39. Cybercrime Newsletter

28.12.2023

1) Online-Shopping – Das sind die häufigsten drei Fallstricke bei Kleinanzeigen für Käufer und Verkäufer

Ein Artikel entpuppt sich als beschädigt, jemand erscheint nicht zum vereinbarten Termin oder Sie haben etwas verkauft, aber die Ware ist angeblich nicht angekommen: Das können Sie dann tun.

Wer sich online auf Schnäppchenjagd begibt, findet auf dem Portal Kleinanzeigen (ehemals Ebay-Kleinanzeigen) eine Menge Angebote – doch nicht immer läuft beim Kauf alles glatt: Was tun, wenn scheinbar heile Artikel Macken aufweisen, das Gekaufte nicht funktioniert oder wenn einem etwas doch nicht gefällt?

Christian Solmecke hat sich als Rechtsanwalt und Partner der Kölner Medienrechtskanzlei WBS.Legal auf das Thema Internetrecht und E-Commerce spezialisiert. Er kennt die häufigsten Fallstricke und klärt auf, welche Rechte man hat, wenn es einmal anders läuft als erhofft.

Vorab: Es macht einen Unterschied, ob man privat etwas verkauft und bei Privatleuten kauft, oder ob der Anbieter ein gewerblicher Händler ist. Die meisten Käufe bei Kleinanzeigen sind Privatkäufe. Nur weil einem ein Artikel nicht gefällt, ist eine Rückgabe dann nicht möglich. Anders sieht das bei gewerblichen Händlern aus: Bei ihnen können Käufer innerhalb einer 14-tägigen Frist Waren einfach zurückgeben.

Lesen Sie auch: Plötzlich muss Verkäufer bezahlen: Betrugsmasche kann Tausende Euros kosten

Fallstrick 1: Die Ware hat Mängel

Das Handydisplay hat Schrammen, der Pulli ein großes Loch unter dem Arm - doch davon war online nichts zu sehen? Wenn ein Verkäufer nicht auf solche Mängel hingewiesen hat, gilt der Artikel als mangelhaft. "Kann der Verkäufer nicht nachbessern, also den Artikel reparieren oder einen passenden zusenden, kann der Kauf rückabgewickelt werden", sagt Solmecke. Um Probleme bei der Rückzahlung des Kaufpreises zu vermeiden, empfiehlt der Anwalt, die Option "sicher bezahlen" zu nutzen, denn dann sei Kleinanzeigen bei der Rückabwicklung behilflich.

Die chinesische Vase kommt in 30 Scherben an: Wenn etwas kaputt ankommt, bleibt die Frage: Ist es auch defekt verschickt worden – oder erst beim Versand beschädigt worden? Der Rechtsexperte erklärt: "Kauft man von einem gewerblichen Verkäufer, trägt dieser das Risiko, dass beim Versand etwas schief geht."

Kommt die Ware beschädigt beim Käufer an, muss der Verkäufer einen heilen Artikel nachliefern oder Schadenersatz leisten. Der Käufer muss nur beweisen, dass der Artikel tatsächlich beschädigt angekommen ist. Anders ist das beim Privatkauf, denn dann liegt

das Risiko beim Käufer. "Der Verkäufer muss dann nur beweisen, die Ware heil losgeschickt zu haben", sagt Solmecke.

Und was passiert, wenn bei einer direkten Übergabe etwas kaputtgeht? Etwa beim Einladen von Möbeln? "Zwischen Käufer und Verkäufer kommt es primär darauf an, wer den Schaden verursacht hat: Wenn es der Verkäufer war, bleibt letztlich dieser auf dem Schaden sitzen, wenn es der Käufer war, dann er", sagt der Anwalt. Rechtlich mache es im Detail einen Unterschied, ob der Schaden vor oder nach Übergabe passiert sei. Auf den Kosten für die Schadenbeseitigung bleibe aber letztlich immer der Verursacher sitzen.

Fallstrick 2: Wo ist der gekaufte oder verkaufte Artikel überhaupt?

Was kann man tun, wenn man etwas gekauft hat – die Ware aber nicht kommt? "Rein rechtlich gesehen besteht dann ein Anspruch darauf, die Sache noch geliefert zu bekommen. Ist das nicht möglich oder weigert der Verkäufer sich, kann man vom Vertrag zurücktreten und Schadensersatz statt der Leistung verlangen", sagt Solmecke. Auch hier hilft es, die Option "sicher bezahlen" zu nutzen. Dann hilft die Plattform und schaltet sich ein. Wer die Option nicht nutzt, muss sich direkt mit dem Verkäufer auseinandersetzen.

Und was, wenn man als Verkäufer etwas verschickt – und der Käufer behauptet, das nicht bekommen zu haben? Hier lohnt sich Gründlichkeit als Verkäufer, sagt Solmecke. Ein gewerblicher Verkäufer trägt so oder so das Risiko des Verlustes auf dem Transportweg. Doch auch private Verkäufer müssen immerhin beweisen, dass sie das Paket versendet haben.

Lesen Sie auch: Betrug gehört zum Alltag und kann jeden treffen: Fünf wichtige Tipps

"Wegen solcher Fälle sollte man irgendwie vorher dokumentiert haben, dass man das Paket auch mit Inhalt versendet hat", rät der Anwalt. "Etwa durch Zeugen oder ein Foto des Pakets mit Inhalt am Postschalter." Zudem sollte man immer die Quittung mit der Sendungsverfolgungsnummer aufbewahren.

Kann man somit den Versand beweisen, hat der Käufer eines Privatkaufs das Nachsehen. "Kann der Verkäufer hingegen überhaupt nicht beweisen, das Paket versendet zu haben, sähe es vor Gericht schlecht aus. Wegen der Beweislastverteilung müsste er entweder das Produkt erneut senden oder Schadensersatz leisten", sagt Solmecke. Idealerweise wählt man ohnehin einen versicherten Versand, auch wenn der etwas teurer ist: Damit lässt sich ein Paket nicht nur rückverfolgen, sondern es ist auch versichert.

Fallstrick 3: Die direkte Übergabe scheitert trotz Vereinbarung

Nun hat man etwa extra ausgemistet, will sperrige Gegenstände loswerden, oder die Zeit drängt, weil der Umzugstermin ansteht – und der Käufer kommt nicht zum vereinbarten Termin und meldet sich nicht mehr. Was nun? Wer eine abgemachte Übergabe verzögert, handelt sich Konsequenzen ein. Das gilt für Käufer und Verkäufer gleichermaßen, erklärt Solmecke.

Wer etwas Gekauftes nicht zum vereinbarten Zeitpunkt abholt, gerät in einen sogenannten Annahmeverzug. Das heißt für ihn: Wenn die Ware beim Lagern jetzt beschädigt wird, hat er das Nachsehen. Der Verkäufer haftet nur bei Vorsatz und grober Fahrlässigkeit. Entstehen ihm durch die Aufbewahrung Kosten, kann er außerdem verlangen, dass der Käufer sie ihm erstattet. Er kann dem Käufer auch eine Frist setzen und dann vom Kauf zurücktreten. Bereits gezahltes Geld muss er dann zurückerstatten.

Natürlich haben umgekehrt auch Käufer Rechte, wenn ein Verkäufer zum vereinbarten Zeitpunkt nicht da ist oder gar abtaucht. Denn dann kommt der in Schuldnerverzug. Das heißt: Wer zum Beispiel Fahrtkosten hat, kann sie dem Verkäufer in Rechnung stellen.

"Daneben sollte man eine Frist setzen, innerhalb derer der Verkäufer die Ware übergibt. Passiert das nicht, kann man vom Vertrag zurücktreten", erklärt der Rechtsexperte.

Und was, wenn man die Bierzeltgarnitur für eine Feier gebraucht hätte, und sie nun gar nicht mehr benötigt? "Wenn man bereits bezahlt hatte, kann man sein Geld zurückverlangen", sagt der Experte. Eine Frist ist dafür dann nicht mehr nötig.

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/haeufigsten-fallstricke-kleinanzeigen-38878454

2) Verbraucherschützer warnen – Darum sollte man beim Onlineshop Temu vorsichtig sein

Die Onlineshopping-App von Temu stürmt die Charts der App-Stores. Hier bekommt man alles besonders billig. Und deswegen ist Vorsicht geboten.

Wer freut sich in Zeiten hoher Inflation und steigender Preise nicht über ein wahres Schnäppchen? Der Onlineshop Temu wirbt gerade wieder mit unglaublich niedrigen Preisen – und dem Slogan "Shoppe wie ein Milliardär!".

In den sozialen Netzwerken und per Onlinewerbung rührt das Unternehmen kräftig die Werbetrommel – mit Erfolg. Die App steht in den App-Stores von Apple und Google Play an erster Stelle der beliebtesten Anwendungen. Doch trotz der Beliebtheit des Onlineshops wird die Kritik daran immer lauter – auch von Verbraucherschützern aus Deutschland.

Kopfhörer für vier, Schallzahnbürste für fünf Euro

Wer sich auf der Website umschaut (man muss sich dafür zunächst registrieren), dem fällt schnell auf, wie unfassbar billig die Produkte sind. Es gibt Bluetooth-Kopfhörer, die gerade einmal knapp vier Euro kosten, T-Shirts für drei Euro, Schallzahnbürsten für fünf Euro.

Auch wenn sich manche über die extremen Schnäppchen freuen, werden andere bei solchen Preisen misstrauisch. Wie kann es sein, dass es eine Schallzahnbürste bei Temu für nur fünf Euro gibt, wenn sie woanders gut und gerne 100 Euro kosten kann?

Nutzer beschweren sich über schlechte Qualität

Die Antwort: Es handelt sich meistens um Billigware. Auf "Trustpilot" findet man viele Bewertungen, in denen über die mangelhafte Qualität der Produkte berichtet wird. In einigen Fällen funktioniere die Ware gar nicht, sei beschädigt oder kaputt.

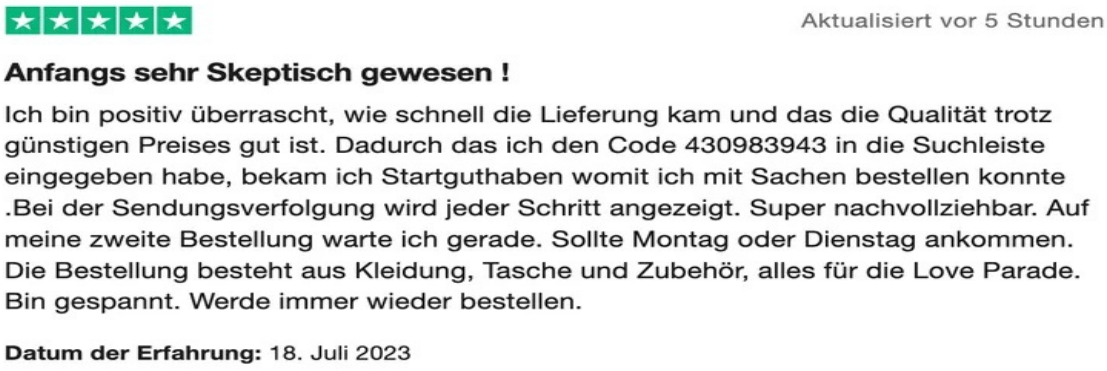
Quelle: Diese Nutzerin beschwert sich über Temu: Ihre Bestellung kam nicht an. (Quelle: Screenshot Trustpilot)

Einige Benutzer geben sogar an, auf Temu betrogen worden zu sein. Sie hätten ihre Bestellung bezahlt, die Ware sei allerdings nie angekommen. Auch über den "schlecht erreichbaren" Kundenservice hagelt es Beschwerden, ebenso wie über die unzähligen Mails mit Angeboten und Rabatten.

"Kundenservice nicht erreichbar"

"Ein Kundenservice ist meist so gut wie nicht erreichbar, schon gar nicht auf Deutsch. Und die Retoure nach China ist teuer und aufwendig und übersteigt in der Regel den Warenpreis", warnt die Verbraucherschutzzentrale Rheinland-Pfalz.

Doch es gibt auch viele positive Bewertungen auf "Trustpilot". Trotz der niedrigen Preise sei die Qualität gut, es gebe keine Lieferkosten, die Lieferung an sich sei schnell und der Kundenservice gut. Ob diese Kritiken echt sind, ist unklar. In auffällig vielen positiven Bewertungen findet sich ein Gutscheincode für den Onlineshop.



Aktualisiert vor 5 Stunden

Anfangs sehr Skeptisch gewesen !

Ich bin positiv überrascht, wie schnell die Lieferung kam und das die Qualität trotz günstigen Preises gut ist. Dadurch das ich den Code 430983943 in die Suchleiste eingegeben habe, bekam ich Startguthaben womit ich mit Sachen bestellen konnte .Bei der Sendungsverfolgung wird jeder Schritt angezeigt. Super nachvollziehbar. Auf meine zweite Bestellung warte ich gerade. Sollte Montag oder Dienstag ankommen. Die Bestellung besteht aus Kleidung, Tasche und Zubehör, alles für die Love Parade. Bin gespannt. Werde immer wieder bestellen.

Datum der Erfahrung: 18. Juli 2023

Quelle: Eine sehr positive Bewertung: Auffällig ist der Rabattcode. (Quelle: Screenshot Trustpilot)

Temu basiert auf Marktplatz-System

Schuld an den Kritikpunkten an Temu ist auch das System, das dahintersteckt. Denn es handelt sich hierbei weniger um einen klassischen Onlineshop als vielmehr um einen Internet-Marktplatz – ähnlich wie etwa AliExpress. Temu fungiert dabei sozusagen als Vermittler zwischen den Kunden und den Händlern, die meistens in China sitzen.

Oft bieten diese Marktplätze Waren aus allen möglichen Bereichen an – von Elektronik über Mode bis hin zu Möbeln. Dieses riesige Angebot ist auch möglich, weil diese Anbieter keine eigenen Lager haben. Der Kunde bestellt zwar auf Temu, kauft aber eigentlich Produkte von einem dritten Händler.

Verbraucherschützer: Bei Nutzung der App ist Vorsicht geboten

Das heißt eben auch, dass Temu oder andere Internet-Marktplätze die Qualität der angebotenen Waren nicht überprüfen können, da sie mit ihnen nicht in Kontakt kommen. Bei einer großen Website mit einem solch enormen Angebot können sich auch Betrüger einschleichen und von dem Hype um die App profitieren.

In Sachen Temu-App warnen die Verbraucherschützer aus Mainz: "Es sollte misstrauisch machen, dass eine Shopping-App Zugriff auf Kamera, Mikrofon, Fotos und das Adressbuch der Nutzer verlangt. Denn diese Daten sind zum Beispiel für die Funktion der App gar nicht erforderlich."

Wer also wirklich mal "wie ein Milliardär" shoppen will, sollte vorsichtig sein. Auch wenn Temu an sich keine Abzock-Website ist, besteht ein gewisses Risiko, dass man doch in eine Falle tappt oder ein Produkt von minderwertiger Qualität erhält. Braucht man eine neue Schallzahnbürste oder Bluetooth-Kopfhörer, ist man besser beraten, solche Geräte in einem Fachgeschäft zu kaufen.

Tipp: Bestellungen aus China: China-Shop Temu: So viel kostet der Zoll

Quelle: https://www.t-online.de/digital/internet/id_100210460/temu-bei-diesem-online-shop-sollten-sie-vorsichtig-sein.html

3) Dringende Warnung an Android-Nutzer: Fiese Malware greift Ihre Banking-PINs ab

Eine überarbeitete Android-Malware greift die PINs von Nutzern ab. Dabei stehen offenbar vor allem Banking-Apps im Fokus.

