Ein neues sorgt allerdings für reichlich Probleme.

Zwar gibt es schon seit einiger Zeit Windows 11, aber noch ist die Vorgängerversion nicht am Ende. So erscheinen auch für **Windows 10** immer wieder neue Updates und Sicherheitspatches. Jüngst ist wieder eines erschienen, das aber direkt für Ärger gesorgt hat.

Windows 10: KB5026361 ist wichtig, sorgt aber für Probleme

Grundsätzlich sollten neue Patches und Updates immer möglichst zügig heruntergeladen und installiert werden. Auch bei KB5026361 für Windows 10 ist das erst einmal nicht anders. Auch hier handelt es sich um eine Aktualisierung, die gleich eine ganze Reihe Sicherheitslücken stopft, wie Neowin berichtet.

Allerdings sollen dem Artikel nach zahlreiche Userinnen und User in verschiedenen Internetforen und auf Microsofts Feedbackseite ihrem Ärger über neue Probleme Luft gemacht haben. Eine verhinderte Installation des Updates, Blue Screens oder ungewollte Neustarts gehören zu den Ärgernissen.

Übrigens: Es gibt einen Windows 10-Trick, auf den du sicher nicht verzichten möchtest. Wir sagen dir, was du dazu tun musst.

Microsoft schweigt noch

Viele Leute geben einen Fehlerbildschirm mit dem Code „Process1 Initialization Failed“ an. Wie WinFuture schreibt, könnte dies auf ein älteres Problem mit der sogenannten Bootcat-Datei deuten. Dieses soll auftreten, wenn die Bootcat.cache-Datei beschädigt ist oder sich ihre Größe seit dem letzten Systemstart verändert hat.

Wer aber „0x800f0922“ als Fehlercode erhält, sollte nicht verzagen. Angeblich sollen mehrere Versuche in diesem Fall die Lösung bringen. Abgesehen davon gibt es aber leider noch kein offizielles Statement von Microsoft zum Windows 10-Problem.

Quelle: https://www.futurezone.de/digital-life/article454656/windows-10-vorsicht-vor-update-kb5026361.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

6) Word: Wie Sie Texte ohne Formatierung kopieren

Beim Kopieren von Textabschnitten zwischen Dokumenten ist das Beibehalten der Formatierung oft hinderlich. Besser ist es, nur den reinen Text zu übernehmen. Eine Einstellung in Word ermöglichen dies.

Wenn Sie Abschnitte aus einem Textdokument per Copy und Paste in ein anderes übernehmen möchten, ist das Beibehalten der Formatierung oftmals eher hinderlich. In diesem Fall passt Word die Formatierung im Absatz des Zieldokuments an das Format des übertragenen Textteils an, was dann immer erst korrigiert werden muss. Besser ist es deshalb, lediglich den reinen Text ohne die Formatierung zu übernehmen. Das können Sie in den Optionen von Word einstellen.

Klicken Sie hierzu auf „Datei –› Optionen –› Erweitert“ und scrollen Sie in dem nachfolgenden Fenster nach unten zu dem Abschnitt „Ausschneiden, Kopieren und Einfügen“. Dort unterscheidet Word dann zwischen vier verschiedenen Fällen: dem „Einfügen innerhalb desselben Dokuments“, dem „Einfügen zwischen zwei Dokumenten“, dem „Einfügen

zwischen Dokumenten, wenn Formatvorlagendefinitionen nicht übereinstimmen“ und dem „Einfügen aus anderen Programmen“.

Zum Lösen des genannten Problems sind die ersten beiden Fälle interessant. In der Voreinstellung sind sie beide auf die Option „Ursprüngliche Formatierung beibehalten (Standard)“ konfiguriert. Um lediglich den Inhalt zu übertragen, stellen Sie um auf „Nur den Text übernehmen“ und bestätigen mit „OK“.

Tipp: Word: Diese neue Tastenkombination spart Zeit

Quelle: https://www.pcwelt.de/article/1918181/word-texte-ohne-formatierung-kopieren.html?utm_date=20230525141119&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Word%3A%20Wie%20Sie%20Texte%20ohne%20Formatierung%20kopieren&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Software-Problem sorgt für leere Festplatten: So sollten Besitzer jetzt reagieren

Aufgrund eines Software-Problems klagen aktuell viele Nutzer über leere Festplatten. Wie Nutzer entgegenwirken können, erfahren Sie hier.

Zahlreiche Besitzer beschweren sich seit einiger Zeit über Probleme mit ihrer SanDisk Extreme und SanDisk Extreme Pro. Wie "Ars Technica" berichtet, hat sich Hersteller Western Digital nun zu dem Problem geäußert.
Es handle sich um einen Fehler in der Firmware. Bei länger andauernder Schreiblast könne das Dateisystem beschädigt werden. Dadurch drohe der Verlust aller gespeicherter Dateien auf dem Gerät. WD bestätigt den Fehler nur für die Vier-Terabyte-Versionen mit den Kennungen SDSSDE61-4T00 und SDSSDE81-4T00.

Datenverlust droht wegen Firmware-Fehler: Das müssen Betroffene jetzt beachten

Allerdings gibt es auch Berichte darüber, dass das Problem bei SSDs mit einer Kapazität von zwei Terabyte auftritt. Ein Mitarbeiter von Ars Techinca konnte den Fehler auch auf einem solchen Gerät reproduzieren.
WD hat unterdessen ein Firmware-Update für die 4-TB-Versionen angekündigt. Dieses soll "bald" veröffentlicht werden. Besitzer betroffener Geräte sollten ihre Daten bis zu dem Update unbedingt zusätzlich auf einem anderen Gerät oder in einer Cloud sichern. Wichtige Daten sollten ohnehin nie nur an einem Ort gespeichert werden.

Quelle: https://www.chip.de/news/Wegen-Software-Bug-Daten-auf-einigen-Festplatten-geloescht_184802982.html?utm_content=CHIP_online%2Fmagazine%2FCHIP&utm_source=flipboard

8) Was diesem Mann mit seinem Google-Konto passiert ist, geht Millionen Nutzer etwas an

Google erklärte einen Mann aus Bayern fälschlicherweise für tot. Beweisen, dass er noch lebt, konnte Peter Stör nicht. Der Grund: Er erreichte keinen menschlichen Google-Mitarbeiter, musste mit Support-Seiten und Roboter-Stimmen vorliebnehmen. Das empfinden auch viele andere Nutzer als Problem.

Als Peter Stör im Oktober 2022 versuchte, sich in seinem Google-Konto einzuloggen, scheiterte er. "Ich bekam die Meldung, dass mein Benutzerkonto deaktiviert ist und ich verstorben bin", sagte er der "Augsburger Allgemeinen" im April.

Ganz offensichtlich handelte es sich bei der Nachricht um einen Fehler. Denn Peter Stör ist ziemlich lebendig. "Ich dachte, dass man das Konto problemlos wieder aktivieren kann", erklärte er.

Doch da irrte sich der Mann, der im mittelfränkischen Eckental in der Nähe von Erlangen wohnt. Denn bei Google war niemand zu erreichen, kein menschlicher Mitarbeiter, der ihm hätte weiterhelfen können.

Stattdessen: Automatisierte Formulare, Roboterstimmen am Telefon. "Ich habe nie mit einem Menschen gesprochen. Man kann da anrufen, kommuniziert aber nur mit einer Maschine." Stör beauftragte sogar einen Anwalt, um wieder in seinen Account zu kommen. Aber auch das änderte nichts an der Situation.

"E-Mail-Anfragen an Google werden mit Textbausteinen beantwortet"

Dass bei Google offenbar kein menschlicher Support zu erreichen ist, ärgert nicht nur Peter Stör. Zahlreiche Nutzer haben sich an unsere Redaktion gewandt, weil sie sich von dem Tech-Riesen bei Account-Problemen im Stich gelassen fühlen.