Sicherheitsexperten schlagen Alarm: Die neueste Version des Android-Banking-Trojaners "Chameleon" setzt auf raffinierte Techniken, um Fingerabdruck- und Gesichtserkennung auszuschalten.

Über den Tarn-Dienst Zombinder, getarnt als Google Chrome, schleust sich die Malware unauffällig in legitime Android-Apps ein. Opfer werden zunächst nichts von der Bedrohung ahnen, während ihre PINs gestohlen werden. Besonders Banking-Apps scheinen hier im Fokus zu stehen.

Gefahr für Android-Nutzer: Trojaner blockiert Fingerabdruck- und Gesichtserkennung

Die Experten von Threat Fabric, die den Trojaner entdeckt haben, berichten, dass hierbei ein raffinierter HTML-Seiten-Trick zum Einsatz kommt. Dieser ermöglicht es, auf den Eingabehilfe-Dienst von Android zuzugreifen.

Sobald dieser infiltriert ist, blockiert der Trojaner die biometrischen Verfahren wie Fingerabdruck- und Gesichtserkennung, zwingt den Nutzer zur Eingabe seiner PIN und überträgt diese heimlich an die Angreifer. Das Ergebnis: Unbekannte können das Gerät aus der Ferne entsperren und darauf zugreifen.
Diese Entwicklung stellt eine erhebliche Bedrohung für die Sicherheit von Android-Nutzern dar.
Um sich zu schützen, sollten Nutzer regelmäßige Sicherheitsupdates installieren, verdächtige Aktivitäten überwachen und Antivirenprogramme nutzen.

Tipp: Virenscanner chancenlos: Vorsicht vor dieser perfiden Malware-Masche

Quelle: https://www.chip.de/news/Android-Nutzer-aufgepasst-Diese-Malware-greift-PINs-ab_185081694.html

4) Parkschein-App – Cyberangriff: Easypark-Kunden müssen mit Phishing rechnen

Datenklau bei der Parkschein-App Easypark: Hacker haben bei einem Cyberangriff Kundendaten gestohlen. Worauf App-Nutzer jetzt achten sollten.

Beim Anbieter der Parkschein-App Easypark wurden digitale Kundendaten gestohlen. Das Unternehmen selbst benennt in einer Mitteilung einen Cyberangriff als Ursache für den Datenschutz-Zwischenfall und rät Kundinnen und Kunden, nun ganz besonders auf der Hut vor Phishing-Angriffen zu sein. Was Phishing genau ist und wie Sie die Gefahr erkennen, lesen Sie hier.

Die Hacker hatten womöglich Zugriff auf Kontaktinformationen wie Namen, Telefonnummer, Anschrift oder E-Mail-Adresse. Zudem seien einige Ziffern der zum Zahlen des Parkvorgangs hinterlegten Kreditkarte, Debitkarte oder IBAN abgeflossen, heißt es von Easypark.

Kein Betrug mit Zahlungen möglich

Mit diesen unvollständigen Informationen sei es aber nicht möglich, Zahlungen vorzunehmen, heißt es auf einer Info-Seite, die das Unternehmen zu dem Zwischenfall eingerichtet hat.

Zudem seien keine Daten zu Standorten, Parkvorgängen oder registrierten Fahrzeugen abgegriffen worden. Es habe auch keine unberechtigten Parkvorgänge gegeben.

Betroffene Kundinnen und Kunden sollen per Info-Banner beim Öffnen der App bereits über den Vorfall informiert worden sein oder noch informiert werden.

Quelle: https://www.t-online.de/digital/aktuelles/id_100305542/easypark-von-cyberangriff-betroffen-kunden-muessen-mit-phishing-rechnen.html

5) DHL-Kunden müssen vorsichtig sein: Betrüger nutzen fiesen Trick zur Tarnung

Sie erwarten ein Paket, das mit DHL Deutsche Post zugestellt wird? Vorsicht! Betrüger nehmen derzeit mit einem fiesen Trick DHL-Kunden ins Visier.

DHL-Kunden sollten in diesen Tagen besonders wachsam sein. Denn Cybergangster versuchen DHL-Kunden auf betrügerische Webseiten zu locken, auf denen diese dann vertrauliche Daten eingeben sollen. Davor warnt die Verbraucherzentrale Schleswig-Holstein.

Der Betrugsversuch kommt wie so oft per Mail. Die Mails haben den Betreff “Sie haben ein Paket, das zugestellt werden muss”. Das typische gelbe Banner mit dem roten DHL-Schriftzug ziert die Mail.

Im eigentlichen Text steht dann, dass die Lieferadresse aktualisiert werden müsse. DHL könne ein Paket nicht zustellen, weil die Lieferadresse falsch sei. Darunter folgen Details zum angeblichen Paket, wie der Liefercode und die Angabe einer Rücksendegebühr.

Rücksendegebühr als clevere Tarnung

Um die Lieferadresse jetzt korrigieren zu können, solle man auf den Link “Nachlieferung” klicken. Dieser befindet sich auf einem roten Button in der Mail. So weit entspricht das alles einer typischen Phishingmail. Doch in diesem Fall tarnen sich die Betrüger clever.

Denn die Gangster versuchen der Mail einen besonders glaubhaften Anschein zu verleihen, indem sie in die Mail schreiben, dass eine Rücksendegebühr in Höhe von 2,99 Euro anfallen würde. Diese sei erforderlich, um die Kosten für die erneute Zustellung abzudecken. Das klingt auf den ersten Blick plausibel und zudem passt das Fordern einer zusätzlichen Gebühr nicht zu einer typischen Phishingmail, die es dem Opfer ja eigentlich besonders einfach machen soll in die Falle zu tappen.

So erkennen Sie den Betrug

Erste Hinweise dafür, dass diese Mail nicht von DHL stammt, sind die fehlende persönliche Anrede und die fehlerhafte Absenderadresse – hier gilt wie immer: Führen Sie den Mauszeiger über die in Ihrem Mailprogramm angezeigte Absenderadresse, um die tatsächliche Mailabsenderadresse angezeigt zu bekommen. Ebenso ist der Link hinter dem roten Button mit der Aufschrift “Nachlieferung” falsch.

DHL betont:

- Offizielle DHL Mitteilungen werden immer von @dhl.com, @dpdhl.com, @dhl.de, @dhl.fr oder einer auf @dhl folgenden anderen Landesdomäne versandt.
- DHL verlinkt nur auf seine eigene Website, die beispielsweise mit https://dhl.com/, https://dpdhl.com/ oder einer Landes-/Kampagnen-Website beginnt.

DHL bittet betroffene Nutzer derartige Phishingmails folgendermaßen weiterzuleiten: Ziehen Sie die verdächtige E-Mail per Drag & Drop in eine neue Mitteilung und senden sie als

Anhang an phishing-dpdhl@deutschepost.de. DHL benötigt den vollständigen Mail-Header, um den Betrug beenden zu können. Dieser Header ist in einer weitergeleiteten Mail nicht enthalten.

In jedem Fall sollten Sie diese Mail löschen und nichts darin anklicken.

Quelle: https://www.pcwelt.de/article/2173095/dhl-kunden-phishing-betrug.html?utm_date=20231227151010&utm_campaign=Security&utm_content=Title%3A%20DHL-Kunden%20m%C3%BCssen%20vorsichtig%20sein%3A%20Betr%C3%BCger%20nutzen%20fiesen%20Trick%20zur%20Tarnung&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) Fakeshop-Finder: So entlarven Sie sofort betrügerische Online-Shops

Nutzen Sie einen kostenlosen Fakeshop-Finder, bevor Sie online in einem Shop einkaufen. So geht's.

Gerade in der Vorweihnachtszeit kauft man viel online ein. Doch welcher Online-Shop ist seriös und wo droht Abzocke? Bereits seit einiger Zeit bieten Verbraucherzentralen so genannte Fakeshop-Finder an, mit denen Verbraucher herausfinden können, ob ein Online-Shop zuverlässig und seriös oder aber kriminell ist.

Solche Fakeshop-Finder finden Sie beispielsweise hier bei der Verbraucherzentrale Niedersachsen und hier bei der Verbraucherzentrale Bundesverband. Die Funktionsweise ist immer die Gleiche: Sie geben die Webadresse des ins Auge gefassten Webshops ein und klicken auf “Shop-URL prüfen”.

So läuft die Prüfung

In Sekundenschnelle sehen Sie das Ergebnis. Ein Button zeigt farbig an, ob ein Risiko besteht: Grün bedeutet, dass der Shop sicher ist und bisher nicht negativ aufgefallen ist. Gelb bedeutet, dass sich der Shop nicht eindeutig bewerten lässt und bisher weder auf Fakeshop-Listen noch als vertrauenswürdiger Shop auf einer Whitelist eingetragen ist. Der Nutzer muss selbst wichtige Details prüfen. Rot bedeutet, dass der Online-Shop schon einmal als Fakeshop aufgefallen ist und auf entsprechenden Listen eingetragen ist. Sie sollten in diesem Fall von einem Einkauf dort Abstand nehmen.

Unter dieser Einstufung nach Ampelfarben folgt dann eine ausführliche Bewertung des Online-Shops. So bewertet das Tool die Versand- und Rücksendemöglichkeiten und überprüft, ob ein Impressum vorhanden ist. Zudem gleicht der Fakeshop-Finder die eingegebene URL mit unterschiedlichen Listen wie zum Beispiel Trustpilot ab, ob diese darin eingetragen sind und wie die URL dort bewertet wird. Außerdem prüft das Tool diverse technische Merkmale wie zum Beispiel das Land, in dem die Webseite gehostet ist.

So funktioniert der Fakeshop-Finder

> Basis des Fakeshop-Finders ist eine Domain-Datenbank, die mittels einer künstlichen Intelligenz stetig wächst. Wird eine Internetadresse eingegeben, die noch nicht bekannt ist, wird die Website auf verschiedene Merkmale gescannt. Dazu gehören neben Impressum und korrekter Umsatzsteuer-ID auch etwa technische Merkmale, die mit bloßem Auge nicht zu erkennen sind. Die daraus errechnete Wahrscheinlichkeit, ob es sich womöglich um einen unseriösen Anbieter handelt, gibt der Fakeshop-Finder in den Ampelfarben aus – ergänzt um Erklärungen zu den einzelnen Ergebnissen. Für Verbraucherinnen und

Verbraucher ist so schnell erkennbar, ob sie einem Shop vertrauen können oder ihn genauer prüfen beziehungsweise besser nicht nutzen sollten.

Verbraucherzentrale Niedersachsen

Tipp: https://www.verbraucherzentrale-niedersachsen.de/fakeshop-finder
https://www.verbraucherzentrale.de/fakeshopfinder-71560

Quelle: https://www.pcwelt.de/article/2172931/fakeshop-finder.html?utm_date=20231227151551&utm_campaign=Security&utm_content=Title%3A%20Fakeshop-Finder%3A%20So%20entlarven%20Sie%20sofort%20betr%C3%BCgerische%20Online-Shops&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Spam-Liste für Dezember – Blockieren Sie diese fünf Nummern am besten sofort

Die nervigsten Spam-Anrufe kommen immer öfter aus Großbritannien. Um einer Abzock-Falle zu entgehen, sollten Sie diese fünf Nummern gleich blockieren.

Nach Hamburg und Berlin in den vergangenen Monaten kommen diesmal die drei nervigsten Spam-Anrufe aus Großbritannien. Das zeigen die jüngsten Zahlen von Clever Dialer. Die Anrufer bedrängten deutsche Bürger "mit massivem Telefonterror und unfreundlichen Anrufen", heißt es.

Clever Dialer unterstützt mit seiner App ("cleverdialer.app") Nutzer bei der Erkennung und Abwehr von ungewollten und betrügerischen Anrufen. Monatlich gibt das Unternehmen t-online die häufigsten Spam-Nummern weiter, die bei seinen Kunden zu Ärger führen.

In der Top 5 der nervigsten Anrufe befindet sich aber auch eine Nummer aus Deutschland. Bei der Nummer mit Frankfurter Vorwahl soll es sich um eine Abzockmasche handeln, berichtet Clever Dialer. Wie bereits in den vergangenen Monaten sei den Gaunern jedes Mittel recht, um irgendwie an die sensiblen Daten der Nutzer zu gelangen, heißt es weiter.

Auffällig: 68 Prozent der gemeldeten Anrufe seien vom Festnetz ausgegangen und 32 Prozent kamen aus dem Mobilfunknetz.

Die Top 5 der Spam-Nummern im November 2023

Von den folgenden Nummern erfolgten im November die meisten Spam-Anrufe.

(Quelle: Clever Dialer)

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

- +447851397260 (Kostenfalle)
- +447707527817 (Kostenfalle)
- +447565591602 (Kostenfalle)
- 069957996610 (Kostenfalle)
- +447762383547 (Kostenfalle)

So können Sie eine Telefonnummer sperren

Die hier genannten Nummern können Sie getrost sperren. Wie das funktioniert, erfahren Sie Schritt für Schritt in dieser Anleitung. Generell gilt: Wirkt ein Anrufer unseriös oder sollen Sie einer unbekannten Person persönliche Daten wie Adresse, Kontonummer, ein Kennwort oder gar TAN-Nummern nennen, legen Sie umgehend auf. Geben Sie die Daten auf keinen Fall weiter. Wichtig auch: Bei unbekannten Nummern sollten Sie im Gespräch ein Wort niemals sagen – welches das ist, erfahren Sie hier.

Tipp:

- Gewinnspiele oder teure Verträge: Spam-Falle: So beenden Sie Abzock-Anrufe
- Aktuelle Liste: Das steckt hinter den nervigen Spam-Anrufen
- Anleitung: So blockieren Sie nervige Spam-Anrufe

Quelle: https://www.t-online.de/digital/aktuelles/id_100296180/fremde-telefonnummern-wie-sie-spam-anrufer-blockieren.html

8) Neue Betrugsmasche – Betrüger locken Apple-Nutzer mit E-Mails in die Falle

Cloud-Dienste bieten Speicherplatz für Bilder und Dokumente. Doch aktuell versuchen Kriminelle, Nutzer des Apple-Dienstes iCloud zu betrügen.

Auch wenn Handys, Computer und andere Geräte heutzutage oft schon einen großen eingebauten Speicher haben, wird es manchmal doch knapp. Cloud-Speicherdienste können da Abhilfe schaffen und mehr Platz für Fotos, Videos und Dokumente bieten.

Viele Apple-Nutzer greifen auf den firmeneigenen Service iCloud zurück – der zurzeit im Mittelpunkt einer Betrugsmasche steht, vor der das Landeskriminalamt Niedersachsen warnt. Cyberkriminelle verschicken einer Pressemitteilung zufolge massenhaft E-Mails, die vermeintlich von Apple stammen.

Nutzer werden in den Nachrichten darauf hingewiesen, dass ihr iCloud-Speicher voll sei – so, wie es auch bei Apple tatsächlich üblich ist. Ihnen wird darin ein kostenloses oder kostengünstiges Upgrade angeboten. Teilweise sehen die E-Mails, von denen dem LKA Niedersachsen zufolge mehrere Versionen in Umlauf sind, sehr überzeugend aus.

iCloud-Betrug: Das rät die Polizei

Klickt man allerdings auf den Link, der einen zur iCloud-Webseite weiterleiten soll, landet man auf einer gefälschten Seite, auf der die Kriminellen nicht nur die Zugangsdaten zum Apple-Konto (Apple-ID), sondern auch Kreditkartendaten stehlen wollen.

In der Folge hätten die Angreifer nicht nur das Apple-Konto gekapert, sondern würden auch versuchen, Kreditkartenzahlungen vorzunehmen und ihre Opfer dazu zu bewegen, die Zahlungen freizugeben, so die Verbraucherschützer von"Watchlist Internet"

Wer auf diesen Betrug hereingefallen ist, sollte sich bestenfalls an den Apple-Support wenden und seine Apple-ID ändern, damit sich Kriminelle mit den gestohlenen Zugangsdaten nicht anmelden können. Wurden etwa Kreditkartendaten eingegeben, sollte man sich unverzüglich an seine Bank wenden und die Karte sperren lassen, wie die Polizei in der Pressemitteilung erklärt. Zudem wird Opfern dazu geraten, Anzeige zu erstatten.

Wer die betrügerische E-Mail erhalten hat, sollte nicht auf den Link klicken und den Absender blockieren. Wurde bei Accounts noch keine Zwei-Faktoren-Authentifizierung eingerichtet, sollte das nachgeholt werden. Dann können sich Angreifer selbst mit abgefischtem Passwort nicht beim Nutzerkonto anmelden.

Wer bei Apple über 50 Gigabyte (GB) Online-Speicher verfügen möchte, muss dafür übrigens monatlich rund einen Euro bezahlen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100206870/icloud-betrug-polizei-warnt-apple-nutzer-vor-betrugsmasche.html

9) Der "nigerianische Prinz" war gestern – Verbraucherzentrale warnt vor neuer Betrugsmasche

Erbe, Spende, Investment: Die Verbraucherzentrale NRW warnt vor neuen Maschen mit dem sogenannten Vorschussbetrug. So können Sie sich schützen.

Die Verbraucherzentrale NRW macht auf neue Betrugsmaschen aufmerksam. Diese fallen unter den Begriff "Vorschussbetrug". Dabei handelt es sich um verschiedene Methoden von Kriminellen, die alle eins wollen: unser Geld.

Die Herangehensweise ist dabei immer ähnlich: Menschen werden über Kettenbriefe per E-Mail oder direkte Nachrichten in den sozialen Netzwerken kontaktiert. Es werden ihnen Erbschaften, Spenden oder vermeintlich lukrative Geschäfte in Aussicht gestellt. Allerdings seien diese frei erfunden und sollen dazu dienen, "ein illegales Schneeballsystem zu finanzieren", so die Verbraucherzentrale NRW.

Vor ein paar Jahren war die gleiche Betrugsmasche als "nigerianischer Prinz" bekannt und für die Kriminellen unglaublich erfolgreich. Heute sind die ausgedachten Geschichten anders, doch das System ist gleich geblieben. Denn: Wer auf die Verbrecher eingeht, wird an irgendeinem Punkt der Geschichte gebeten, zunächst Geld vorab zu zahlen.

In jedem Fall soll eine Vorabzahlung getätigt werden

Laut Verbraucherzentrale NRW ist eine beliebte Behauptung der Betrüger zum Beispiel, man müsse "vorab die Mehrwertsteuer oder andere Steuern bezahlen, um Geld aus dem Ausland erhalten zu können". In einem der anderen Tricks solle das vorab gezahlte Geld dazu dienen, die Glaubwürdigkeit zu prüfen.

Manchmal schieben die Kriminellen auch Gründe vor, warum sie weitere Vorabzahlungen benötigen. Der Ausgang der Geschichte bleibt aber in jedem Fall gleich: Das Geld ist futsch. Außerdem bricht der Kontakt zu dem vermeintlichen Vermögensverwalter – oder wer auch immer die Person vorgibt zu sein – komplett ab.

So können Sie sich schützen

Am besten ist es daher, gar nicht erst auf solche Nachrichten einzugehen. Auch wenn die Geschichte als noch so glaubhaft erscheint, stecken dahinter Kriminelle, die es auf Ihr Geld abgesehen haben. Daher sollten Sie die Absender auch blockieren.

Sollten Sie auf die Masche hereingefallen sein, erstatten Sie unbedingt Strafanzeige bei der

Polizei – entweder vor Ort oder über die entsprechende Internetwache in Ihrem Bundesland. In diesem Fall sollten Sie die Nachrichten oder den Chatverlauf zwischen Ihnen und den Betrügern unbedingt aufheben, diese dienen als wichtiges Beweismittel.

Tipp:

- Inhalte immer professioneller: Immer mehr Betrugs-E-Mails
- Betrugsversuch: Phishingmail melden – so geht's
- Betrugsnachrichten: Phishing-Mail geöffnet? – Das können Sie jetzt tun

Quelle: https://www.t-online.de/digital/aktuelles/id_100295220/vorschussbetrug-verbraucherzentrale-warnt-vor-neuen-maschen.html

10) Vorsicht vor Jobangeboten – Warnung vor neuer Betrugsmasche per SMS und WhatsApp

Wenn Sie in den nächsten Tagen eine bestimmte SMS oder WhatsApp-Nachricht erhalten, sollten Sie diese umgehend löschen. Auch wenn das Angebot noch so gut klingt.

Bis zu 1.000 Euro am Tag von zu Hause aus verdienen und dafür lediglich ein paar Hotels bewerten? Das Jobangebot, das bei einigen Verbrauchern in den letzten Tagen als SMS oder WhatsApp-Nachricht einging, klingt für viele zu gut, um wahr zu sein. Und die Skepsis ist berechtigt. Denn dahinter steckt nicht etwa wie in der Nachricht angegeben eine Online-Personalvermittlungsagentur, sondern Kriminelle.

Worum geht es genau?

Aktuell kursiert eine neue Scamming-Methode. Dabei werden Nachrichten via SMS oder WhatsApp versendet, in denen eine Online-Personalvermittlungsfirma angibt, auf den Lebenslauf des Empfängers aufmerksam geworden zu sein. Ihm möchte das Unternehmen daher einen Teilzeitjob anbieten, der in der Freizeit und von zu Hause aus ausgeübt werden könne. Der tägliche Verdienst dafür läge bei bis zu 1.000 Euro. Um den Job anzunehmen, müsse der Empfänger lediglich eine WhatsApp-Nachricht an eine bestimmte Nummer senden – und über 20 Jahre alt sein.

Die unabhängige Informationsplattform "watchlist-internet.at" geht davon aus, dass Verbraucher mit der Nachricht auf eine Plattform gelockt werden sollen, auf der sie sich dann registrieren müssen. Dabei könne es sich unter anderem um die Seiten depopnr.com, kaykaorg.com, oder privko.live handeln, so "watchlist-internet.at". Anschließend müssten die Verbraucher entsprechende Bewertungen abgeben, damit sie hierfür Geld bekommen, heißt es weiter. "Oftmals wird Ihnen vorgegaukelt, dass Sie für ein bekanntes Unternehmen arbeiten. Missbraucht werden zum Beispiel Unternehmen wie Willhaben, Otto, Zalando oder Expedia."

So funktioniert die Scamming-Methode

Zwar sieht der Nutzer dann, dass mit jeder erfüllten Aufgabe der Geldbetrag auf seinem Onlinekonto bei der Bewertungsplattform wächst, doch sobald er sich diesen Lohn auszahlen lassen möchte, komme es zu Problemen: Entweder muss der Nutzer erst Geld einzahlen, damit ihm sein Guthaben ausgezahlt werden kann, oder sein Guthaben sinkt vorher aus unerklärlichen Gründen in den Minusbereich und muss erst durch eine Einzahlung mit (echtem) Geld ausgeglichen werden, ehe es überwiesen werden kann. In beiden Fällen heißt es seitens der Bewertungsplattform, dass das eingezahlte Geld wieder erstattet wird. Das ist jedoch nicht der Fall. Meist erhält das Opfer weder den Lohn für die Tätigkeit noch sein eingezahltes Geld zurück.

Woher haben die Kriminellen meine Handynummer?

Durch Datenlecks kommen Kriminelle oft an die Smartphone-Nummern und/oder E-Mail-Adressen ihrer Opfer. Teilweise werden die Telefonnummern auch automatisch von einem Programm erstellt und quasi nacheinander abgearbeitet.

Wie erkenne ich eine Scamming-Nachricht?

In diesem Fall ist es einfach: die Grammatik und Logik: "Unsere Aufgabe ist einfach: Wir bewerten einfach Ihre Lieblingshotels". Wenn es eine Tätigkeit ist, die der Empfänger ausüben soll, weshalb übernimmt dann die Personalvermittlungsfirma die Bewertung? Und woher weiß sie, was die Lieblingshotels des Empfängers sind? Wer kurz über den Inhalt und seine Logik sinniert, kann darauf kommen, dass es sich um eine Phishing-Methode handelt.

Die Indizien sind jedoch nicht immer so eindeutig. Spätestens, wenn Sie auf eine andere Plattform wechseln oder persönliche Daten wie Name, Adresse, E-Mail-Adresse, Telefonnummer oder Ihre IBAN preisgeben sollen, sollten Sie stutzig werden. Darüber hinaus ist es äußerst selten, dass eine Online-Personalvermittlungsfirma Jobangebote per SMS oder WhatsApp auf gut Glück verschickt. Sollte es ein Recruiter wirklich auf Sie abgesehen haben, wird er Sie eher anrufen und Ihnen auch genau mitteilen können, woher er Ihre Daten hat und weshalb Sie für das Stellengesuch geeignet sind.

Jobbörsen warnen vor Job-Scamming

Bereits seit 2017 gibt es Betrugsnachrichten mit gefälschten Jobangeboten – sowohl per SMS als auch WhatsApp, Facebook-Messenger, Signal oder Nachricht bei den entsprechenden Internet-Jobbörsen. So warnte bereits Stepstone vor Job-Scamming. "Die Betrüger geben sich oft als potenzielle Arbeitgeber oder Online-Jobportale aus und locken ihre Opfer mit vermeintlich lukrativen Jobangeboten.

Sie nutzen die vertraute Umgebung von WhatsApp, um persönliche Informationen wie Adresse, Geburtsdatum oder sogar Bankdaten zu erschleichen", heißt es dort. "Sei besonders wachsam, wenn du Nachrichten von unbekannten Kontakten erhältst, die dich sofort mit Jobangeboten überhäufen." Denn seriöse Arbeitgeber kommunizieren nicht über WhatsApp und Co., bevor ein persönliches Kennenlernen stattgefunden habe.

Tipp:

- Sparsam mit Daten: Sieben Tipps gegen Identitätsdiebstahl

Quelle: https://www.t-online.de/digital/aktuelles/id_100294086/warnung-vor-betrugsmasche-job-scamming-angebote-via-sms-und-whatsapp.html

11) "Sofort löschen" – Krankenkasse AOK warnt vor Betrugsversuchen per SMS

AOK-Versicherte aufgepasst. Zurzeit versuchen Betrüger per SMS, an Ihre Daten zu gelangen.

Die AOK hat vor Betrugsversuchen per SMS gewarnt. Versicherte in Sachsen-Anhalt würden derzeit immer wieder aufgefordert, einen Link ("erneuerung-aok.com") anzuklicken, um angeblich eine neue Gesundheitskarte zu beantragen, teilte die AOK Sachsen-Anhalt am Freitag mit. In anderen Fällen würden die Versicherten aufgefordert, ihre Krankenkassendaten zu ändern.

Die AOK empfiehlt, die Nachrichten nicht zu beantworten und umgehend zu löschen. "Wir kommunizieren mit unseren Versicherten nicht per SMS", erklärt Sprecherin Anna Mahler. Die

Krankenkasse rufe entweder an, sende eine verschlüsselte E-Mail oder nehme über das gesicherte Kundenportal oder per Brief Kontakt auf. Die AOK betreut in Sachsen-Anhalt nach eigenen Angaben rund 830.000 Versicherte.

Grundsätzlich sollten Versicherte niemals persönliche Daten am Telefon oder im Internet preisgeben oder E-Mail-Anhänge öffnen, wenn ihnen der Absender nicht bekannt ist, rät die Krankenkasse. Bei Betrugsversuchen bittet die AOK die Betroffenen, die Fälle der Kasse zu melden und gegebenenfalls Anzeige bei der Polizei zu erstatten.

Quelle: https://www.t-online.de/leben/aktuelles/id_100288916/krankenkasse-aok-warnt-vor-betrugsversuchen-per-sms.html

12) SIM-Swapping: So stehlen Hacker Ihre Handynummer

Smartphone-Nutzer aufgepasst: Kriminelle machen sich den Trick mit der Ersatz-SIM-Karte zunutze, um auf persönliche Dienste wie Online-Banking zuzugreifen. Lesen Sie, was SIM-Swapping ist, wie es funktioniert und wie Sie sich schützen können.

Da praktisch jeder mittlerweile ein Handy oder ein Smartphone besitzt und ständig mit sich führt, werden mobile Endgeräte verstärkt zum Überprüfen der persönlichen Identität verwendet, insbesondere durch Onlinedienste. Dazu wird ein Einmal-Passcode via SMS oder Voicemail an das Handy des Benutzers durchgegeben. Dieser muss den Code danach zur Authentifizierung auf einer Website oder App eingeben, eventuell als Bestandteil einer Multi-Faktor-Authentifizierung (MFA) oder zur Wiederherstellung eines Accounts.

Codeauthentifizierung wird zum Werkzeug für Hacker

Bei der Codeauthentifizierung handelt es sich um eine benutzerfreundliche, jedoch vermeintlich sichere Methode der Authentifizierung. Denn die Tatsache, dass die allermeisten Nutzer ihre Mobilfunknummern mit Bank-, E-Mail- und Social-Media-Konten verknüpft haben, lockt auch Angreifer auf den Plan. Verschaffen Sie sich mithilfe von **SIM-Swapping** Zugang zu einer fremden Handynummer, können Sie diese für eine Reihe krimineller Zwecke verwenden. So bekommt ein Angreifer alle SMS und Anrufe weitergeleitet oder kann selbst simsen oder – zum Beispiel kostenpflichtige Dienste im Ausland – anrufen.

Darüber hinaus ist der Hacker dann in der Lage, (nahezu) die gesamte Onlinepräsenz an sich zu reißen, indem er Accounts hackt, bei denen eine Mobilfunk-basierte Authentifizierung (etwa Twitter) oder Wiederherstellung des Passworts möglich ist – dazu gehören beispielsweise auch Gmail, Facebook oder Instagram. Prominente Opfer sind unter anderem Twitter-Mitbegründer und Ex-CEO **Jack Dorsey** oder Schauspielerin **Jessica Alba**: Ihre Twitter-Accounts wurden via SIM-Swapping gehackt, um im Anschluss daran anstößige Posts auf der Plattform zu versenden.

Teuer wird es, wenn das Opfer das immer noch (zu) oft genutzte mTAN- oder smsTAN-Verfahren zur Freigabe von Onlineüberweisungen verwendet, also die Bank die Transaktionsnummer per SMS an den Kunden schickt. Verfügt der Hacker zusätzlich über die Zugangsdaten für das Online-Banking, kann er bequem von zu Hause aus das Konto seines Opfers leerräumen. Dass diese Methode nicht nur jenseits des großen Teiches, sondern auch hierzulande eingesetzt wird, dokumentiert eine Meldung der Zentralstelle Cybercrime Bayern.

Diese nahm Mitte 2019 ein Verbrechertrio fest, das mittels SIM-Swapping Zugriff auf mindestens **27 fremde Bankkonten** erlangt hatte und Überweisungen vornahm.