"Seit Jahren habe ich keinen Zugriff mehr zum Admin-Bereich meines kostenlosen Google-Kontos", schreibt ein Mann aus München. Das Unternehmen habe seine Identität überprüfen wollen und ihm dazu eine SMS mit einem Zahlencode an die alte Handynummer geschickt.

Auf die hat der Bayer eigenen Angaben zufolge allerdings keinen Zugriff mehr. Auch er versuchte, mit menschlichen Google-Mitarbeitern in Kontakt zu treten. Das Problem irgendwie zu lösen, am besten im Dialog mit jemandem, der sich auskennt. Aber: Fehlanzeige.

"Email-Anfragen an Google werden mit Textbausteinen beantwortet, die mich immer wieder in denselben ausweglosen Kreislauf von Hilfetipps führen und bei einer SMS oder einem Anruf an meine alte Handynummer enden", ist in seiner E-Mail zu lesen. "Telefonisch Kontakt zu Google herzustellen, ist nicht möglich."
Gmail, web.de, Telekom: Wie sicher sind die gängigsten E-Mail-Provider?

Google spielt im Leben der meisten Menschen eine wichtige Rolle

Für den Münchner hatte das ernste Folgen. "Ich bin selbstständig", schreibt er. "Ich musste meine Gmail-Anschrift von Geschäftspapieren und von der Webseite tilgen und alle Kunden bitten, bis auf Weiteres eine andere Adresse zu verwenden. Das ist nicht nur sehr ärgerlich, sondern auch geschäftsschädigend."

Google gehört für die meisten Menschen zum Alltag. Viele nutzen die hauseigene Suchmaschine, aber auch E-Mail-Konten, die Cloud oder den Bezahlservice des Tech-Riesen. Wer ein Android-Handy besitzt, ist ohnehin auf einen Google-Account angewiesen. Andernfalls lässt sich der Play Store nicht nutzen.

Eric Mayer, der seinen richtigen Namen nicht im Internet lesen will, hatte "sein halbes Leben" im Google-Konto gespeichert, wie er im Gespräch mit CHIP erzählt. Als er abends mit seiner Freundin ein YouTube-Video schauen wollte, war er plötzlich nicht mehr in seinem Account eingeloggt. "Ich habe versucht, mich wieder anzumelden, aber es ging nicht. Da saß ich kerzengerade im Bett."

Ausweiskopien, Steuerunterlagen, private Bilder - Mayers Google-Account war eine Art persönliches Archiv. Umso schlimmer, nicht mehr auf all die Daten, all die Nachrichten und

Informationen, zugreifen zu können. Wie andere Betroffene wandte sich Mayer per Mail an Google, erhielt standardisierte Antworten und Verweise auf das Account-Wiederherstellungsformular.

"Ich wurde gehackt", sagt Mayer

Nichts funktionierte. Anfragen, sein Konto zu sperren oder zu löschen, blieben unbeantwortet. Also ging Mayer zur Polizei und erstattete Anzeige gegen Unbekannt. "Ich bin gehackt worden, da war ich mir schnell sicher", sagt er.

Die Kriminellen hatten seinen Angaben zufolge einen Bluetooth-Key eingerichtet. Dabei handelt es sich um einen externen Sicherheitsschlüssel, der notwendig ist, um sich im betreffenden Account anzumelden. Mayer dachte schon, er würde sich nie wieder in sein Konto einloggen können.

"Aber plötzlich, als ich von der Polizei nach Hause zurückkehrte, konnte ich mich wieder anmelden. Die Hacker hatten den Key entfernt und mein Passwort funktionierte", sagt er. Trotzdem: Die Geschehnisse haben Spuren hinterlassen. Mayer hat Handy und Laptop zurückgesetzt, und überall, wo es möglich war, die 2-Faktor-Authentifizierung aktiviert.

"Ein blödes Gefühl habe ich immer noch", sagt er. Die Frage, die bleibt, ist: Warum ist es so schwer, an menschlichen Google-Support zu kommen? Mitarbeiter zu erreichen, die Menschen wie Peter Stör oder Eric Mayer helfen können? Reddit-Nutzer diskutieren darüber schon seit Jahren, es gibt zahlreiche Diskussionsstränge auf der Plattform.
Gängige Irrtümer: Das sollten Sie bei der Passwort-Wahl unbedingt beachten

Google reagiert überraschend konkret auf Vorwürfe

Wer bei Google nachfragt, warum der Konzern am "menschlichen Faktor" spart, erhält überraschend konkrete Antworten.
"Google bietet für viele Produkte und Dienste menschlichen Support, einschließlich Telefon, E-Mail und Chat. Die meisten unserer Online-Formulare, einschließlich der Kontowiederherstellung, leiten Support-Interaktionen mit echten Support-Mitarbeiter:innen ein", schreibt Pressesprecherin Enita Ramaj auf CHIP-Anfrage.

Und weiter: "Wir bieten Nutzer:innen nicht nur die Möglichkeit, ihr Problem online zu lösen, sondern auch gebührenfreie Telefonnummern und E-Mail-Support in allen Ländern des europäischen Wirtschaftsraums und in allen Sprachen, in denen Google-Produkte angeboten werden."

Deutsche Nutzer können entweder die **Telefonnummer 0800-5894309** anrufen oder eine Nachricht an **support-deutschland@google.com** schicken.
In der schriftlichen Antwort verweist Ramaj außerdem auf verschiedene Support-Seiten des Tech-Riesen. Darunter Formulare, die helfen sollen, ein gehacktes oder manipuliertes Google-Konto zu schützen oder die erklären, was im Fall eines deaktivierten Accounts zu tun ist. Seiten, auf die viele verzweifelte Nutzer wahrscheinlich längst gestoßen sind.
WhatsApp und Co.: Diese Gefahr schlummert in alltäglichen Apps

Mayer ist nachhaltig verunsichert

Am Ende bleibt der "menschliche Faktor" bei Google zwar immer noch obskur. Offenbar haben Nutzer aber sehr wohl die Möglichkeit, mit Mitarbeitern des Konzerns in Kontakt zu treten. Auch, wenn Google dieses Angebot nicht sehr prominent ausweist.

Mayer, der sich wieder in seinen Account einloggen kann, ist trotzdem nachhaltig verunsichert. "Als ich dringend Hilfe brauchte, habe ich keinen richtigen Ansprechpartner gefunden", sagt er. Auch Peter Stör, den Google für tot erklärte, hat inzwischen wieder Zugriff auf sein Konto.
Allerdings nur, weil sich das BR-Magazin "quer" an den Konzern wandte. "Es kam tatsächlich eine Mail, dass das Konto wieder hergestellt ist. Für den, der sich das angeschaut hat, war das ein Klick. Der hat nur einen Haken gesetzt, keine Minute Arbeit."

Quelle: https://www.chip.de/news/Was-diesem-Mann-mit-seinem-Google-Konto-passiert-ist-geht-Millionen-Nutzer-etwas-an-1_184770942.html

9) „Sofort deaktivieren“: Experten warnen vor eigentlich harmloser Handy-Einstellung

Nicht alle Funktionen deines Smartphones sind dauerhaft notwendig. In einem Fall raten Fachleute sogar aktiv davon ab.

Manche **Handy-Einstellungen** sind so selbstverständlich, dass wir sie gar nicht mehr ausschalten. Musst du nicht gerade auf deinen Akkuverbrauch achten, ist das in der Regel kein Problem. Bei mobilem WLAN allerdings raten Fachleute dringend dazu, die entsprechende Funktion regelmäßig abzustellen. Läuft sie nämlich durchgehend, ist nicht etwa die Batterie dein Problem.