Wie SIM-Swapping funktioniert

Die bevorzugte Methode zum Kapern einer Mobilfunknummer ist **SIM-Swapping**, **SIM-Swap**

oder **SIM-Hijacking**. SIM-Swapping erfolgt in der Regel über das Kundenportal oder die Kunden-Hotline des Mobilfunk-Providers. Dort gibt sich der Hacker dann als sein Opfer aus und beantragt eine neue SIM, beispielsweise weil sein Handy mitsamt der SIM-Karte verlorengegangen ist oder wegen des Formats nicht mehr bei dem neuen Smartphone passt. Oder aber er kündigt den Vertrag und beantragt eine Rufnummernmitnahme/Rufnummerportierung zum neuen Provider.

In beiden Fällen genügt natürlich nicht nur die Angabe der Mobilfunknummer. Der Hacker muss weitere persönliche Informationen des Opfers bereitstellen. Hierzu gehören zum Beispiel das Geburtsdatum, die Adresse oder das Kundenkennwort – Daten, die er sich unter anderem in sozialen Netzwerken beschafft (Social Engineering), via Phishing-Mails erhalten oder im Darknet gekauft hat. Bei einem Anruf im Servicecenter des Mobilfunkanbieters können mit ein bisschen Überredungsgeschick schon leichter zugängliche Daten genügen, damit der Mitarbeiter dem Änderungswunsch trotz mangelnder Legitimation nachkommt.

Anschließend muss sich der Angreifer bei herkömmlichen SIM-Karten noch die physische SIM beschaffen, etwa, indem er den Brief des Mobilfunkanbieters abfängt oder gleich zu Beginn eine andere Adresse angibt. Einfacher geht dies mit einer eSIM, die beispielsweise die vergangenen vier Smartphone-Generationen von Apple und Google unterstützen: Hier wird der eingebaute Chip auf elektronischem Wege mit dem eSIM-Profil beschrieben.

Wurde Ihre Mobilfunknummer gestohlen?

Wenn SMS-Versand, Smartphone-Telefonate und mobile Datenverbindungen auf einmal nicht mehr möglich sind, kann dies ein Indiz dafür sein, dass die Rufnummer möglicherweise den Besitzer gewechselt hat. Es ist allerdings wahrscheinlicher, dass man sich lediglich in einem Funkloch befindet oder eine technische Störung des Mobilfunknetzes vorliegt.

Eindeutiger ist es, wenn man plötzlich nicht mehr auf verschiedene Dienste zugreifen kann oder ungewöhnliche Vorgänge auf seinem Konto registriert. Da viele Angreifer nachtaktiv sind, bemerkt man die Probleme häufig erst am nächsten Morgen – dann ist es jedoch in der Regel bereits zu spät.

Wie Sie sich am besten vor SIM-Swapping schützen

Beim Schutz vor SIM-Swapping gelten viele Tipps, die auch bei anderen Betrugsmaschen im Internet helfen. Nutzen Sie ein aktuelles Betriebssystem mit den neuesten Sicherheits-Updates und – wo es Sinn macht – Antivirensoftware.

Verwenden Sie kein einheitliches Passwort für verschiedene Onlinedienste, sondern jeweils einen individuellen Code, der zudem ausreichend lang und komplex ist. Aktivieren Sie die Zwei-Faktor-Authentifizierung als zusätzliche Komponente sicherer Passwörter.

Überprüfen Sie gelegentlich, ob es ein Datenleck bei einem der von Ihnen genutzten Dienste gab und Ihre Daten in falsche Hände geraten sind. Hinweise dazu liefert etwa der Identity Leak Checker vom Hasso-Plattner-Institut oder haveibeenpwned.com.

Banken, Mobilfunkbetreiber & Co.: Vorsicht vor Phishing-Mails

Seriöse Unternehmen, insbesondere Banken, fordern ihre Kunden niemals dazu auf, persönliche Daten über einen Link in einer E-Mail preiszugeben, und kommunizieren dies dementsprechend regelmäßig.

Auch die Mobilfunkbetreiber haben nach dem Aufkommen erster SIM-Swapping-Fälle in Deutschland Vorkehrungen getroffen. So bietet beispielsweise die Telekom seit dem Sommer 2018 die Identifikation per Stimme (Sprach-ID) an. Bei der Telekom, bei Vodafone und O2 ist ein spezielles Kundenkennwort bei der Kunden-Hotline verpflichtend. Nutzen Sie diese

Möglichkeiten.

Empfehlenswert ist darüber hinaus, so- weit möglich anstelle von SMS oder Anruf eine andere Methode wie etwa Face-ID oder Yubikey zur Zwei-Faktor-Authentifizierung zu wählen.

Quelle: https://www.pcwelt.de/article/1535299/sim-swapping-hacker-stehlen-handynummer.html?utm_date=20231228120953&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20SIM-Swapping%3A%20So%20stehlen%20Hacker%20Ihre%20Handynummer&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

13) Geld vom Finanzamt: So läuft ein aktueller Betrug

Cybergangster starten im Namen des Finanzamts eine Betrugswelle. So erkennen Sie die Attacke.

Das auf Warnungen vor Cyberbetrug und Phishing-Angriffe spezialisierte Online-Portal Mimikama warnt vor einer betrügerischen Mail, die vorgibt, vom Finanzamt zu kommen. Die SMS hat diesen Inhalt:

> „INFORMATION: Das Finanzamt hat entschieden, dass Sie einen Betrag von 671,48 erhalten Bestätigen Sie Ihre Bank, um die Rückerstattung zu erhalten: https:rebrand.ly/bundesamt Hinweis: Dies ist eine automatisch generierte Nachricht“

Wer auf den angegebenen Link klickt oder tippt, landet auf einer Seite, die mit “bund.de Verwaltung Digital” sowie “Erstattung 2022” überschrieben ist und das schwarz-rot-goldene Farbmuster der Bundesrepublik Deutschland aufnimmt. Die Seite zeigt ein Online-Formular, in dem Sie Ihren Namen, Adresse, Mobiltelefon- und Festnetznummern, Geburtsdatum und Ihre IBAN eingeben sollen. Mit diesen Daten ist der perfekte Identitätsdiebstahl möglich. Cybergangster können damit auch illegale Käufe und Geldgeschäfte im Internet tätigen.

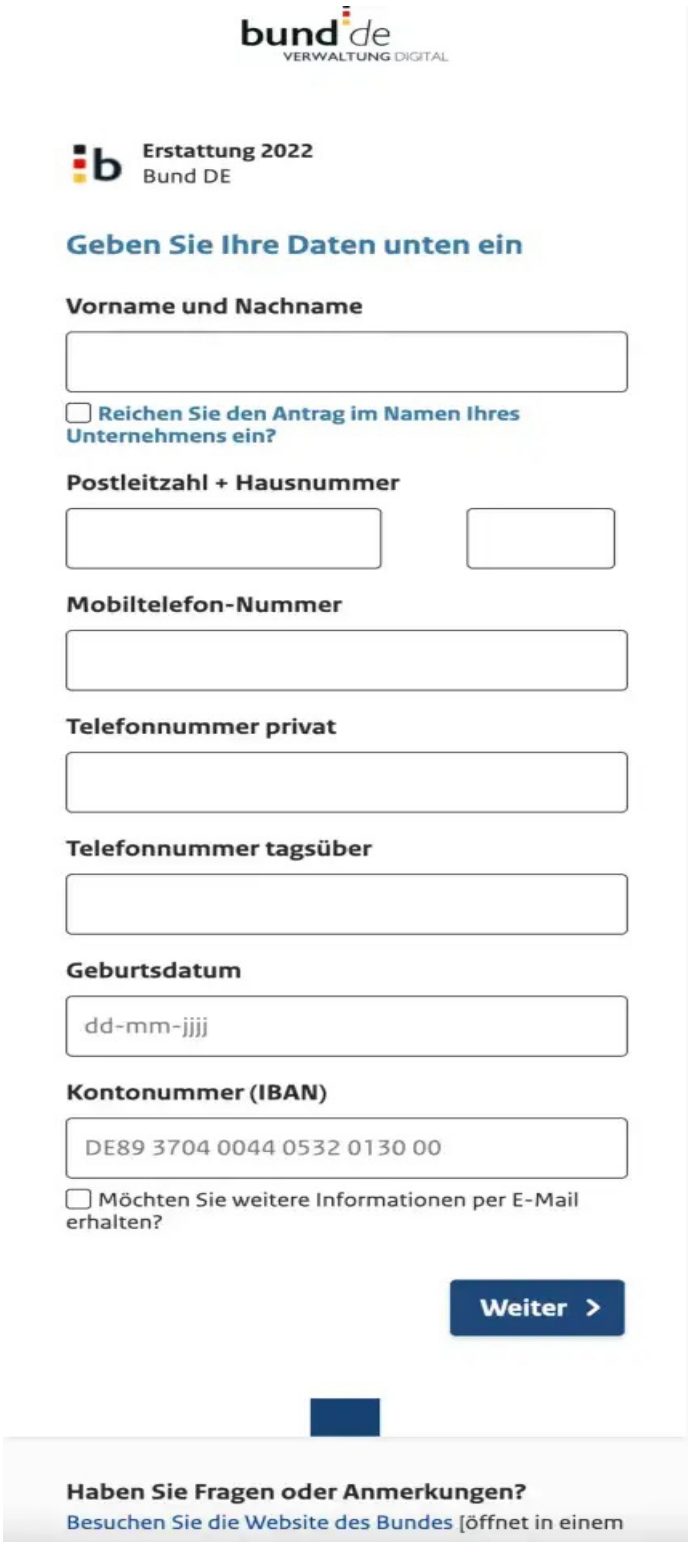
Die Cybergangster versuchen der Webseite ein seriöses Erscheinungsbild zu verpassen. Deshalb haben sie eine Checkbox integriert, die es ermöglicht, weitere Informationen per E-Mail anzufordern. Außerdem gibt es einen Bereich “Haben Sie Fragen und Anmerkungen?”.

Laut Mimikama.at war die betrügerische Webseite ursprünglich aber anders gestaltet. Sie enthielt anscheinend anfangs nicht das oben abgebildete Web-Formular, sondern zeigte eine gefakte Webseite des Finanzministeriums mit weiterführenden Links zu einigen bekannten Banken. Diese Links waren natürlich gefälscht, wer darauf klickte, landete auf Phishing-Seiten, auf denen die Benutzer ihre IBAN und BIC eingeben sollten.

Diese SMS ist genauso wie alle darin verlinkten Webseiten und Online-Formulare eine Fälschung und dient nur dazu, an Ihre persönlichen Daten und Kontodaten zu gelangen. Die SMS nutzt offensichtlich das Wissen vieler Menschen über das kürzlich beschlossene Maßnahmenpaket der Bundesregierung aus. Vor dem Hintergrund dieser Unterstützungsmaßnahmen wie beispielsweise der Gaspreisbremse könnte eine solche SMS, in der eine Rückerstattung angekündigt wird, vielen Empfängern plausibel erscheinen – das hoffen vermutlich die Betrüger.

So schützen Sie sich

Das Bundesfinanzministerium verschickt keine SMS. Löschen Sie alle derartigen Kurznachrichten, ohne auf einen Link darin zu tippen/klicken.



So sieht das gefälschte Online-Formular aus. Quelle: Mimikama

Ähnlicher Betrugsversuch

Vor einigen Tagen machte ein ähnlicher Betrugsversuch in Zusammenhang mit einer angeblichen Corona-Hilfe die Runde. Mehr dazu lesen Sie hier: [279,99 Euro Corona-Hilfe? So läuft ein fieser Betrug im Namen der Bundesregierung.]

Quelle: https://www.pcwelt.de/article/1397608/geld-vom-finanzamt-so-lauft-ein-aktueller-betrug.html

Anwenderinformationen:

1) Software – YouTube: F für Vollbild und andere nützliche Tipps, die ihr kennen solltet

Diese Tastatur-Shortcuts machen euch das Anschauen von YouTube-Videos leichter und sparen euch Zeit.

YouTube in eurem Browser bietet wie viele Apps nützliche Tastatur-Shortcuts, die euch das Anschauen von Videos leichter und schneller machen. Wir haben euch letzte Woche nützliche Tipps für die YouTube-App auf dem Handy gezeigt und heute widmen wir uns den Desktop-Nutzern. Tastatur-Shortcuts für YouTube

Wir haben für euch die wichtigsten Shortcuts in der untenstehenden Tabelle zusammengefasst.

Shortcut	Funktion
Leertaste	Wiedergabe und Pause, wenn der Video-Player ausgewählt ist.
Leertaste gedrückt halten	Wiedergabe mit doppelter Geschwindigkeit
K	Wiedergabe und Pause
J	10 Sekunden zurückspringen
L	10 Sekunden vorwärts springen
Linker Pfeil	5 Sekunden zurückspringen
Rechter Pfeil	5 Sekunden vorwärts springen
. (Punkt)	Während das Video pausiert ist: ein Frame vorwärts
, (Komma)	Während das Video pausiert ist: ein Frame rückwärts
Shift + Punkt	Erhöht die Wiedergabegeschwindigkeit in 0,25x-Schritten
Shift + Komma	Verringert die Wiedergabegeschwindigkeit in 0,25x-Schritten
Pos1	Springt zum Anfang des Videos (bei ausgewähltem Video-Player)
Ende	Springt zum Ende des Videos (bei ausgewähltem Video-Player)
Zahlen von 0 bis 9	Springt zu 0 bis 90 Prozent des Videos
#	Aktiviert die Suchzeile
Shift + N	Nächstes Video (Funktioniert nur bei Playlists)
Shift + P	Vorheriges Video (Funktioniert nur bei Playlists)
F	Aktiviert den Vollbildmodus
T	Aktiviert den Kinomodus
I	Aktiviert den Miniplayer
M	Stummschaltung ein- und ausschalten
C	Untertitel ein- und ausschalten
+ (Plus)	Untertitel vergrößern
- (Minus)	Untertitel verkleinern
O	Ändert die Transparenz der Untertitel in vier Stufen

Das Verkleinern und Vergrößern der Untertitel hat bei uns nicht über die Tasten auf dem Nummernblock funktioniert. Dafür werden Plus und Minus auf der linken Seite neben Enter und Shift verwendet.

Wenn eure Tastatur Multimedia-Tasten besitzt, könnt ihr eure YouTube-Videos auch damit steuern. So könnt ihr einfach die Wiedergabe starten, pausieren oder in Playlists zum nächsten und vorherigen Video springen.

Solltet ihr eine MMO-Maus besitzen, könnt ihr mit dieser ganz einfach mit den Zahlen zu gewünschten Stellen im Video springen.

Quelle: https://www.gamestar.de/artikel/youtube-shortcuts-desktop,3405977.html?utm_source=flipboard&utm_content=other

2) Messenger – WhatsApp: Neue Funktion schafft bessere Übersicht

Schnell über das Wichtigste informiert sein – das soll mit der neuen "Fixieren"-Funktion von WhatsApp gehen. So funktioniert es.

Früher hat man noch Einladungskarten verschickt, inzwischen lädt man gerne mal per WhatsApp-Gruppenchat zum Geburtstag oder einer anderen Feierlichkeit ein. Doch solche Chats können schnell im Chaos enden. Da kann es auch passieren, dass die wesentlichen Informationen verloren gehen.

Damit soll bei WhatsApp nun Schluss sein. Denn der Messenger hat eine neue Funktion eingeführt, auf die viele Nutzer gewartet haben – das Fixieren von Nachrichten.

Wenn man eine Nachricht fixiert, taucht sie oben im Chat als Banner auf. Klickt man darauf, springt man direkt zu der Nachricht und kann sie lesen. Das funktioniert sowohl in privaten Chats als auch in Gruppen – und sogar in der Web-Anwendung. Zudem kann man auswählen, ob die Nachricht 24 Stunden, sieben Tage oder 30 Tage angepinnt bleiben soll.