Handy-Einstellung: Deshalb das WLAN deaktivieren

Was es schwierig machen kann, wenn deine WLAN-Verbindung immer aktiviert ist, ist nicht die Funktion selbst. Aber dafür der **Zugang, den sie zu deinem Gerät und deinen Daten ermöglicht**. Gleich über verschiedenen Anlaufstellen soll es Fremden bei aktivierter oder nicht optimierter Handy-Einstellung nämlich gelingen können, auf dein Telefon zuzugreifen.

Miklos Zoltan, CEO und Sicherheitsforscher bei Privacy Affairs, hält das Risiko für hoch. Er rät deshalb zur kompletten Deaktivierung der Funktion.

> „Die eine Handy-Einstellung, die du sofort ausschalten solltest, ist das WLAN. Öffentliche WLAN-Netzwerke werden oft von Hackern kontrolliert (…). Verbindest du dich mit diesen Fake-Netzwerken, können sie alles überwachen, was du tust. Ergo, schalte es (das WLAN) ab (…), so dass deine persönlichen Daten sicher und geschützt bleiben“.
>
> *Miklos Zoltan, CEO und Sicherheitsforscher Privacy Affairs*

Auch andere Expert*innen raten vom Dauer-WLAN ab

Erst Ende 2021 wurde eine Studie an der Universität Hamburg durchgeführt, die zu ähnlichen Ergebnisse kam. Auch damals zeigten Forschende die negativen Folgen der aktivierten Handy-Einstellung WLAN.

Im Rahmen der Untersuchung gelang es zehntausende SSIDs sowie Hinweise auf sensible Daten wie Passwörter, Namen, E-Mail-Adressen und sogar Unterkünfte wie Ferienhäuser zu entdecken.

Bleibt das WLAN an, tu zumindest das

Wer sich vom Aus der Handy-Einstellung nicht überzeugen lässt, hat noch eine alternative Schutzmöglichkeit. Wie Caroline Lee von CocoSign, einer Softwarelösung für sichere digitale

Unterschriften, erklärt, sollte dann eine wichtige Vorkehrung getroffen werden. Sie hilft ebenso, dich vor Hackern zu bewahren: „Halte dein Telefon versteckt vor anderen Geräten, wenn du öffentliches WLAN benutzt“.

Das verhindert Lee zufolge vor allem, dass Fremde dein Smartphone über Funktionen wie „Drucken“ oder das Teilen von Daten kompromittieren können. Das sind „die WLAN-Einstellungen, die du unbedingt deaktivieren musst“, sagt Lee. Um anonym zu surfen und dein Handy für andere unsichtbar zu machen, helfen dir zum Beispiel VPN-Apps weiter.

Wie funktioniert WLAN einfach erklärt?

Besteht eine aktive WLAN-Verbindung mit deinem Endgerät, kannst du dich mittels dieser Funkverbindung über den Router mit deinem Computer ins Internet einwählen. Am Computer benötigst du dafür dann zum Beispiel anders als bei einer herkömmlichen LAN-Verbindung kein Kabel mehr.

Dein Handy stellt automatisch eine Verknüpfung zu entsprechenden WLAN-Netzwerken in der Nähe her, mit denen es bereits verbunden war. Das WLAN selbst steht dabei im Prinzip also nur für den drahtlosen Zugang zum Internet, daher auch die Bezeichnung „Wireless Local Area Network“ (WLAN).

WLAN ausschalten unter Android und iOS

Das WLAN auszuschalten, ist am Handy leicht. Die Schritte unterscheiden sich zwischen Android-Geräten und iPhones nur minimal und sind in jedem Fall schnell durchgeführt.

Android

1. Wische vom oberen Rand nach unten, um die Schnellnavigationsleiste zu öffnen. Tippe auf das Symbol für WLAN, um es auszuschalten.
2. Alternativ kannst du die Einstellungen aufrufen, auf „Verbindungen“ tippen und den Schalter neben „WLAN“ verschieben.

iOS

1. Öffne die Einstellungen und navigiere in den Bereich WLAN. Lege dort den Schalter um. Im Kontrollzentrum kannst du kontrollieren, ob dein WLAN ausgeschaltet ist. Wenn das Symbol dafür durchgestrichen ist, sind WLAN und Funkschnittstellen deaktiviert.

Für wen und wann lohnt sich WLAN?

Achtest du darauf, mit welchem Netzwerk du dich verbindest, ist das WLAN sehr hilfreich. Ist der Abstand zwischen Endgerät und Router zum Beispiel sehr groß oder sollen mehrere Endgeräte online gehen, die sich nicht in unmittelbarer Nähe befinden, lohnt sich die Verbindung besonders.

Die Handy-Einstellung erlaubt es zudem, unabhängig von den eigenen vier Wänden ins Internet zu gehen. Netzwerke von Freunden und Bekannten oder sichere öffentliche Hotspots sollten dabei am besten bevorzugt werden.

Wer dies allerdings nicht benötigt oder auf mobile Daten zurückgreift, kann das WLAN ausstellen. Für den Handy-Akku ist dies zumindest einen Erleichterung.

Nicht nur WLAN: Achte auch auf diese Handy-Einstellungen

Hast du ab sofort ein Auge auf dein WLAN, prüfe auch die folgenden Handy-Einstellungen. Von Expert*innen werden sie unter bestimmten Umständen nämlich ebenfalls als kritisch eingestuft. Dein Bluetooth am Smartphone kann beispielsweise zum Problem werden. Dagegen gibt es gleich mehrere Handy-Einstellungen unter Android, die nicht unbedingt

empfehlenswert sind. Vor allem, wenn du Wert auf deine Privatsphäre legst, lohnt sich ein Blick auf die Funktionen.

Quelle: https://www.futurezone.de/digital-life/article456548/sofort-deaktivieren-experten-warnen-vor-eigentlich-harmloser-handy-einstellung.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

10) Sofort löschen! Beliebte App zeichnet Audio auf

Dass Anwendungen mit Trojaner-Viren infiziert sind, ist nicht gerade selten. Doch diesmal soll der Schadcode nachträglich per Update auf das Handy gelangt sein. Betroffene sollten die infizierte App schnellstmöglich deinstallieren.

Apps mit Schadcode finden sich regelmäßig in Googles Play Store und auch im Apples App Store wieder. Zwar setzen beide Plattformen auf ausgeklügelte Sicherheitsmaßnahmen, doch wo ein Zaun ist, da ist auch ein Spalt. Im aktuellen Fall war ein Spalt zunächst jedoch nicht notwendig. Denn ursprünglich enthielt die Anwendung auch keinerlei Malware.

Spionage-Features nachträglich ergänzt

Die Sicherheitsforscher von Eset warnen aktuell vor der Android-App iRecorder. Diese sollte ursprünglich zum Aufzeichnen des Bildschirms genutzt werden und genoss mit einer Wertung von 4,2 und über 50.000 Downloads eine hohe Popularität. Im Gegensatz zu den meisten anderen Spionage-Apps veröffentlichte der Entwickler diese gegen Ende 2021 ohne Malware-Features. Diese seien nach Angaben von Eset erst im August 2022 per Update ergänzt worden.

Mit dem Update gelangte AhRat, eine modifizierte Variante das Open Source RATs AhMyth (Fernzugriffstrojaner) auf das Smartphone. Dieses soll das Mikrofon des Mobiltelefons unbemerkt dazu genutzt haben, um alle 15 Minuten eine einminütige Tonspur aufzuzeichnen und diese an die Server des Entwicklers zu schicken. Ferner erhielt iRecorder eine Funktion zum Stehlen von Dateien wie Lesezeichen, Bilder, Audio, Video und Dokumenten.

Nachdem Eset seine Erkenntnisse mit Google teilte, entfernte der Android-Entwickler die Spionage-App aus dem Play Store. Hast du iRecorder jedoch bereits vorher heruntergeladen, musst du die infizierte Anwendung nun manuell deinstallieren. Weitere Programme des Entwicklers Coffeeholic Dev scheinen ohne Schadprogramme auszukommen – zumindest ist es aktuell der Fall.

So minimierst du das Risiko

Es existieren mehrere Möglichkeiten, das Risiko von Malware auf dem Handy zu verringern. Zunächst einmal empfiehlt es sich, vor einer Installation auf die Bewertungen zu achten. Denn infizierte Apps werden dem beworbenen Funktionsumfang gelegentlich nicht gerecht. Ferner solltest du die Installation von Apps aus unbekannten Quellen generell vermeiden – also von außerhalb des offiziellen Play Stores. Zu guter Letzt solltest du stets auf die Berechtigungen achten, die eine Anwendung einfordert. Möchte etwa eine Wecker-App Zugriff auf deine Kontaktliste, ist dies ein Grund, um misstrauisch zu werden.

Quelle: https://www.inside-digital.de/news/beliebte-app-zeichnet-audio-auf-virus

11) Nicht nur zum Aufladen: 3 Dinge, die dein USB-C-Kabel noch kann

Jede*r hat mindestens ein elektronisches Gerät, das über den Anschluss verfügt. In den meisten Fällen nutzen wir allerdings nicht das volle Potenzial dahinter.

Das Format gibt es schon seit Ende 2014, erst in den vergangenen Jahren scheint sich **USB-C** aber mehr und mehr durchgesetzt zu haben. Grund genug, einmal genauer hinzuschauen und wirklich alle Fähigkeiten der Kabel und Stecker zu nutzen. Stromversorgung ist nämlich nur ein Teil davon.

Was ist ein USB-C-Anschluss?

Das physische Steckerformat USB-C (auch USB Typ-C) ? wurde vor rund acht Jahren eingeführt. Zu finden ist es mittlerweile bei PCs, Handys, Notebooks und Festplatten und soll irgendwann alle aktuellen USB-Stecker ersetzen. Damit verkörpert es am besten die Eigenschaft „universell“, für die die Bezeichnung USB (Universal Serial Bus) steht.

- **Lesetipp**: Das ist der Unterschied zwischen USB-C und Thunderbolt

Kennst du diese 3 USB-C-Funktionen?

Wie groß der Bedarf an einem einheitlichen Standard ist, zeigt der Beschluss der EU, der selbst Apple in die Knie zwingt. Demnach wird der USB-C-Anschluss ab 2024 verpflichtend. Für das iPhone könnte USB-C deshalb schon 2023 kommen, wenn man einem Analysten glaubt.

Allein angesichts der unterschiedlichen Einsatzmöglichkeiten, die ein USB-C-Anschluss an Handys erlaubt, ist diese Entwicklung überfällig. Die folgenden drei Features zeigen das ebenso.

#1 Datentransfer in hoher Geschwindigkeit

Mit der neuen USB4 2.0-Spezifikation kann USB-C Daten mit einer Geschwindigkeitsrate von bis zu 80 Gigabit pro Sekunde (Gbps) übertragen. Erste Geräte dafür sollen 2024 kommen. Ganz aktuell können Stecker des Formats USB Typ C 3.1 bis zu zehn Gbps übermitteln.

Zum Vergleich: Zu Beginn der USB-Ära lagen entsprechende Raten bei rund einem Megabit pro Sekunde.

#2 Alternative Transfer-Modi

Neben Energie und Daten erlaubt USB-C die Übertragung von Video- und Audiosignalen. So kannst du mit dem Kabel und Stecker auch nicht-USB-Protokolle nutzen. Dazu zählen HDMI, DisplayPort, Thunderbolt und MHL. Dadurch sind Geräte mit nur einen USB-Anschluss zu verschiedenen Dinge wie Video- und Audio-Output fähig. Sowohl für ihr Design als auch ihre Nutzung bringt das Vorteile.

Hinweis: Nicht alle USB-C-Anschlüsse unterstützen auch alle Modi. Es hängt von den Geräten und Kabeln ab.

#3 Umkehrbarer Stecker

Anders als bei vorherigen USB-Spezifikationen lassen sich Daten und auch Strom mit USB-C in beide Richtungen übertragen. Dazu kommt, dass der Stecker für das USB-C-Format beidseitig nutzbar ist. Es ist egal, wie herum er in den Anschluss gesteckt wird, er funktioniert in beiden Fällen sofort – der signifikanteste Vorteil, der er gegenüber seinen Vorgängern

mitbringt.

Quelle: https://www.futurezone.de/digital-life/article456225/nicht-nur-zum-aufladen-3-dinge-die-dein-usb-c-kabel-noch-kann.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

12) Unbedingt Widerspruch einlegen: Telekom, o2 und Co verkaufen Ihre Daten

Mobilfunkanbieter haben eine Menge Daten von Ihnen. Manche davon werden für Analysen und Tracking verwendet. Möchten Sie das unterbinden, zeigen wir Ihnen zwei einfache Wege zum Ziel. Doch einen Haken hat die Sache.

Bewegungsdaten, Postleitzahl, Alter, Geschlecht: Die Mobilfunkanbieter kennen einige Daten von Ihnen und werten diese auch aus – manchmal werden diese Informationen auch an Dritte weitergegeben. Doch nicht jeder möchte das.

Wenn Sie dazugehören, dann können Sie sich in wenigen Schritten vom Tracking abmelden. Allerdings gibt es einen Haken, denn von den drei großen Anbietern Telekom, o2 und Vodafone bietet **einer keine Möglichkeit** dazu.

Verkauf von Bewegungsdaten unterbinden

Zumeist werden die Daten komplett anonymisiert und sind auch grob genug, sodass keine Individuen damit erkannt werden können. So werden bei der Telekom aus dem Vertrag nur das Geschlecht, die Altersgruppe in 10-Jahres-Schritte sowie die ersten vier Stellen der Postleitzahl genutzt.

Wenn Sie sich bei der Telekom von der Datenverwendung austragen wollen, dann besuchen Sie einfach den Opt-Out Service auf der Herstellerseite. Sie müssen dort ganz unten lediglich die Vorwahl und Ihre Handynummer eingeben. Sie erhalten einen Code per SMS, den Sie im vorgesehenen Feld eingeben. Das klappt auch mit anderen Anbietern wie Congstar oder Klarmobil, die zur Telekom gehören.

Ähnlich einfach ist es bei o2 Telefónica und dem Service namens "Selbst entscheiden". Hier senden Sie einfach eine SMS mit dem Text **Abmelden** an die Kurzwahl 66866. Kurz darauf erhalten Sie eine Bestätigung von o2. Roaming-Kunden im Ausland müssen hingegen den Text **Unsubscribe** an die Nummer +491771789498 schicken.

Derselben Anleitung können auch Nutzer von Aldi Talk folgen, da dieser Anbieter ebenfalls zur Telefónica-Gruppe gehört. Das gilt auch für simplytel, allerdings werden die Daten hier nicht verwendet, darum ist ein Widerspruch nicht möglich.

Vodafone bietet keine Widerspruchsmöglichkeit

Der Wermutstropfen: Bei Vodafone gibt es aktuell keine Möglichkeit, einen solchen Widerspruch bei den Bewegungsdaten einzureichen. Laut einem Forumsbeitrag werden diese aber nicht weitergegeben und nur anonym ausgewertet, um die Netzqualität zu prüfen. Sie können hier nur in der App Mein Vodafone die Einstellungen prüfen und nachschauen ob Nutzungsdaten an den Mobilfunkanbieter übertragen werden.