So kann man Nachrichten bei WhatsApp fixieren

Und so geht es:

- **Bei iPhones:** Lange auf die Nachricht tippen, die fixiert werden soll ➡"Fixieren" auswählen (findet sich manchmal auch unter dem Reiter "Mehr") ➡Dauer der Fixierung auswählen ➡Nachricht wird fixiert
- **Bei Android-Handys:** Lange auf die Nachricht tippen, die fixiert werden soll ➡Die drei senkrechten Punkte anwählen und "Fixieren" auswählen ➡Dauer der Fixierung auswählen ➡Auf "Fixieren" tippen
- **Web/Desktop:** Mit der Maus über den rechten Rand der Nachricht fahren, bis ein Pfeil nach unten erscheint ➡"Fixieren" auswählen ➡Dauer der Fixierung auswählen ➡Auf "Fixieren" tippen

Führt man diese Aktion durch, erscheint im Chatverlauf der Hinweis, dass man selbst oder der Chatpartner eine Nachricht fixiert hat. Die Nachricht ist dann für den Chatpartner beziehungsweise alle Gruppenmitglieder als Banner sichtbar.

So kann man fixierte Nachrichten wieder lösen

Wenn die ausgewählte Frist von 24 Stunden, sieben oder 30 Tagen abgelaufen ist, wird die Nachricht von selbst aus der Fixierung gelöst. Allerdings kann man das auch manuell machen:

- **Bei iPhones:** Lange auf die Nachricht tippen ➡ "Lösen" auswählen
- **Bei Android-Handys**: Lange auf die Nachricht tippen ➡ "Lösen" auswählen und bestätigen
- **Web/Desktop:** Mit der Maus über den rechten Rand der Nachricht fahren, bis ein Pfeil nach unten erscheint ➡ "Lösen" auswählen

Einen Wermutstropfen gibt es bei der neuen Funktion dennoch. Wenn neue Mitglieder in einen Gruppenchat aufgenommen werden, können sie keine fixierten Nachrichten sehen, die vor ihrem Eintritt versendet wurden.

Die neue Funktion wird derzeit noch ausgerollt. Wer sie noch nicht sieht, sollte einfach ein paar Tage warten oder manuell im App- oder Play Store prüfen, ob die aktuelle Version von WhatsApp verfügbar ist.

Tipp:

- Selbstzerstörung: Praktische neue Funktion bei WhatsApp
- Nach 120 Tagen ist Schluss: WhatsApp: Vorsicht, ungefragte Löschung
- WhatsApp: WhatsApp: Die wichtigsten Einstellungen

Quelle: https://www.t-online.de/digital/aktuelles/id_100302534/whatsapp-neue-fixieren-funktion-fuer-bessere-chat-uebersicht.html

3) Bild in Bild einfügen am iPhone – so geht's ohne Extra-App

Sie wollen ein Bild in ein anderes Bild einfügen? Mit diesem Trick geht es auf dem iPhone ohne Extra-App!

Wenn Sie im Internet nach einer Lösung suchen, wie Sie auf dem iPhone ein Bild in ein anderes Bild einfügen können, heißt es meistens: *"Laden Sie sich dafür eine Extra-App herunter."* Seitdem man aber unter iOS Motive ausschneiden kann, können Sie diese auch auf dem iPhone in ein anderes Foto einfügen.
Mithilfe eines kleinen Tricks können Sie auf das Herunterladen einer Extra-Applikation verzichten. Alles, was Sie dafür benötigen, liefert das iPhone von Haus aus mit. Und so geht's:

1. Gehen Sie in die **Foto-App** und wählen Sie die zwei Fotos aus, die Sie miteinander kombinieren möchten.
2. Drücken Sie auf den Pfeil unten links und wählen Sie "***In Dateien sichern***" aus
3. Erstellen Sie in ***Dateien*** einen eigenen Fotos-Ordner, damit Sie die Fotos später leichter finden können.

Gehen Sie nun in die Dateien-App in den Ordner, in dem sich die gespeicherten Fotos befinden.

1. Wählen Sie das Foto mit dem Motiv aus, welches Sie ausschneiden möchten.
2. Drücken und halten Sie das Motiv, bis Sie das Foto ausschneiden können.
3. Halten Sie das ausgeschnittene Motiv mit einem Finger auf dem Bildschirm fest, während Sie mit einem anderen Finger zum zweiten Foto wechseln.
4. Sie können nun das ausgeschnittene Motiv im anderen Bild skalieren.
5. Drücken Sie anschließend auf "*Fertig*", im Dateien-Ordner wird ein neues Bild abgespeichert. Sie können übrigens im Nachhinein das eingefügte Motiv noch weiter verändern, in dem Sie dieses länger gedrückt halten.

Lesetipp: iPhone: 10 Foto-Tricks, die Sie lieben werden!

Quelle: https://www.macwelt.de/article/2154591/iphone-bild-in-bild-einfuegen.html

4) Support-Scam – Achtung: Gefälschte Microsoft-Warnmeldungen im Browser

Support-Scam ist eine Masche, bei der sich Betrüger als Mitarbeiter großer Unternehmen ausgeben. Angebliche Windows-Warnungen können ihr Einfallstor sein.

Dass Betrüger anrufen und sich als Microsoft-Mitarbeiter ausgeben, um auf die Rechner ihrer Opfer zu gelangen, hat man schon einmal gehört.

Bei einer anderen Spielart dieser Angriffsmasche sollen Nutzerinnen und Nutzer aber selbst dazu gebracht werden, die Täter anzurufen, etwa über gefälschte Microsoft-Meldungen im Browser. Davor warnt das Verbraucherschutzportal "Watchlist Internet".

Die Pop-ups, die meist beim Klicken auf Werbung oder beim Besuch unseriöser Seiten auftauchen, deklarieren die Betrüger dabei als Sicherheitswarnung des in Windows integrierten Virenscanners Defender: Schadsoftware sei gefunden, das Gerät aus Sicherheitsgründen blockiert worden, heißt es da. Dazu wird eine angebliche Telefonnummer des Microsoft-Supports angegeben.

Auf keinen Fall den falschen Support anrufen

Diese Nummer sollte man aber keinesfalls anrufen, warnen die Verbraucherschützer. Sonst landet man direkt bei den Betrügern, die dann etwa Geld in Gestalt einer frei erfundenen Servicegebühr verlangen oder ihre Opfer drängen, Fernwartungssoftware zu installieren, die dann aber nur dazu dient, den Rechner für Datendiebstahl, Erpressung und weitere Betrügereien zu übernehmen.

Beeindrucken lassen sollte man sich auch nicht von Audio-Einspielern, die die Pop-ups begleiten: Um den Druck zu erhöhen, erklärt eine Stimme, dass der Computer bereits Microsoft alarmiert habe, da dieser mit einem Trojaner infiziert sei und bereits Log-in-Daten von Onlinediensten sowie Kreditkartendaten in den Händen von Hackern seien.

Einfach den Tab oder den Browser schließen

Stattdessen gilt es, den jeweiligen Tab oder besser noch gleich den ganzen Browser zu schließen. Auf das Schließen-Symbol (X) der gefälschten Windows-Warnung sollte man nicht klicken, weil dann die Anzeige in den Vollbild-Modus wechselt, was noch bedrohlicher wirken kann. Das Vollbild kann man in aller Regel mit der F11-Taste verlassen.

Taucht die gefälschte Warnung auch nach einem Neustart des Browsers immer wieder auf, raten die Verbraucherschützer zum Löschen von Website-Daten, Cache und Cookies in den Browser-Einstellungen. Notfalls müsse der Browser zurückgesetzt werden. Auch Microsoft selbst bietet auf seinen Support-Seiten Hilfestellungen zum Thema Support-Scam.

Quelle: https://www.t-online.de/digital/aktuelles/id_100296240/support-scam-microsoft-warnmeldungen-im-browser-gefaelscht.html

5) Kälte schwächt Handy – Smartphone aufladen im Winter – Tipps für die kalte Jahreszeit

Der Winter steht vor der Tür. Wenn Sie bei niedrigen Temperaturen mit dem Smartphone unterwegs sind, treten mitunter Probleme auf.

Gegen eisiges Wetter ziehen wir dicke Jacken und warme Mützen an. Doch was ist mit unserem Handy? Es gibt zwei Komponenten an unseren mobilen Geräten, die sehr

empfindlich auf extreme Temperaturen reagieren. Zum einen der Akku und zum anderen das Display. Jeder weiß, dass man im Sommer sein Handy nicht in der prallen Sonne oder im Auto liegen lässt. Im Winter sind ebenfalls einige Vorsichtsmaßnahmen sinnvoll.

Auch Smartphones mögen es kuschelig

Genaue Angaben machen die Hersteller der Geräte fast nie. Eine Ausnahme bietet hier Apple. Der iPhone-Hersteller gibt an, dass die Geräte nur für eine Umgebung zwischen 0 und 35 Grad Celsius geeignet sind. Zu Hause bleiben muss das Handy trotzdem nicht.

Die besten Tipps für mobile Geräte im Winter

Natürlich können Sie Ihre Geräte auch mitnehmen, wenn Sie in einer verschneiten Schneelandschaft unterwegs sind. Darauf sollten Sie achten:

1. Lassen Sie kein Akkugerät über einen längeren Zeitraum im Auto.
2. Tragen Sie Ihr Smartphone nah am Körper, da die Körperwärme ein Auskühlen verhindert.
3. Gönnen Sie Ihrem Handy eine vollumschließende Hülle, die ebenfalls das Display schützt.
4. Telefonieren Sie unterwegs mit einem Headset, sodass das Telefon in der warmen Jackentasche bleibt.
5. Vermeiden Sie schnelle Temperaturschwankungen. Betreten Sie wieder einen geheizten Raum, lassen Sie dem Gerät Zeit, sich zu akklimatisieren, bevor Sie es intensiv nutzen.
6. Setzen Sie Ihre Geräte niemals dem direkten Kontakt mit Schnee oder vereisten Flächen aus.

Tipp:

- Lebensdauer erhöhen: So schonen Sie Ihren Smartphone-Akku
- Smartphone-Tricks: So laden Sie Ihr Smartphone effizienter
- Lademethoden im Vergleich: Smartphone: Drahtlos oder mit Kabel laden?

Auswirkungen von extremen Temperaturen aufs Smartphone

Die hoch entwickelten Displays können durch sehr hohe, aber auch durch sehr niedrige Temperaturen zerstört werden. In der Regel wird Ihr Handy zunächst mit Ausfallerscheinungen reagieren und sich möglicherweise selbst abschalten oder nur noch eingeschränkt funktionieren. Die Akkukapazität fällt unter Umständen sehr schnell und schädigt die Ladefähigkeit des Akkus nachhaltig. Durch extreme Temperaturschwankungen kondensiert eventuell Luftfeuchtigkeit am und im Gerät und beschädigt es.

Quelle: https://www.t-online.de/ratgeber/technik/smartphone-und-telefone/id_100259020/smartphone-aufladen-im-winter-tipps-fuer-die-kalte-jahreszeit.html

6) Mythen und Fakten – Darum sollten Sie Ihr Smartphone nicht über Nacht laden

Die Lebensdauer von Smartphone-Akkus zu verlängern, lohnt sich. Wir zeigen Ihnen, worauf dabei zu achten ist und welche Ratschläge Sie besser ignorieren.

Der Akku Ihres Smartphones ist nicht auswechselbar. Sein Defekt hat meist einen Neukauf eines kompletten Gerätes zur Folge. Um Ihr Handy möglichst lange zu nutzen, sollten Sie also einem frühzeitigen Verschleiß der Batterie vorbeugen.

Diese Mythen helfen nicht – keine Vorteile für den Akku

Nicht alle Tipps sind wirklich hilfreich. Lernen Sie als Erstes diese vier Mythen kennen:

1. Der Memory-Effekt: Eine vollständige Ladung ist nicht erforderlich, um Ihren Akku zu schützen.
2. Laden über Nacht: Laden Sie Ihr Smartphone nachts, ist der Akku am Morgen voll. Im Hinblick auf die Lebensdauer wirkt sich dies jedoch negativ aus, da der Energiespeicher dadurch täglich über mehrere Stunden hinweg an seiner oberen Kapazitätsgrenze verweilt.
3. Falsches Netzteil: Im Grunde liefern alle passenden Ladegeräte die richtige Versorgungsspannung. Den Ladevorgang kontrolliert eine Ladeelektronik innerhalb des Smartphones. Welches Netzteil Sie verwenden, spielt also in Bezug auf die Lebensdauer Ihres Smartphone-Akkus keine Rolle.
4. Jedes Anstecken ist ein Ladezyklus: Hersteller von Li-Ionen-Akkus geben die Lebensdauer üblicherweise in Ladezyklen an. Diese beziehen sich jedoch nicht darauf, wie häufig Sie Ihr Mobiltelefon mit einer Stromquelle verbinden, sondern lediglich auf die tatsächlich nachgeladene Energiemenge. Wer beispielsweise viermal um jeweils 25 Prozent nachlädt, hat insgesamt einen vollständigen Ladezyklus genutzt.

Mit diesen Tipps verlängern Sie die Lebensdauer Ihres Smartphone-Akkus wirklich

Und hier kommen vier Ratschläge, die Ihrem Akku wirklich guttun:

1. Halten Sie die Ladung Ihres Smartphone-Akkus idealerweise zwischen 30 und 70 Prozent. Je näher Sie sich in Richtung der Kapazitätsgrenzen bewegen, desto stärker beeinträchtigen Sie die Lebensdauer der Zellen.
2. Viele moderne Smartphones verfügen über Einstellungen, mit denen sich eine Obergrenze für den Ladevorgang definieren lässt. Wenn Sie Ihr Handy über Nacht laden wollen, setzen Sie eine Grenze bei 70 bis 80 Prozent, sodass das Gerät automatisch aufhört zu laden.
3. Li-Ionen-Akkus sind üblicherweise nicht für extreme Temperaturen ausgelegt. Schützen Sie Ihr Mobiltelefon daher so gut es geht vor übermäßiger Einwirkung von Wärme und Kälte. Ideal sind Temperaturen zwischen 10 und 25 Grad Celsius.
4. Halten Sie den Energieverbrauch Ihres Smartphones niedrig, indem Sie beispielsweise das Display abdunkeln, ungenutzte Apps deinstallieren und Energiesparfunktionen des Betriebssystems nutzen. Wenn Ihr Smartphone weniger Energie verbraucht, sind auch weniger Ladezyklen erforderlich, was die Lebensdauer des Akkus effektiv verlängert.

Benötigen Sie Ihr Smartphone nicht, lagern Sie es mit einem Ladezustand des Akkus von 50 Prozent. Schalten Sie dann das Handy aus und achten auf eine Umgebungstemperatur zwischen 10 und 20 Grad.

Quelle: https://www.t-online.de/digital/smartphone/id_100259246/smartphone-akkus-lebensdauer-verlaengern-und-schonend-laden-vier-tipps.html

7) Anleitung – WLAN-Passwort anzeigen: So finden Sie es heraus

Was tun, wenn man ein Gerät ins WLAN einbinden will und den Netzwerkschlüssel vergessen hat? Mit diesen Tricks können Sie sich das Passwort anzeigen lassen.
Zu Hause nutzen die meisten das heimische WLAN, um auf dem Smartphone, Tablet oder Notebook zu surfen. Nach der ersten Passworteingabe verbinden sich die Geräte dann automatisch über das Drahtlosnetzwerk mit dem Internet, sobald man wieder in Reichweite des WLAN-Routers ist.