Anmerkung der Redaktion: Weitere Infos sind unter dem u.g. Link abrufbar

Quelle: https://www.chip.de/news/Unbedingt-Widerspruch-einlegen-Telekom-o2-und-Co-verkaufen-Ihre-Daten_184655740.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=25-05-2023%2B17%253A00%253A04&utm_content=nl_chipmob&utm_term=

13) USB-Stick reparieren: So einfach geht's

Ist Ihr USB-Stick kaputt und enthält wichtige Dateien? Dann sollten Sie versuchen, den Datenträger zu reparieren. So kann es gelingen.

Zeigt Ihnen das Betriebssystem eine Fehlermeldung an, wenn Sie ihren mobilen Speicher nutzen wollen? Wenn Sie auf Ihre Daten nicht mehr zugreifen können, kann die Dateistruktur auf dem Laufwerk beschädigt sein.

Keine Panik, womöglich können Sie einen Datenverlust vermeiden. Denn in einigen Fällen lässt sich der beschädigte USB-Stick mithilfe von Software-Tools oder Windows-eigenen Lösungen reparieren und eine Datenrettung vornehmen.

Schließen Sie den defekten Stick an Ihren Windows-PC an und überprüfen Sie, ob dieser ihn erkennt. Öffnen Sie den Explorer, klicken Sie mit der rechten Maustaste auf "Wechseldatenträger", "Eigenschaften", "Tools" und "Prüfen". Wählen Sie nun "Systemfehler automatisch reparieren" und "Fehlerhafte Sektoren suchen/wiederherstellen".

Reparatur auch mit kostenloser Software möglich

Wählen Sie nun "Systemfehler automatisch reparieren" und "Fehlerhafte Sektoren suchen/wiederherstellen" aus. War die Überprüfung erfolgreich, wurden die beschädigten Daten wiederhergestellt. Hat das nicht geholfen, können Sie eine Reparatur auch mit einer kostenlosen Software vornehmen.

Dafür bietet sich beispielsweise das Programm "PC Inspector File Recovery" an, das vom Computer-Portal "Chip.de" gut bewertet wurde. Führen Sie damit eine Datenrettung durch, sichern Sie die Daten anschließend extern auf einer Festplatte und formatieren Sie Ihren USB-Stick, um erneuten Fehlermeldungen vorzubeugen.

USB-Stick reparieren: Alternativen

Wird Ihr USB-Stick nicht erkannt, kann das Fehlen eines passenden Treibers die Ursache sein. Im Normalfall wird der richtige Treiber sofort nach dem Einstecken des USB-Sticks installiert und gestartet.

Funktioniert das nicht, entfernen Sie den Stick und schließen Sie ihn an eine andere USB-Buchse an. Hilft das nicht, starten Sie Ihren Computer neu und versuchen es nochmal.

Sind Sie mit diesen Maßnahmen nicht erfolgreich, suchen Sie im Internet einen passenden Treiber für Ihr Gerät und installieren Sie ihn manuell. Möglicherweise behebt eine aktuellere Treiber-Version die Fehlfunktion.

Liegt ein Problem mit den mechanischen Komponenten Ihres USB-Sticks vor, können kaputte Lötstellen, Leiterbahnen oder elektronische Teile die Ursache sein. Sind Sie kein Hobby-Bastler, ziehen Sie unbedingt einen Fachmann hinzu, um die Schäden zu beheben.

So vermeiden Sie typische Fehler

Haben Sie es geschafft, Ihren USB-Stick zu reparieren, beugen Sie Fehlfunktionen in Zukunft vor. Verschließen Sie nach jeder Nutzung Ihren Stick mit der dafür vorgesehen Kappe, so schützen Sie ihn vor Staub, Nässe und direktem Sonnenlicht, die ihm schaden können.

Achten Sie darauf, dass der Stick weder beim Transport noch bei der Lagerung gequetscht wird. Vermeiden Sie außerdem Gewalteinwirkung beim Anstecken und Abziehen des Geräts.

Entfernen Sie Ihren USB-Stick immer erst dann von der USB-Buchse, nachdem Sie "Hardware sicher entfernen und Medium auswerfen" ausgewählt haben.

Sichern Sie wichtige Dateien regelmäßig und verwenden Sie Ihren USB-Stick lediglich zum Transport Ihrer Daten zwischen verschiedenen Endgeräten.

Quelle: https://www.t-online.de/digital/hardware/id_67094642/usb-stick-reparieren-so-geht-s.html

Allgemeines:

1) Diese Autoschlüssel-Funktion kennt nicht jeder: Kann Ihr PKW das auch?

Wie gut kennen Sie eigentlich Ihr Auto? Es gibt sicherlich die ein oder andere Funktion, die Sie noch nie ausprobiert haben. Dazu zählt ein Trick mit dem Autoschlüssel, der ziemlich praktisch ist und Zeit spart.

Kaum jemand liest sich das Handbuch des eigenen Autos bis ins kleinste Detail durch – und manche wissenswerte Tipps sind auch nur beiläufig oder überhaupt nicht erwähnt, obwohl sie im Alltag ziemlich praktisch sein können.
Einer davon betrifft Ihren Autoschlüssel, genauer gesagt die Fernbedienung zum Öffnen und Schließen des Fahrzeugs. Wer diesen Trick kennt, der macht sich das Leben vor allem bei sonnigem Wetter etwas leichter.

Autoschlüssel-Trick: Alle Fenster auf einmal öffnen

Viele Autohersteller haben in den Fernbedienungen des Schlüssels eine Funktion eingebaut, mit der sich alle Fenster auf einmal öffnen oder schließen lassen. Das ist etwa praktisch, wenn das Fahrzeug lange in der Sonne stand, denn so können Sie vor der Fahrt durchlüften, statt in einen sprichwörtlichen Backofen einzusteigen.

Der Trick funktioniert denkbar einfach: Sie müssen nur auf dem Autoschlüssel die **Öffnen-Taste so lange gedrückt halten**, bis die Fenster nach unten fahren. Sobald Sie loslassen, stoppt der Vorgang. Öffnen Sie also die Fenster nur einen Spalt oder komplett. Umgekehrt klappt es genauso, indem Sie die Schließen-Taste gedrückt halten.

Wichtig zu wissen: Der Trick klappt nicht mit jedem Auto, auch wenn Sie einen Schlüssel mit Fernbedienung dafür haben. Wichtig ist zum Beispiel, dass sich alle Fenster des PKW elektrisch öffnen und schließen lassen – sind hinten noch Fenster zum selbst kurbeln, dann wird es wahrscheinlich nicht klappen. Probieren Sie es einfach mal aus.

Quelle: https://www.chip.de/news/Diese-Autoschluessel-Funktion-kennt-nicht-jeder-Kann-Ihr-PKW-das-auch_184801183.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=23-05-2023%2B17%253A00%253A05&utm_content=nl_chipmob&utm_term=

2) 14 wichtige Tipps – Auto kaufen: Die fiesesten Abzock-Fallen umgehen

Jeder dritte Tacho ist manipuliert – und auch sonst sind viele Gebrauchtwagen nicht das, was der Verkäufer verspricht. Wie Sie die versteckten Hinweise darauf finden.

Wer sich beim Gebrauchtwagenkauf unsicher ist, kann eine Werkstatt oder seinen Automobilclub aufsuchen. Dort prüft ein Experte, ob der Gebrauchte etwas taugt. Aber erstens ist das nicht in jedem Fall möglich und zweitens auch nicht immer nötig. Denn viele

Schwächen können Sie selbst entlarven – wenn Sie wissen, worauf zu achten ist.

1. Lohnende Anreise

Ob sich eine lange Anreise zu einem Kaufangebot rentiert, hängt ganz vom Fahrzeug und Preis ab, so Marcel Mühlich vom Auto Club Europa (ACE). "Exoten oder spezielle Autos finden sich selten in der Nähe. Auch gibt es häufig regionale Preisunterschiede, daher kann sich eine weite Anreise durchaus lohnen."

2. Richtige Kontaktaufnahme

Wer ein passendes Angebot findet, sollte zuerst den Verkäufer kontaktieren, aber nicht unbedingt mitteilen, dass er von weiter weg anreist. "Das verschlechtert die Basis für die Preisverhandlung", sagt Mühlich.

3. Auf Unterschied zwischen Privat und Händler achten

"Privatverkäufer können die Sachmängelhaftung ausschließen, gewerbliche Verkäufer können das nicht", sagt Marcel Mühlich. Einige Händler wollen das umgehen, indem sie als Vermittler auftreten und das Auto "nur an Gewerbe", "für den Export" oder "im Auftrag" verkaufen. "Interessenten sollten davon die Finger lassen und besser weitersuchen", sagt Mühlich.

4. Nicht allein zum Kauf

Wer sich einen Gebrauchtwagen kaufen will, nimmt zur Besichtigung einen möglichst kundigen Begleiter mit. Dadurch sinkt das Risiko, sich blenden zu lassen.

Auch Jochen Kurz von Autoscout24 rät, zu einer Besichtigung zu zweit zu fahren: "Vier Augen sehen mehr als zwei, und der Begleiter kann vor Fehlkäufen warnen", sagt er. Vor Treffen an unbekannten, einsamen und dunklen Orten warnt der Experte, ebenso bei angeblichem Zeitmangel des Verkäufers. "Bei einer Besichtigung bei Tageslicht sollten beide Seiten ausreichend Zeit für Fragen und eine Probefahrt einplanen", sagt er.

ACE-Vertrauensanwalt Arndt Kempgens rät, darauf zu achten, wer überhaupt der Verhandlungspartner ist: "Wer zeigt mir das Auto? Halter, Fahrer, ein Freund des Halters? Das sollte zu Beginn der Besichtigung geklärt werden", sagt er. Danach folgen Fragen zum Verkaufsgrund, wie lange das Auto im Besitz war und zum Pflegezustand. "Die Geschichte muss passen, ebenso wie die Einträge im Scheckheft mit der Kilometeranzeige im Cockpit", sagt er.

Die gute Nachricht: Selbst Laien können einige Schwachpunkte eines Gebrauchtwagens erkennen. Zum Beispiel im Innenraum: Hinweise auf ein Qualitätsmanko können ein übermäßig abgegriffenes Lenkrad, stark verkratzte Oberflächen oder eine defekte Sitzverstellung geben. Wenn bereits der Innenraum ungepflegt ist, sollten Sie beim Rest des Autos umso genauer hinsehen.

Interessenten sollten auch im Serviceheft nachsehen, ob es Hinweise auf regelmäßige Wartung gibt. Noch besser allerdings sind dafür konkrete Rechnungen geeignet, weil die Arbeiten dort detailliert aufgelistet sind.

5. Gründliche Probefahrt

Zum Gebrauchtwagenkauf gehört eine gründliche Probefahrt. Sie sollte mit kaltem Motor beginnen und über ruhige Straßen, aber auch über Land führen. Denn manche Mängel verraten sich erst bei höheren Drehzahlen oder Geschwindigkeiten.

Der Motor sollte rund laufen und auf Befehle des Gaspedals gut ansprechen. Ein Knacken

beim Abbiegen mit vollem Lenkeinschlag könnte auf fehlerhafte Antriebswellen oder Radlager hinweisen. Kann das Auto die Spur nicht halten, dürfte etwas mit der Fahrwerksgeometrie nicht in Ordnung sein.

Wie lässt sich der Wagen schalten? Ohne Geräusche und leichtgängig? Gut. Eine schwache Leistung und ein Zur-Seite-Ziehen beim Bremsen wiederum machen auf Probleme aufmerksam.

6. Unterboden und Motorraum prüfen

Auch der Unterboden gibt wichtige Hinweise auf den Zustand des Autos. Hier können Beulen, Schleifspuren und Kratzer auf Aufsetzer hinweisen. Schweißspuren sind eventuell Folge reparierter Unfallschäden.

Auf einer Hebebühne lassen sich das Fahrwerk und die Auspuffanlage genauer ansehen. Die Abgasanlage sollte unter anderem weder Rost noch Risse aufweisen, intakt befestigt sein und nicht klappern. Prüfen Sie auch die **Reifen** auf Risse und auf ein genügend sowie gleichmäßig abgefahrenes Profil.

Unter der Motorhaube können auch Laien Mängel entdecken. Ölrückstände deuten beispielsweise auf undichte Motor- und Gehäuseteile. Achten Sie auf durchgescheuerte Kabel und gammelige Batterien. Weißlich eingetrocknete Spuren können auf undichte Kühlsysteme hinweisen.

Die Besichtigung machen Sie am besten bei Tageslicht und lassen sich nicht unter Zeitdruck setzen.

7. Auf ESP und Crashtest-Einstufung achten

Eine sogenannte Fahrdynamikregelung, auch bekannt als Elektonisches Stabilitäts-Programm (ESP), erhöht die Fahrsicherheit eines Autos enorm. Vor dem Jahr 2014 zugelassene Fahrzeuge hatten dieses Assistenzsystem aber zumindest in den unteren Fahrzeugklassen nicht unbedingt serienmäßig an Bord. Achten Sie darauf, ob ESP und gegebenenfalls weitere Sicherheitssysteme vom Spur- bis zum Notbremsassistenten vorhanden sind und auch funktionieren.

Laut der Dekra-Statistik sind im Schnitt bei mehr als jedem zehnten Fahrzeug im Alter von drei bis acht Jahren das ESP, die Airbags oder das Antiblockiersystem (ABS) nicht in Ordnung. Werkstätten können solche und andere Mängel bei einem Gebrauchtwagen-Check aufspüren.

8. Wurde der Tacho manipuliert?

Jeder dritte Tacho an Gebrauchtwagen ist manipuliert, schätzt die Polizei. Den Betrug zu erkennen, ist beinahe unmöglich. Es gibt aber Indizien. Wenn der Besitzer das Serviceheft (auch Checkheft oder Scheckheft genannt) nicht vorlegen kann, sollten Sie das Auto nicht kaufen. Aber auch hier fälschen die Betrüger. Falls beispielsweise alle Stempelabdrücke gleich aussehen, ist Skepsis geboten.

Im Idealfall sind zusätzlich Prüfberichte und Werkstattrechnungen sowie optimalerweise auch die Zettel der vorangegangenen Ölwechsel verfügbar. Denn auf letzteren sind in der Regel die Kilometerstände notiert. Hier kontrollieren die Käufer, ob die Zeit- und Kilometerangaben glaubwürdig sind. Der aktuelle Ölwechselzettel hängt meist im Motorraum. Ist der dort angegebene Stand des letzten Wechsels höher als der aktuelle Tachostand, ist der Betrug offensichtlich. Wenn der Wagen bereits in einer Vertragswerkstatt war, lassen sich dort unter Umständen die dort bereits hinterlegten Tachoangaben in Erfahrung bringen.

Ein stark verschlissener Innenraum, eine zu weiche Schaltung, sehr viele Kratzer auf Scheinwerfern und Frontscheibe – auch das sind Indizien für eine hohe Laufleistung des Autos.