WLAN-Passwort in Windows auslesen – so geht's

Doch was tun, wenn man ein neues Gerät mit dem Heimnetzwerk verbinden will und das WLAN-Passwort vergessen hat? Wir zeigen, wie Sie das Kennwort auf verschiedenen Geräten herausfinden können.

Bei Windows 10 das WLAN-Passwort auslesen

Im Betriebssystem Windows 10 kann man sich das WLAN-Passwort ganz einfach in den **Netzwerkeinstellungen** anzeigen lassen. So geht's:

1. Öffnen Sie die **Systemsteuerung**. Am einfachsten geht das, indem Sie das Wort in die Suchleiste neben dem Windows-Startbutton eingeben.
2. In der Systemsteuerung klicken Sie mit der linken Maustaste auf **Netzwerk und Internet**.
3. Weiter geht es mit dem **Netzwerk- und Freigabecenter**.
4. Klicken Sie im nächsten Schritt auf die **WLAN-Verbindung**, die Sie gerade nutzen.
5. Es öffnet sich ein Dialogfenster, in dem Sie die **Drahtloseigenschaften** aufrufen können.
6. Dort wechseln Sie in den Reiter **Sicherheit**. Hinter **Sicherheitsschlüssel** verbirgt sich das WLAN-Passwort. Sie müssen nur noch das Häkchen neben **Zeichen anzeigen** setzen, um es auslesen zu können.

Alternativ können Sie auch über einen Klick auf das WLAN-Symbol in der Taskleiste in die Internet- und Netzwerkeinstellungen gelangen. Diese Fotoshow zeigt, wie es geht.

Um das WLAN-Passwort auslesen zu können, müssen Sie bei Windows in einem Nutzerkonto mit Adminrechten angemeldet sein. Nutzer mit eingeschränkten Berechtigungen, beispielsweise Gastnutzer, haben aus gutem Grund keinen Zugriff auf gespeicherte Kennwörter. Wechseln Sie gegebenenfalls das Konto oder wenden Sie sich an den Eigentümer des Netzwerks oder des Geräts.

WLAN-Passwort über die Eingabeaufforderung auslesen

Falls gerade keine WLAN-Verbindung besteht, können Sie ein früher eingegebenes Kennwort auch über die Windows-Eingabeaufforderung abfragen. Auch dazu benötigen Sie Adminrechte.

1. Starten Sie die Eingabeaufforderung, indem Sie **cmd.exe** in das Suchfeld eingeben und auf **Als Administrator ausführen** klicken, sobald die App angezeigt wird.
2. Bestätigen Sie die Sicherheitsabfrage.
3. In der Konsole geben Sie nun den folgenden Befehl ein: **netsh WLAN show profile name=[SSID-Name] key=clear**. Anstelle von [SSID-Name] geben Sie den Namen des gewünschten WLAN-Netzes ein.
4. Bestätigen Sie die Eingabe mit Enter. Nun wird eine Liste mit Eigenschaften und Sicherheitseinstellungen des Netzwerks angezeigt, darunter auch der Netzwerkschlüssel.

Wie lässt sich das WLAN-Passwort beim Router auslesen?

Viele Hersteller liefern ihre Router mit einem aufgedruckten Standardschlüssel oder Pre-Shared-Key aus. Den können Gastnutzer dann von der Unterseite des Geräts ablesen oder einen QR-Code einscannen, um sich mit dem Netzwerk zu verbinden. Wie Sie ein sicheres Gast-WLAN einrichten können, erfahren Sie hier.

Allerdings ist es nicht immer ratsam, das Standardpasswort zu verwenden, da Angreifer dieses leicht erraten können. Experten empfehlen, gleich bei der Router-Einrichtung ein

eigenes Kennwort sowie einen einzigartigen Namen für das Netzwerk zu vergeben. Über die Router-Software können Sie das Passwort später auslesen oder ändern – vorausgesetzt Sie haben Zugriff auf die Weboberfläche des Routers. Diese sollte in der Regel ebenfalls mit einem eigenen Routerkennwort geschützt sein.

Tipp: Verwenden Sie nicht dasselbe Passwort mehrfach. Nutzen Sie am besten einen Passwortmanager, um sichere Kennwörter zu erstellen und zu verwahren. Für den PC gibt es zahlreiche kostenlose Lösungen wie beispielsweise die Open-Source-Software Keepass. Apple-Nutzer haben mit dem iCloud-Schlüsselbund schon eine einsatzfertige Lösung auf dem iPhone parat.

WLAN-Passwort auf der Fritzbox auslesen

Nutzer eines Fritzbox-Routers gelangen über die URL http://fritz.box in die Interneteinstellungen ihres Heimnetzwerks. Auf der linken Seite findet sich eine Menü-Übersicht. Klicken Sie dort auf **WLAN** und dann auf **Sicherheit**. Im Feld **WLAN-Netzwerkschlüssel** wird das WLAN-Passwort im Klartext angezeigt.

WLAN-Passwort bei einem Speedport-Router auslesen

Nutzer eines Speedport-Routers öffnen die Weboberfläche, indem sie die URL http://speedport.ip in der Adresszeile des Browsers eingeben. Suchen Sie im Routermenü nach den Sicherheits- und WLAN-Einstellungen, um das aktuelle Passwort herauszufinden.

Bei anderen Routerherstellern wie TP-Link können Sie es mit den Standard-IP-Adressen **192.168.1.1** oder **192.168.2.1** in der Browserzeile versuchen.

WLAN-Passwort auf einem Android-Handy anzeigen

Auch Smartphones, die mit einem bestimmten WLAN-Netz schon mal verbunden waren, haben sich das Kennwort gemerkt und können es dem Nutzer verraten – sofern er die Netzwerkeinstellungen nicht zurückgesetzt hat und das Passwort nicht geändert wurde.

Auf einem Android-Handy machen Sie Folgendes:

1. Rufen Sie die **WLAN-Einstellungen** auf. Das geht beispielsweise, indem Sie auf dem Bildschirm von oben nach unten wischen und im Schnellmenü das WLAN-Symbol gedrückt halten.
2. Tippen Sie auf das **Drahtlosnetzwerk**, mit dem Sie aktuell verbunden sind.
3. In den nun angezeigten Netzwerkdetails findet sich unter Android 11 auch die Option zum **Teilen**. Wenn Sie darauf tippen, wird ein **QR-Code** angezeigt, den andere Smartphone-Nutzer einfach scannen können, um sich in dasselbe Netzwerk einzuwählen. Auch das WLAN-Passwort wird an dieser Stelle verraten.

Je nach Hersteller und Android-Version kann sich das WLAN-Passwort aber auch in einem anderen Untermenü oder in den erweiterten Einstellungen verbergen, beispielsweise unter dem Eintrag **WLAN ändern** oder **Kennwort anzeigen**.

In der Regel muss der Nutzer seine Identität bestätigen (zum Beispiel per Fingerabdruck oder PIN-Eingabe), bevor er Zugriff auf das Passwort hat.

WLAN-Passwort auf dem iPhone anzeigen

Auf einem iPhone müssen Sie einen Umweg über den Rechner nehmen, um das WLAN-Passwort zu erfahren: Falls Sie auf beiden Geräten den iCloud-Schlüsselbund nutzen, finden Sie das WLAN-Passwort in der Schlüsselbundverwaltung im Menü **Netzwerke** und können es sich im Klartext anzeigen lassen.

Wer Angst hat, sein WLAN-Passwort zu vergessen, kann es aber auch einfach im hauseigenen Passwortmanager von Apple hinterlegen. Dann hat man es bei Bedarf immer auf dem iPhone griffbereit und kann sogar Siri danach fragen.

Kann ich das WLAN-Passwort unter Windows 10 ohne Adminrechte auslesen?

Sofern es nicht irgendwo offen einsehbar an der Hardware oder in der Umgebung angebracht ist, kann nur der Geräte- beziehungsweise Netzwerkeigentümer das WLAN-Passwort einsehen und ändern. Das dient der Sicherheit des Netzwerks und der damit verbundenen Geräte.

Unter Windows gibt es daher keine einfache Möglichkeit, das WLAN-Passwort ohne Umwege herauszufinden, wenn man keine Adminrechte besitzt. Jeder Versuch, diese Schutzvorkehrungen zu umgehen und sich ohne Wissen des Eigentümers in ein WLAN-Netzwerk einzuwählen, könnte als illegaler Hackerangriff ausgelegt werden.

Zugang ohne WLAN-Passwort dank WPS

Eine Alternative zum kennwortgeschützten WLAN-Netz bietet die WPS-Funktion einiger Router. WPS steht für Wi-Fi Protected Setup. Bei dieser Methode tauschen Router und Geräte die nötigen Informationen (WLAN-Name und Passwort) quasi in Eigenregie aus. Der Nutzer muss fast nichts machen, außer die WPS-Funktion in den WLAN-Einstellungen des Endgeräts zu aktivieren. Auf dem Router genügt – sofern die Funktion aktiviert ist – ein Knopfdruck, um so ein "spontanes" WLAN-Netz zu erschaffen.

Allerdings sollte man darauf achten, dass sich die Funktion nach einiger Zeit wieder automatisch ausschaltet und nicht dauerhaft aktiv ist, um keine "ungebetenen Gäste" anzulocken. Eine WPS-Funktion, die sich aus der Ferne aktivieren lässt und nur mit einer PIN gesichert ist, stellt ein potenzielles Sicherheitsrisiko dar.

Tipp:

- Netzwerkcheck: Browser-Test checkt Ihre PC-Sicherheit
- Zehn Tipps fürs Heimnetzwerk: Diese Kniffe machen Ihr WLAN sicherer
- Fritzbox-Tipp: Wie Sie ein sicheres WLAN für Besucher einrichten

Quelle: https://www.t-online.de/digital/internet/id_84138344/wlan-passwort-vergessen-so-finden-sie-es-heraus.html

8) Malware stoppen – Viren auf dem iPhone: So erkennen und beseitigen Sie Schadsoftware

iPhones sind immun gegen Viren, heißt es – das stimmt leider nicht. Erfahren Sie, wie Sie schädliche Programme erkennen, finden und kostenlos entfernen.

Obwohl iPhones als relativ sicher gelten, ist es möglich, dass sie von Viren oder Malware – also schädlichen Programmen – befallen werden. In diesem Artikel geben wir Ihnen Tipps, wie Sie Viren auf Ihrem iPhone erkennen, finden und loswerden.

Sind iPhones vor Viren sicher?

Die weitverbreitete Meinung, dass iPhones völlig immun gegen Viren sind, ist nicht ganz korrekt. Zwar ist das Risiko, sich ein Virus einzufangen, aufgrund der strengen Sicherheitsmaßnahmen von Apple geringer als bei Android-Geräten, aber dennoch existent.

Vor allem sogenannte Jailbreaks und das Herunterladen von Apps aus unsicheren Quellen können die Tür für Schadsoftware öffnen.

Was ist ein Jailbreak?

Ein Jailbreak beschreibt die Veränderung des Betriebssystems, um bestimmte Funktionen einzubauen. Damit umgehen Nutzer die von Apple auferlegten Einschränkungen und Sicherheitsvorkehrungen, etwa um nicht autorisierte Apps installieren zu können. Dadurch wird das Gerät aber auch weniger sicher.

So erkennen Sie Viren

Wenn Ihr iPhone von einem Virus befallen ist, kann es verschiedene Symptome zeigen:

- Ungewöhnlich hoher Akkuverbrauch
- Plötzlich langsame Leistung
- Unautorisierte App-Installationen
- Unerwartete Pop-ups oder Anzeigen
- Anstieg des mobilen Datenvolumens

Sollten Sie eines oder mehrere dieser Anzeichen bemerken, ist es ratsam, Ihr iPhone auf Viren zu untersuchen.

Scannen Sie Ihr iPhone

Um Viren auf Ihrem iPhone zu finden, können Sie spezielle Antiviren-Apps verwenden. Wichtig ist, dass Sie eine vertrauenswürdige App aus dem App Store wählen. Zwei kostenlose und beliebte Optionen sind "Avira mobile Security" und "TotalAV Mobile Security ". Diese Apps helfen Ihnen dabei, verdächtige Dateien oder Anwendungen auf Ihrem Gerät aufzuspüren.

Entfernung von iPhone-Viren

Wenn eine Antiviren-App ein Virus auf Ihrem iPhone entdeckt hat, befolgen Sie die Anweisungen der App, um die schädliche Software zu entfernen. In den meisten Fällen wird die App die Malware automatisch beseitigen.

Sollte das Problem weiterhin bestehen, versuchen Sie, alle kürzlich installierten Apps manuell zu deinstallieren und Ihr iPhone auf die Werkseinstellungen zurückzusetzen. Vergessen Sie nicht, vorher ein Backup Ihrer wichtigen Daten anzulegen.

Sicherheitstipps

Um Ihr iPhone vor Viren zu schützen, befolgen Sie diese Sicherheitstipps:

- Verzichten Sie auf Jailbreaks.
- Laden Sie Apps nur aus dem App Store herunter.
- Aktualisieren Sie Ihr Betriebssystem und Ihre Apps regelmäßig.
- Verwenden Sie sichere Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung.

Indem Sie diese Sicherheitsmaßnahmen umsetzen, gewährleisten Sie den optimalen Schutz Ihres iPhones und erhalten langfristig eine verlässliche Leistung.

Web-Sicherheit

Sicheres Browsen ist ein weiterer wichtiger Faktor, um Ihr iPhone vor Viren und Malware zu schützen. Achten Sie darauf, dass Sie einen vertrauenswürdigen Browser wie Safari, Google Chrome oder Firefox verwenden.

Vermeiden Sie den Besuch von unsicheren oder unbekannten Websites und klicken Sie nicht auf verdächtige Links in E-Mails oder Nachrichten, da diese möglicherweise zu schädlichen

Websites führen können.

Tipp: Die besten Sicherheits-Apps für Android-Smartphones

Quelle: https://www.t-online.de/digital/smartphone/id_100162966/iphone-vor-viren-schuetzen-so-erkennen-und-beseitigen-sie-schadsoftware.html

9) Tipp für Ihren Telefonanschluss – Rufumleitung Festnetz aufs Handy: So gelingt die Einrichtung

Sie bekommen regelmäßig Anrufe auf dem Haustelefon, sind aber viel unterwegs? Dabei hilft eine Rufumleitung vom Festnetz auf Ihr Handy.

Rufumleitung vom Festnetz auf das Handy einrichten

Eine Rufumleitung vom Festnetz der Deutschen Telekom auf Ihr Mobiltelefon richten Sie durch sogenannte Tastencodes ein. Das funktioniert unabhängig davon, was für ein Telefon Sie verwenden.

Starten Sie dafür einen Anruf mit Ihrem Festnetztelefon. Der zu wählende Tastencode unterscheidet sich je nach Szenario, für das Sie die Rufumleitung einrichten möchten. Grundlegend gibt es drei verschiedene Anwendungsfälle:

1. Sofortige Weiterleitung **aller** eingehenden Anrufe: ***21*Zielrufnummer#**
2. Weiterleitung bei **Nichtannahme** des Anrufs: ***61*Zielrufnummer#**
3. Weiterleitung bei **besetztem** Anschluss: ***67*Zielrufnummer#**

Bei der Zielrufnummer handelt es sich jeweils um die Rufnummer, auf der Sie die umgeleiteten Anrufe empfangen möchten. Wenn Sie also auf dem Handy die Festnetzanrufe erhalten wollen, geben Sie Ihre entsprechende Mobilfunknummer ein.

Nachdem Sie den passenden Tastencode gewählt haben, hören Sie eine Ansage über den Hörer. Sobald Sie aufgelegt haben, ist die Rufumleitung aktiv.