9. Vorsicht bei zu verlockendem Angebot

Extrem günstige Angebote sollten generell skeptisch machen. Denn im Internet kann sich eigentlich jeder Verkäufer über das realistische Preisgefüge informieren. Gibt der Verkäufer einen guten Grund dafür an, warum er sein Auto etwa nach einer sehr kurzen Haltezeit schon wieder verkaufen will? Macht er generell einen seriösen Eindruck oder preist er das Auto überschwänglich an? Beantwortet er Fragen vernünftig oder hat er Ausreden?

10. Vertrag checken

Um die meisten Streitpunkte zu vermeiden, sollten Interessenten eine anerkannte Kaufvertragsvorlage etwa von Autoclubs wie dem ADAC oder den Gebrauchtwagen-Börsen ausdrucken und die zusammengetragenen Punkte beachten. Dabei unbedingt das Foto auf dem Ausweis mit dem Verkäufer abgleichen. "Ein vorläufiger Ausweis reicht nicht, da er leicht zu fälschen ist", sagt Kempgens.

"Alle Zusagen oder Vereinbarungen, die während der Besichtigung genannt werden, sollten schriftlich in den Kaufvertrag aufgenommen werden", sagt er. Bei Verträgen mit Händlern unbedingt darauf achten, dass Gewährleistung gegeben wird.

Bestehen Sie darauf, dass der Verkäufer den Kilometerstand verbindlich im Vertrag festschreibt. Formulierungen wie "soweit bekannt", "laut Vorbesitzer" und "wie abgelesen" streicht man besser. Empfohlen dagegen: "Der Tachostand entspricht der tatsächlichen Laufleistung des gesamten Fahrzeugs".

Dann können Sie das Auto unter Umständen zurückgeben oder den Preis mindern, wenn es sich als manipuliert erweist – aber eben nur dann.

11. Papiere kontrollieren

Unterlagen wie Fahrzeugschein und Fahrzeugpapiere kontrollieren Interessenten gründlich. "Stimmt die Fahrgestellnummer im Auto mit den Papieren überein? Ist der letzte Halter auch der Verkäufer, gibt es Vorschäden?", sagt Rechtsanwalt Kempgens.

"Je mehr Unterlagen wie Rechnungen von Reparaturen, Wartungen oder HU-Protokolle der Verkäufer zeigen kann, umso besser", sagt Marcel Mühlich. Damit lässt sich die Historie nachverfolgen und lassen sich eventuelle frisierte Kilometerangaben aufdecken.

12. Preisverhandlung

"Bei der Preisverhandlung rentiert es sich, wenn sich der Interessent neutral verhält", sagt Jochen Kurz. Mit einer vorherigen Preisrecherche hat man schon eine marktgerechte und realistische Preisidee. Bei der Besichtigung entdeckte Argumente für Preissenkungen, etwa Reparaturkosten sollten einfließen.

13. Bezahlung abwickeln

Am sichersten mit Bargeld. Beim Bezahlen schauen beide Seiten genau hin. Die Zahlung wird mit dem genauen Betrag im Kaufvertrag quittiert. Vor Vorabüberweisungen raten die Experten ebenso ab wie von Bezahlungen per Paypal-Konten.

14. Abmeldung/Ummeldung

Am sichersten ist es, das Auto abgemeldet zu verkaufen. In der Praxis werden gebrauchte

Autos von Privat aber meist mit gültigen Kennzeichen verkauft. "Daher unbedingt in den Kaufvertrag reinschreiben, bis wann das Auto umgemeldet werden muss", rät Kempgens.

Quelle: https://www.t-online.de/auto/technik/id_87742774/gebrauchtwagenkauf-die-besten-tipps-darauf-sollten-sie-achten-.html

3) Dieser Antrag verschafft Familien bis zu 240.000 Euro extra

Zwar gibt es das Baukindergeld nicht mehr, ab Juni soll aber dafür das neue Förderprogramm "Wohneigentum für Familien" starten. Dafür soll die KfW zinsgünstige Kredite bis 240.000 Euro bereitstellen.

Sich ein Eigenheim bauen, ist derzeit eine besonders teure Sache und das **Baukindergeld**, für das der Staat fast **10 Milliarden Euro** bereitgestellt hat, lässt sich nicht mehr anzapfen. Doch ein Nachfolger ist schon auf der Zielgeraden, eine Art Baukindergeld 2023, wenn auch unter anderem Namen.
Lang ist nicht mehr hin, bis zum geplanten **Förderstart im Juni 2023**. Bundesbauministerin Klara Geywitz hatte schon Anfang des Jahres eine neue Eigentumsförderung für Familien angekündigt.

Nach Wegfall des Baukindergelds will man über das Programm **Wohneigentum für Familien (WEF)** der Förderbank KfW vor allem Familien mit geringen bis mittleren Einkommen beim Kauf von selbstgenutztem Wohnraum unterstützen.
Bei der KfW läuft das Programm unter dem Kürzel **WEF (300)**. Bisher gibt es aber weder ein Merkblatt mit genauen Förderrichtlinien noch die Möglichkeit, Antragsformulare einzusehen. Doch wichtige Eckpunkte der neuen Förderung sind bereits bekannt.

Kredit statt Zuschuss

Der größte Unterschied zwischen Baukindergeld und WEF ist, dass es sich bei der neuen Förderung nicht um einen Zuschuss handelt. Vielmehr sollen Familien einen zinsgünstigen Kredit kriegen. Die genauen Konditionen dafür wurden bisher aber noch nicht veröffentlicht. Was bekannt ist:

- Berechtigt für die KfW-Förderung WEG (300) sollen Familien mit einem **Jahreseinkommen bis zu 60.000 Euro** sein.
- Für jedes weitere im Haushalt lebende, minderjährige Kind, darf das Jahreseinkommen 10.000 Euro höher liegen.
- Das Kreditvolumen soll insgesamt bei 350 Millionen Euro im Jahr liegen, maximal soll ein Kredit von **bis zu 240.000 Euro** je Antragsteller bereitstehen.
- Die Förderung gilt bei Neubauten oder Erstkauf, die mindestens den Standard Effizienzhaus 40 erfüllen, aber **nicht für Bestandsimmobilien**.
- Es gilt als wahrscheinlich, dass die KfW auch in diesem Fall Bau bzw. Kauf einschließlich Nebenkosten fördert sowie Kosten für Planung und Baubegleitung durch Experten für Energieeffizienz und Berater für Nachhaltigkeit sowie Nachhaltigkeitszertifizierung
- Antragsteller müssen die Immobilien selbst bewohnen, dürfen kein Baukindergeld in Anspruch genommen haben und müssen Eigentümer sein.

Wichtige Details fehlen noch

KfW-Fördermaßnahmen müssen in der Regel vorab beantragt werden. Wer also die neue Förderung zumindest prüfen möchte, sollte mit dem Abschluss eines Kaufvertrags noch warten, bis die Förderung gestartet ist und alle Details auf dem Tisch liegen.
Die neue Förderung soll sich mit anderen Fördermöglichkeiten kombinieren lassen.

Quelle: https://www.chip.de/news/Dieser-Antrag-verschafft-Familien-bis-zu-240.000-Euro-extra_184781683.html?utm_source=nl_chipd-wy&utm_medium=chip-newsletter&utm_campaign=21-05-2023%2B07%253A00%253A52&utm_content=nl_chipmob&utm_term=

4) Blackbox fürs Auto wird Pflicht – das sind die Folgen für Autofahrer

Jedes neue Auto besitzt bald einen Event Data Recorder (EDR), also eine Blackbox, in der alle Daten rund um einen Unfall gespeichert werden. Diese Daten können auch gegen den Willen des Fahrers ausgelesen werden.