Hinweis: Für den zweiten Fall, also bei Nichtannahme des Anrufs, können Sie zusätzlich angeben, wie lange Ihr Festnetztelefon klingeln soll, bevor die Weiterleitung erfolgt. Ergänzen Sie dafür im Tastencode einen beliebigen Zeitwert in Sekunden zwischen 5 und 60 nach folgendem Muster: ***61*Zielrufnummer*Zeitwert#**

So deaktivieren Sie die Rufumleitung wieder

Wenn Sie Ihre Rufumleitung wieder deaktivieren möchten, machen Sie dies ebenso mithilfe von Tastaturcodes. Auch dafür gelten die oben geschilderten drei Anwendungsfälle:

- Sofortige Weiterleitung **aller** eingehenden Anrufe deaktivieren: **#21#**
- Weiterleitung bei **Nichtannahme** des Anrufs deaktivieren: **#61#**
- Weiterleitung bei **besetztem** Anschluss deaktivieren: **#67#**

Erneut folgt nach der Wahl eine Ansage über den Hörer. Nachdem Sie aufgelegt haben, ist die Rufumleitung wieder deaktiviert.

So viel kostet die Rufumleitung vom Festnetz auf das Handy

Die Kosten für die Weiterleitung des Anrufes orientieren sich üblicherweise an dem von Ihnen gewählten Tarif für Ihren Festnetzanschluss. Sie bezahlen folglich die gleichen Minutenpreise, als würden Sie sich selbst vom Festnetz aus auf Ihrem Handy anrufen. Der ursprüngliche Anrufer hingegen trägt weiterhin die Kosten für seinen Anruf auf Ihre Festnetznummer.

Tipp:

- Funktionen freischalten: So nutzen Sie die versteckten Codes für Ihr Handy
- Mit Steuercodes: Handy-Mailbox richtig einstellen
- Bequem und günstig: So kommt das Festnetz aufs Handy

Quelle: https://www.t-online.de/digital/handy/id_100081906/rufumleitung-festnetz-aufs-handy-so-einfach-richten-sie-sie-ein.html

10) Probleme mit Deutschlandticket in DB-App – Plötzlich Schwarzfahrer – das rät die Bahn

Viele reisen über die Feiertage mit der Bahn zur Familie. Doch dabei kann es offenbar zu einem unschönen Erlebnis kommen: Das Ticket ist plötzlich weg.

Nicht erst seit dem Sturmtief "Zoltan" sind Reisende auf Probleme mit der Deutschen Bahn eingestellt. Doch zu den oft schon einkalkulierten Verspätungen gesellt sich nun offenbar noch eine weitere Erschwernis. So schildert ein Nutzer der Bahn-App "DB Navigator", dass diese ihm bei der Ticketkontrolle plötzlich kein Deutschlandticket mehr angezeigt habe – trotz des vorhandenen Abos.

Demnach half es weder, sich neu in der App einzuloggen, noch den Umweg über die DB-Homepage zu gehen. Kein Deutschlandticket, nirgends. "Mir wird die Sache furchtbar unangenehm", schreibt der Reisende laut "Fefes Blog", einem Watchblog des deutschen IT-Sicherheitsexperten Felix von Leitner. "Ich sage zur Schaffnerin, dass ich nicht weiß, was da los ist und hole meinen Ausweis raus, weil ich kurz vorm Aussteigen bin. Die Reaktion von ihr hat mich am meisten schockiert."

Der Schilderung zufolge wies ihn die Zugbegleiterin darauf hin, dass dieses Problem häufiger auftrete und Reisende zur Sicherheit einen Screenshot von ihrem Deutschlandticket machen sollten. "Sie ließ mich dann aufgrund der Feiertage ziehen. Offensichtlich sah ich schockiert genug aus, dass ich nicht wie ein Schwarzfahrer wirkte", so der Betroffene weiter.

t-online hat bei der Deutschen Bahn nachgefragt, ob es sich um ein verbreitetes Problem handelt. Eine Sprecherin teilte mit, dass diese Frage erst nach den Feiertagen von der Fachabteilung geklärt werden könne.

Deutsche Bahn: So taucht das Ticket wieder auf

Gänzlich unbekannt scheint der Bahn das Phänomen jedenfalls nicht zu sein. So beantwortet das Unternehmen in der Rubrik "Häufig gestellte Fragen" auf seiner Webseite die Frage "Wieso erscheint mein Deutschland-Ticket nicht in der App?" wie folgt: "Möglicherweise haben Sie den DB Navigator noch nicht aktualisiert."

Diese Schritte sollen dann helfen: "Wird Ihr Deutschland-Ticket nicht mehr angezeigt, aktualisieren Sie bitte den Bereich 'Meine Tickets' in der App, indem Sie die Seite auf dem Bildschirm einmal nach unten ziehen. Erscheint Ihr Deutschland-Ticket weiterhin nicht, überprüfen Sie bitte oben unter den Filteroptionen, welche Filter gesetzt sind. Setzen Sie den Filter auf 'Alle', um alle vorhanden Tickets anzuzeigen."

Schon im Oktober klagten Nutzer über nicht angezeigte Deutschlandtickets in der Bahn-App. Damals wurde der "DB Navigator" auf die Version 24.1.0 aktualisiert. Die Bahn gab damals zusätzlich den Hinweis, fehlende Tickets händisch hinzuzufügen: "Sollte ein Ticket nicht angezeigt werden, können Sie dieses im Bereich 'Reisen' über das '+'-Zeichen mit Ihrer Abonummer (diese haben Sie mit der Aktivierungsmail erhalten) und Ihrem Nachnamen hinzufügen."
Quelle: https://www.t-online.de/digital/aktuelles/id_100308796/deutschlandticket-in-db-app-verschwunden-das-raet-die-bahn.html

11) "Elon-Modus" aktiviert – Deutsche Hacker manipulieren Autopilot von Tesla

IT-Experten haben sich Zugang zu Teslas Autopiloten verschafft und konnten auf Firmengeheimnisse zugreifen. Dabei haben sie sogar den "Elon-Modus" aktiviert.

Drei Sicherheitsforscher der Technischen Universität Berlin haben es geschafft, sich in den Autopiloten von Tesla zu hacken. Die IT-Experten hätten sich durch einen sogenannten Hardware-Hack Zugriff auf die Platine verschafft, berichtet "Spiegel.de".

Die Forscher Christian Werling, Niclas Kühnapfel und Hans-Niklas Jacob haben für den Hack das System ausgebaut und die Spannung manipuliert. Dadurch hätten sie Zugang zur geschützten Platine des Autopilotsystems erhalten, Teile des Systems ausgelesen und sogar einen "Elon-Modus" aktiviert. Dieser würde es dem Auto ermöglichen, vollständig autonom zu fahren.

Werkzeug für rund 600 Euro frei zugänglich

"Wir müssen dazu den exakt richtigen Moment erwischen", sagt Niclas Kühnapfel dem Spiegel. "Wenn man einmal weiß, wie es geht, ist es recht einfach." Der benötigte technische Aufwand für diesen Hack sei mit Werkzeug für rund 600 Euro vergleichsweise gering, während der potenzielle Wert des dadurch zugänglichen geistigen Eigentums von Tesla als beträchtlich einzuschätzen ist.

Außerdem konnten die drei Wissenschaftler die Funktionsweise des Systems rekonstruieren und sogar ein zuvor gelöschtes Video eines Tesla-Fahrers wiederherstellen. Sie gehen davon aus, dass sämtliche Tesla-Fahrzeuge von der entdeckten Lücke betroffen sind, da die gehackte Platine in allen vom Unternehmen ausgelieferten Modellen verbaut ist.

Die Forscher, die sich auf IT-Sicherheit spezialisiert haben, betonen jedoch, dass ihr Ziel nicht finanzieller Natur sei. Vielmehr suchten sie nach bisher unbekannten Schwachstellen, um Unternehmen darüber zu informieren und die Nutzer insgesamt vor möglichen Angriffen zu schützen.

Tesla grundsätzlich gut gerüstet

Christian Werling sei überrascht gewesen, wie einfach sie auf Firmengeheimnisse von Tesla zugreifen konnten. Er hätte gedacht, dass das Unternehmen dieses wertvolle geistige Eigentum besser schützen würde. Die Forscher haben ihre Erkenntnisse bereits an Tesla weitergegeben. Sie erklärten, dass der Autohersteller in Sachen IT-Sicherheit grundsätzlich gut gerüstet sei.

Bereits im August konnten sich die IT-Experten Zugriff auf das Infotainment-System von Tesla verschaffen. Dadurch ließen sich etwa Bezahlfunktionen von Tesla-Fahrzeugen kostenlos freischalten oder die Sitzheizungen auf der Rückbank aktivieren.

Die gute Nachricht für alle Tesla-Fahrer: Außerhalb des Labors wird sich der Hack der drei Doktoranden wohl kaum rekonstruieren lassen. Dazu müssten die Angreifer erst einmal physischen Zugang zur Platine bekommen, sie ausbauen und anschließend gemeinsam mit dem genutzten Hacker-Werkzeug wieder im Auto einsetzen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100309312/tesla-autopilot-gehackt-deutsche-forscher-aktivieren-elon-modus-.html

12) Neues WhatsApp-Feature: Das passiert, wenn ihr länger auf euer Profilbild drückt

Wer bei WhatsApp nun länger auf sein Profilbild drückt, wird eine neue Funktion entdecken. Wir verraten euch, was ihr mit dem längeren Druck auslösen könnt.

m Hauptmenü von WhatsApp ist seit einiger Zeit auf Android-Handys euer Profilbild in der rechten oberen Ecke zu sehen. Mit einem kurzen Druck auf dieses ruft ihr die Einstellungen des Messengers auf. Nun kommt eine weitere Funktion hinzu.

Haltet ihr euren Finger auf dem Profilbild etwas gedrückt, ploppt ein Menü auf, über das ihr ein zweites WhatsApp-Konto dem Gerät hinzufügen könnt. Über einen Druck auf das Profilbild könnt ihr dann künftig zwischen den Konten wechseln.

Schneller Wechsel zwischen zwei Konten

Bislang musstet ihr Tricks anwenden, um zwei WhatsApp-Konten auf einem Gerät zu verwenden. Die Funktion ist beispielsweise interessant, wenn ihr WhatsApp mit zwei verschiedenen Nummern im privaten und beruflichen Kontext verwendet. Derzeit ist die Funktion nur auf Android-Handys verfügbar. Wann sie auf dem iPhone ausgerollt wird, ist noch unklar. Dazu macht WhatsApp noch keine Angaben.

WhatsApp geht immer mehr dazu über, Buttons doppelt zu belegen. Ein weiteres Beispiel neben dem Profilbild ist der Mikrofon-Button über den ihr seit einiger Zeit sowohl Sprach- als auch Video-Sofortnachrichten versenden könnt.

Quelle: https://www.netzwelt.de/news/225131-neues-whatsapp-feature-passiert-laenger-profilbild-drueckt.html#utm_source=newsshowcase&utm_medium=gnews&utm_campaign=CDAqDggAKgYICjD0umIw_v0NMPenkgI&utm_content=bullets&gaa_at=la&gaa_n=AYRtylYjasu6LP9VenSiJEIJIoEY5BUGOd8I_wga85fsZUZcmlB71SxEj1Hk4YVtmmRzkHjsSPbheGh8asZSuwUDLRRF_JeLjKMwPNI%3D&gaa_ts=6564f272&gaa_sig=uqAiWaGXcGJIHAi-X0jM8OhGcLZOc_rbKjzB0aulSeXVUfVgQ2z5hyqmY3Wnq66gPjbhqdpv0afrgB1mQcc_TA%3D%3D

13) So lange halten Daten auf USB-Sticks wirklich

Sie haben wichtige Daten, die Sie sicher aufbewahren wollen. Für diesen Zweck scheint der handliche USB-Stick die perfekte Lösung zu sein. Doch Sie sind sich nicht sicher, wie lange ein Stick eigentlich Daten sicher verwahren kann.

Die Lebensdauer von Daten auf einem USB-Stick hängt von vielen Faktoren ab: Unter idealen Bedingungen sollen Daten auf einem qualitativ hochwertigen USB-Stick mindestens zehn Jahre oder sogar länger liegen können. Aber was bedeutet das genau und unter welchen Bedingungen stimmt das? USB-Sticks oder auch Flash-Laufwerke speichern Daten mithilfe von NAND-Flash-Speicher.

Dieser sichert die Informationen in Form von Binärwerten (Nullen und Einsen) in Speicherzellen. Interessanterweise sind es Elektronen, die in einer Art von „schwebendem Tor“ – dem Floating Gate – gefangen sind, die diese Werte repräsentieren. Aber diese Elektronen können mit der Zeit „auslaufen“. Das führt dazu, dass sich die Daten verschlechtern, weil es schwieriger wird zu lesen, ob der Ladungszustand eine Eins oder eine Null repräsentiert.

Es gibt mehrere Faktoren, die die Lebensdauer von Daten auf einem USB-Stick beeinflussen können: Dabei spielen die Qualität des NAND-Flash-Speichers genauso wie die allgemeine Verarbeitung des Sticks eine Rolle. Billigere Modelle haben in der Regel auch eine kürzere

Lebensdauer. Dazu kommt die Anzahl der Schreibzyklen, welche beschreibt, wie oft sich Daten schreiben und löschen lassen.

Mit zunehmender Anzahl an Schreibzyklen steigt die Wahrscheinlichkeit einer Datenverschlechterung. Auch extreme Temperaturen sowie ungünstige Lagerbedingungen wie etwa hohe Luftfeuchtigkeit oder Staub können der Lebensdauer Ihrer Daten auf dem Speichermedium schaden. Ist der Stick über längere Zeit hohen Temperaturen ausgesetzt, kann das dazu führen, dass die Elektronen schneller „auslaufen“, was den Daten schaden und zu deren Verlust führen kann.

Insgesamt macht das den USB-Stick nicht zum idealen Speichermedium fürs längerfristige Aufbewahren von wichtigen Daten – schon gar nicht als einzige Methode. Sie kommen um regelmäßige Backups auf anderen Speichermedien nicht herum. Wenn Sie Daten wirklich über längere Zeit sichern möchten, sollten Sie auf archivtaugliche Bänder oder auf optische Datenträger setzen.

Und denken Sie daran: Es ist nie eine gute Idee, wichtige Daten nur an einem Ort und auf einem einzigen Medium zu speichern. USB-Sticks eignen sich am besten für den flotten Dateitransfer oder zum Erstellen von bootfähigen Medien.

Tipp: Datenarchivierung: Das sind die besten Methoden

Quelle: https://www.pcwelt.de/article/2017558/so-lange-halten-daten-auf-usb-sticks.html?utm_date=20231228113739&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20So%20lange%20halten%20Daten%20auf%20USB-Sticks%20wirklich&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

14) Windows 10: 240 Millionen PCs wegen Support-Ende Elektroschrott

Eine Untersuchung ergab, dass mit dem Support-Ende von Windows 10 Ende 2025 über 240 Millionen PCs zu Elektroschrott erklärt werden könnten.

Ist ein Workflow nur auf Windows-Systemen möglich, könnten ältere Rechner mit dem nahenden Schritt auf Windows 11 am Ende sein. Frühestens am 14. Oktober 2025 soll es so weit sein: dann, wenn Microsoft den kostenlosen Support für Windows 10 einstellt und Betroffene nicht von den erweiterten, kostenpflichtigen Updates Gebrauch machen möchten.