Flugzeuge besitzen schon seit Ewigkeiten eine Blackbox, aus der Ereignisse vor und kurz nach einem Absturz ausgelesen werden können. Auch in Autos kommt so ein Gerät immer öfter zum Einsatz: Der sogenannte Event Data Recorder (EDR) zeichnet bei einem Unfall eine kurze Zeitspanne vor und nach dem Crash auf. Bereits jetzt sollen laut ADAC viele Fahrzeuge mit einem EDR ausgestattet sein, denn seit dem 6. Juli 2022 müssen alle neuen Fahrzeugtypen einen EDR besitzen.

Doch ab dem 7. Juli 2024 wird die Blackbox sogar für alle neu zugelassenen PKW und Nutzfahrzeuge bis 3,5 Tonnen Pflicht. Jeder Neuwagen muss also ab diesem Stichtag einen EDR besitzen. Für PKWs/Busse mit mehr als neun Sitzen und für LKWs, die mehr als 3,5 Tonnen wiegen, wird der EDR ab dem 7. Januar 2026 beziehungsweise ab dem 7. Januar 2029 Pflicht.

Die ohnehin schon recht schweren modernen Autos werden damit noch schwerer: Sicherheit macht Autos schwerer.

Das kann der EDR

Die Aufgabe des EDR soll darin liegen, ein besseres Verständnis über einen Unfall durch dabei aufgezeichnete Daten zu bekommen. Verbaut ist der EDR meistens im Airbag-Steuergerät, da hier alle relevanten Informationen von Beschleunigungssensoren zusammenlaufen – diese Informationen werden auch für die Auslösung der Datenaufzeichnung des EDR verwendet.

Der EDR zeichnet Daten auf wie die Geschwindigkeit, Motordrehzahl, Lenkwinkel oder ob der Airbag ausgelöst wurde. Die Aufzeichnung wird in einem zeitlichen Fenster von fünf Sekunden vor und 300 Millisekunden nach dem Crash ausgelöst.

Wo liegen die Daten und wie greift man darauf zu?

Die Daten werden lokal im Fahrzeug gespeichert und verbleiben dort. Sie sollen sich nicht online auslesen lassen. Mit Hilfe von bestimmten Tools können sie über die ODB-Schnittstelle oder direkt am Airbag-Steuergerät ausgelesen werden.

Wer hat Zugriff auf die Daten?

Zwar liegt datenschutzrechtlich die Hoheit der Daten aus dem EDR beim Fahrer bzw. Halter. Um im Zusammenhang mit zivil- oder strafrechtlichen Verfahren aber zu erfahren, wie es zu einem Unfall kam, kann ein Gericht oder die Staatsanwaltschaft einen Sachverständigen beauftragen, die Daten aus dem EDR auszulesen. Das darf dann auch gegen den Willen des Autofahrers passieren.

Der Fahrer selbst dürfte schon allein aufgrund der technischen Hürden am wenigsten auf “seine” EDR-Daten zugreifen können.

Jedem Autofahrer sollte klar sein, dass bei jeder HU-Prüfung oder jedem Werkstatt-Aufenthalt

ein Auslesen der EDR-Daten theoretisch möglich ist.

Die Daten aus dem EDR sollten jedoch nicht als einzige Quelle zur Unfallrekonstruktion hinzugezogen werden. Vielmehr dienen sie als zusätzliches Element zum Spurenbild am Unfallort sowie den Schäden an den beteiligten Fahrzeugen, wie der ADAC betont. So können sie die herkömmliche Rekonstruktion eines Unfalls unterstützen, nicht jedoch ersetzen. Der EDR speichert nur Daten über das eigene Fahrzeug und nicht über andere Verkehrsteilnehmer. Auch Videoaufzeichnungen sind mit ihm nicht möglich.

Ab 6.7.: Diese Systeme werden jetzt Pflicht im Auto – mehr Sicherheit & höhere Kosten

Lesetipp: Datenkrake Auto dient als Beweismittel gegen den Fahrer

Quelle: https://www.pcwelt.de/article/1916673/edr-blackbox-auto-ab-2024-pflicht.html?utm_date=20230525145319&utm_campaign=Security&utm_content=Title%3A%20Blackbox%20f%C3%BCrs%20Auto%20wird%20Pflicht%20%E2%80%93%20das%20sind%20die%20Folgen%20f%C3%BCr%20Autofahrer&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Punkte in Flensburg kostenlos online abfragen: So geht’s

Du bist dir nicht sicher, wie es um deine Verkehrssünderkartei steht? Wir zeigen dir, wie du deine Punkte in Flensburg ganz einfach kostenlos online abfragen kannst.

Zu Beginn dieses Jahres waren in Deutschland rund 48,76 Millionen Fahrzeuge zugelassen. Damit erreichte die Zahl der gemeldeten Pkw den höchsten Stand aller Zeiten.

Doch wer sich mit seinem Auto im Straßenverkehr bewegt, muss sich auch an zahlreiche Regeln halten. Denn bei Regelverstößen drohen Bußgelder oder sogar Punkte in Flensburg.

Die Verkehrssünderkartei, in der die sogenannten Punkte in Flensburg gesammelt werden, kann inzwischen sogar kostenlos online eingesehen werden. So kannst du prüfen, wie viele Punkte du tatsächlich hast.

So kannst du deine Punkte in Flensburg kostenlos online abfragen

In Deutschland können Behördengänge zunehmend auch digital erledigt werden. Das gilt inzwischen auch für das Fahreignungsregister. Denn auch beim Kraftfahrt-Bundesamt (KBA) kannst du deine Punkte in Flensburg kostenlos online abfragen.

Neben der Registerauskunft auf dem Postweg sowie vor Ort in Flensburg bietet die Online-Auskunft einen schnellen Überblick über die gesammelten Punkte. Die Auskunft ist für dich gebührenfrei und in nur wenigen Klicks erledigt.

Das benötigst du für die Auskunft

Willst du deine Punkte in Flensburg kostenlos online abfragen, benötigst du das erforderliche technische Equipment. Wie bei anderen Online-Behördengängen sind das:

- einen Online-Ausweis inklusive selbstgewählter sechsstelliger PIN
- ein NFC-fähiges Smartphone oder einen Kartenleser für den PC
- eine Software zum Auslesen des Online-Ausweises wie beispielsweise die AusweisApp2

Schritt für Schritt Punkte in Flensburg kostenlos online abfragen

Sind diese Voraussetzungen erfüllt, musst du nur noch wenige Schritte erledigen, um an deinen Punktestand zu gelangen. Rufe hierfür zunächst die Website für die Online-Registerauskunft auf.

Hier musst du dich nun authentifizieren. Dafür kommt die AusweisApp2 ins Spiel. Halte für diesen Schritt unbedingt auch deinen Personalausweis sowie deine PIN bereit.

Ist die Authentifizierung erfolgt, musst du diese mit einem Klick auf „Weiter“ bestätigen. Im Anschluss kannst du die Daten prüfen, die aus deinem Personalausweis ausgelesen wurden.

Nun musst du nur noch auswählen, welche Informationen du vom Kraftfahrt-Bundesamt erhalten möchtest. Diese werden dir dann als PDF-Datei zur Verfügung gestellt.

Die Auskunft ist gebührenfrei

Bitte beachte, dass die Auskunft beim Kraftfahrt-Bundesamt in jedem Fall gebührenfrei ist. Das gilt sowohl für die Online-Auskunft als auch für eine Abfrage auf dem Postweg oder vor Ort.

Solltest du im Netz auf kostenpflichtige Angebote stoßen, stammen die meinst von Drittanbietern. Diese verlangen Geld dafür, die Abfrage beim Kraftfahrt-Bundesamt für dich zu übernehmen.

Quelle: https://www.basicthinking.de/blog/2023/05/29/punkte-in-flensburg-kostenlos-online-abfragen/?utm_source=flipboard&utm_content=topic%2Fde-automobil