Der Grund sind laut Marktforschungsunternehmen „Canalys“ die gesteigerten Hardware-Anforderungen des aktuellen Windows-Systems. Sie beziffern die Zahl der auszumusternden Geräte auf über 240 Millionen PCs, die von heute auf morgen zu Elektroschrott erklärt werden: rund ein Fünftel aller im Einsatz befindlichen Windows-10-Rechner.

Windows 11 hat im Vergleich zu Windows 10 Sicherheitsvorkehrungen integriert, die u.a. eine Intel-CPU ab Generation 8 (2017) oder einen AMD-Chip ab der zweiten Ryzen-Generation voraussetzen. Zwar lässt sich dieser Hardware-Zwang von Windows 11 umgehen, was auch in den meisten privaten Anwendungsfällen kaum Probleme macht; im Unternehmensumfeld sind solche Workarounds aber problematisch. Einerseits sollten Sicherheitsfeatures im Interesse aller Beteiligten genutzt werden, andererseits dürften Support-Anfragen bei Microsoft schwierig werden, wenn vorgesehene Features bewusst umgangen und ausgehebelt werden.

Microsoft gab vor kurzem bekannt, dass Firmen und auch Privatleute für maximal drei Jahre weitere Sicherheitsupdates für Windows 10 erhalten können. Die Kosten dafür sind aber noch nicht bekannt. Je nach eingesetzten Systemen dürften die Updates dazu auf Dauer kostspieliger sein, als zeitnah aufzurüsten.

Was tun mit alten Rechnern?

Abgesehen von Entsorgen und Neukaufen steht Firmen und auch Privatleuten frei, die Geräte mit einem anderen Betriebssystem zu betreiben, sofern das möglich ist und in den Arbeitsprozess passt. Beispiele sind diverse Linux-Distributionen oder Chrome OS Flex von Google. Eine andere Möglichkeit wäre, diese Systeme nach einem Wiederaufbereitungsprozess inkl. Neuinstallation eines unterstützenden Betriebssystems zu spenden.

Quelle: https://www.connect-living.de/news/windows-10-support-ende-pcs-laptops-elektroschrott-canalys-3206608.html?utm_source=nachrichten-NL&utm_medium=newsletter

15) Firefox 121: Mozilla stopft Lücken und verbessert PDF-Unterstützung

In der neuen Firefox-Version 121 haben die Mozilla-Entwickler etliche Sicherheitslücken geschlossen. Für Firefox ESR, Tor Browser und Thunderbird stehen ebenfalls Updates bereit.

In der neuen Firefox-Version 121 haben die Mozilla-Entwickler vor allem Browser-Schwachstellen beseitigt. Der eingebaute PDF-Betrachter erhält eine Schaltfläche für mehr Komfort. Updates auf Firefox ESR 115.6.0, Tor Browser 13.0.7 sowie Thunderbird 115.6 sind ebenfalls verfügbar.

In Firefox 121.0 haben die Entwickler mindestens 18 Schwachstellen behoben. Darunter sind wenigstens fünf Lücken, die Mozilla in seinem Sicherheitsbericht als hohes Risiko einstuft. Ein Angreifer könnte die eine oder andere Sicherheitslücke ausnutzen, um Code einzuschleusen und auszuführen. So besteht etwa die Schwachstelle CVE-2023-6856 in einem Pufferüberlauf bei der Nutzung von WebGL auf Systemen mit Mesa VM-Treiber. Angriffe auf Firefox-Nutzer sind bislang nicht bekannt.

Kleinere Neuerungen in Firefox 121

Große Neuigkeiten hat die Firefox-Version 121 nicht zu bieten. Unter Windows fordert Firefox jetzt zur Installation der Videoerweiterung AV1 (aus dem Microsoft Store) auf, falls diese nicht vorhanden ist. Diese ermöglicht Hardware-Unterstützung für das Dekodieren von AV1-Videos. Der PDF-Betrachter erhält eine schwebende Schaltfläche, mit der Operationen wie das Löschen von Text oder das Einfügen von Bildern einfacher werden sollen.

Firefox für Android offen für viele Erweiterungen

Mozilla ermöglicht es, mehr als nur eine kuratierte Auswahl aus 22 Browser-Erweiterungen in Firefox für Android zu nutzen. Hatte Mozilla die Zahl der nutzbaren Erweiterungen zunächst auf 50 erhöht, ist das Add-on-System seit 14. Dezember weit geöffnet. Seitdem ist die Zahl der für den Android-Browser verfügbaren Add-ons auf 518 gewachsen – Tendenz weiter steigend. Mozilla hat auch Firefox 121 für iOS freigegeben.

Firefox ESR, Tor Browser, Thunderbird

Firefox ESR 115 bekommt ein Update auf die Version 115.6.0, in der die Entwickler wenigstens 11 Lücken geschlossen haben. Auch für den auf Firefox ESR basierende Tor Browser ist ein Update verfügbar. Der neue Tor Browser 13.0.7 (für Windows, macOS, Linux und Android) basiert auf Firefox 115.6 und bringt die Erweiterung Noscript 11.4.29 mit. In der aktuellen Version 115.6.0 des Mail-Programms Thunderbird haben die Entwickler mindestens 11 Schwachstellen beseitigt, die weitgehend mit den Firefox-Lücken übereinstimmen.

Am 23. Januar will Mozilla Firefox 122 sowie Firefox ESR 115.7 veröffentlichen, die nächsten Streiche sollen im Vier-Wochen-Takt folgen.

Quelle: https://www.pcwelt.de/article/2176484/firefox-121-verbessert-pdf-unterstutzung.html?utm_date=20231228115503&utm_campaign=Security&utm_content=Title%3A%20Firefox%20121%3A%20Mozilla%20stopft%20L%C3%BCcken%20und%20verbessert%20PDF-Unterst%C3%BCtzung&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

16) Daten langfristig speichern – das ist die beste Methode

Die langfristige Speicherung digitaler Daten ist wichtig, aber auch herausfordernd. Archivierungs-CDs wie M-Discs bieten eine gute Lösung mit hoher Haltbarkeit.

Daten langfristig zu speichern, ist für viele Menschen und Organisationen von großer Bedeutung. Nicht nur Unternehmen oder wichtige Personen wollen, dass ihre Daten möglichst lange sicher verwahrt werden, sondern auch für Privatpersonen ist es sehr wichtig, dass sich persönliche Erinnerungen wie Fotos oder Videos sowie rechtliche oder finanzielle Dokumente möglichst lange aufbewahren lassen.

Die Herausforderungen bei der langfristigen Speicherung digitaler Daten sind vielfältig: Digitale Speichermedien wie Festplatten und SSDs können sich mit der Zeit verschlechtern und ausfallen. Dateiformate können veralten, sodass sie mit neuerer Software inkompatibel sind. Sicherheitsrisiken wie Hackerangriffe, Malware und Naturkatastrophen bedrohen ebenfalls gespeicherte Daten.

Die beste Option für die langfristige digitale Aufbewahrung sind Archivierungs-CDs vom Typ M-Disc (Millenial Disc). Im Gegensatz zu herkömmlichen CDs und DVDs verwenden sie eine spezielle Datenschicht aus Materialien, die gegen den Abbau durch UV-Licht und Feuchtigkeit resistent sind.

Die Hersteller versprechen, dass diese Discs bis zu tausend Jahre oder länger halten können – echte Tests sind dabei natürlich nicht umsetzbar. Die M-Discs gibt es in verschiedenen Speicherkapazitäten. Allzu teuer sind die Datenträger nicht, denn fünf Discs mit je 25 Gigabyte Speicher kosten knapp 20 Euro.

Um Daten für Jahrzehnte oder sogar für Jahrhunderte zu speichern, sollten Sie in Betracht ziehen, archivierungsfähige optische Discs wie M-Discs zu verwenden. Gleichzeitig kann Sie allerdings auch der haltbarste Datenträger nicht davor bewahren, regelmäßige Sicherungen durchzuführen, um Datenverlust vorzubeugen.

Tipp: Datenarchivierung: Das sind die besten Methoden
Die besten SSDs 2023: Kaufberatung & Tipps für jeden Geldbeutel

Quelle: https://www.pcwelt.de/article/1981720/daten-langfristig-speichern-m-disc.html?utm_date=20231228120455&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Daten%20langfristig%20speichern%20%E2%80%93%20das%20ist%20die%20beste%20Methode&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

Allgemeines:

1) Bußgelder ungültig? Diese Blitzer-Geräte kann man anfechten!

Manchmal trifft einen unerwartet der Blitzer. Jedoch ist der Bußgeldbescheid nicht in allen Fällen korrekt und deshalb oft erfolgreich anfechtbar.

In der Regel reicht eine **Geschwindigkeitsüberschreitung von 4 km/h** und schon sieht man **rot**. Genauer: das gleißende Licht der Radarfalle, auf deren Tarnungslist man hereingefallen ist.

Natürlich sind Geschwindigkeitsbegrenzungen wichtig und Raserei ist gefährlich. Jedoch **trifft einen** manchmal der **Blitzer unrechtmäßig**, denn auch die **Polizei** und die **Messgeräte sind nicht unfehlbar.**

Aber **wann ist man im Recht** und wann ist man **einfach nur zu schnell gefahren** und das Bußgeld gerechtfertigt? **Das erklären wir hier.**

Der Blitzer muss einen Mindestabstand zum Geschwindigkeitsschild haben

Die Polizei darf Blitzer **nicht wahllos** aufstellen. Es muss **ein Mindestabstand** vom **Geschwindigkeitsbegrenzungs-Schild** zum Blitzer bestehen, damit Autofahrer:innen Zeit haben, zu reagieren. Das Gleiche gilt auch für den Abstand von Ortstafeln zu Blitzern.

In den meisten Fällen beträgt der **vorgegebene Abstand 75 bis 200 Meter**. **Jedes Bundesland** hat den jeweils geltenden **Abstand festgelegt**. **Welcher Abstand** im **jeweiligen Bundesland gilt**, haben wir in der nachfolgenden Tabelle **zusammengefasst**.

Abstand zum Geschwindigkeitsschild nach Bundesländern

Bundesland	Mindestabstand in Metern
Bayern	200
Thüringen	200
Brandenburg	150
Bremen	150
Niedersachsen	150
Sachsen	150
Hessen	100
Rheinland-Pfalz	100

Bundesland	Mindestabstand in Metern
Saarland	100
Sachsen-Anhalt	100
Schleswig-Holstein	100
Mecklenburg-Vorpommern	100 bzw. 250 auf Autobahnen und Kraftfahrstraßen
Berlin	75 vor/ hinter Verkehrsschildern, welche eine Geschwindigkeitsänderung angeben), 150 vor/ hinter einer Ortstafel
Hamburg	Kein Mindestabstand vorgegeben
Nordrhein-Westfalen	Kein Mindestabstand vorgegeben

Hat die **Polizei den Blitzer** also **zu nah hinter dem Tempolimit-Schild** aufgestellt, ist der **Bußgeldbescheid anfechtbar**.

Aber natürlich gibt es auch hier **Ausnahmen**.

Dann gilt der Mindestabstand vom Schild zum Blitzer nicht

Auch wenn jedes **Bundesland den Mindestabstand** zwischen **Tempo-Schild und Blitzer festgelegt** hat, ist die Regel nicht ohne Ausnahmen.

In manchen Fällen ist der Mindestabstand auch **aufgehoben**. Diese Ausnahmen sind:

- Gefahrenstellen, wie Tempo-30-Strecken nahe Schulen und Altenheimen oder unübersichtliche Einmündungen
- Nach Geschwindigkeitsrichtern

Quelle: https://www.maennersache.de/bussgelder-unguelig-diese-blitzer-geraete-kann-man-anfechten-92655.html?utm_source=flipboard&utm_content=topic%2Fde-automobil

2) Hochwasser kommt: Diese Karte zeigt, ob Sie gefährdet sind

Das befürchtete Hochwasser kommt. Eine offizielle Karte zeigt für ganz Deutschland die aktuelle Hochwasserlage in Echtzeit.

Update 23.12.2023: Ein heftiger Sturm und extrem starker Regen führen zum befürchteten Hochwasser in vielen Teilen Deutschlands. Bereits jetzt steigen die Pegel vieler Flüsse deutlich und für den ersten und zweiten Weihnachtsfeiertag werden besonders hohe Pegel erwartet.

Auf hochwasserzentralen.de sehen Sie sofort, ob Ihre Gegend durch das Hochwasser gefährdet ist.

Update Ende, Beginn der ursprünglichen Meldung

Es geht los, die erwarteten Hochwasser kommen. Tauwetter und Regen führen nicht nur in Bayern zu Überschwemmungen, sondern zum Beispiel auch in Hessen und am Rhein.

In Teilen Bayerns fielen in der letzten Woche Unmengen von Schnee. Doch jetzt steigen die Temperaturen und dann schmelzen die Schneemassen, zudem kommen neue Niederschläge, die die durchnässten Böden aber kaum noch aufnehmen können. Die unvermeidliche Folge: Hochwasser in Teilen Deutschlands, vor allem an Rhein und Donau.

Diese Webseite informiert in Echtzeit über Hochwasser

Auf hochwasserzentralen.de sehen Sie jetzt sofort, wie in ganz Deutschland die Hochwasserlage ist.

Die Webseite zeigt eine Karte von Deutschland. Mit unterschiedlichen Farben wird der Pegel der Flüsse dargestellt. Klickt man die Punkte an, bekommt man Detailinformationen. Außerdem kann man sich die Hochwasserlage nach Bundesländern getrennt anzeigen lassen.

Aktuell sieht man zwar überwiegend noch viele grüne Punkte: Dort ist derzeit kein Hochwasser. Doch es gibt auch schon viele gelb eingefärbte Punkte. Das signalisiert „kleines Hochwasser“ und ein oranger Farbtupfer steht für „mittleres Hochwasser“.

Bedrohlich wird es, wenn der Punkt rot eingefärbt ist, was an einigen Stellen ebenfalls schon der Fall ist. Das signalisiert „großes Hochwasser“. Leuchtet der Punkt sogar in dunkelviolett, dann handelt es sich um ein „sehr großes Hochwasser“. Was das konkret bedeutet, ist von Bundesland zu Bundesland leicht verschieden.

Aktuelle Lage in Bayern: Angespannt

Derzeit springen in Bayern mehrere orange und auch ein paar rote Tupfer ins Auge. Dort können Gewässer über die Ufer treten. Für die Drei-Städte-Stadt Passau, traditionell eine von Hochwasser oft heimgesuchte Grenzstadt im Freistaat Bayern, gibt es dagegen derzeit noch keine Hochwasserwarnung.

Besonders wichtig ist aber diese ergänzende Karte mit den Hochwasserwarnungen. Darauf sieht man, wie große Teile Bayerns sowie Hessen. Thüringen und Niedersachsen und das Allgäu besonders gefährdet sind. Auch der Rhein ist als besonders gefährdet markiert.

Woher die Daten stammen

Die Seite hochwasserzentralen.de wird von den deutschen Bundesländern betrieben: „Jedes teilnehmende Bundesland stellt hierfür laufend aktuelle Daten einer Auswahl von Hochwassermeldepegeln und eine Kurzinformation zur aktuellen Hochwasserlage zur Verfügung. Weitere Pegeldaten werden von der Wasser- und Schifffahrtsverwaltung des Bundes (WSV) sowie den zuständigen Behörden der Nachbarländer bereitgestellt“.

Quelle: https://www.pcwelt.de/article/1196910/hochwasser-karte-deutschland-echtzeit.html?utm_date=20231228122810&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Hochwasser%20kommt%3A%20Diese%20Karte%20zeigt%2C%20ob%20Sie%20gef%C3%A4hrdet%20sind&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4