41. Cybercrime Newsletter

29.04.2024

1) Betrugs-Ticker – Gefälschtes Amazon-Schreiben: Kunden sollen in die Falle gelockt werden

Betrüger denken sich immer wieder neue Maschen aus, um Menschen um ihr Geld zu bringen. Wir zeigen Ihnen, wie gegenwärtig abgezockt wird.

Es ist eine regelrechte Abzockwelle, die derzeit über Konsumenten hereinbricht. Betrüger versuchen vor allem über digitale Kanäle, Zugang zu sensiblen Daten, Kreditkarten und Konten zu erhalten. Mit welcher Masche sie zurzeit unterwegs sind, lesen Sie immer aktuell hier.

++ Amazon-Kunden sollen abgezockt werden (19.04.2024) ++

Kunden des Online-Händlers Amazon sind zunehmend Ziel von Phishing-Angriffen. Diese Woche kursiert eine E-Mail, die sich als Mitteilung des Unternehmens ausgibt und die Empfänger zur Überprüfung ihrer "Amazon-Kontosicherheit" auffordert, wie die Verbraucherzentrale berichtet.

Die Betrugs-E-Mail behauptet, es seien "ungewöhnliche Anmeldeaktivitäten" auf dem Nutzerkonto festgestellt worden. Aus diesem Grund sollen die Benutzer "zur Sicherheit" ihr Passwort zurücksetzen. Hierbei wird eine dreistufige Anleitung bereitgestellt: Nutzer werden gebeten, sich über einen in der E-Mail enthaltenen Button bei ihrem Konto anzumelden, daraufhin erhalten sie einen Code zum Zurücksetzen des Passworts und werden dann dazu angeleitet, den Prozess abzuschließen. Zusätzlich beinhaltet die E-Mail einen Kontaktverweis für eventuelle Fragen.

amazon

Amazon-Kontosicherheit

Liebe Kundin, lieber Kunde,

Wir haben ungewöhnliche Anmeldeaktivitäten auf Ihrem Amazon-Konto festgestellt. Um die Sicherheit Ihres Kontos zu gewährleisten, bitten wir Sie, Ihr Passwort zurückzusetzen. Bitte folgen Sie den folgenden Schritten:

1. Klicken Sie auf die Schaltfläche unten, um sich bei Ihrem Amazon-Konto anzumelden.
2. Nach der Anmeldung werden Sie aufgefordert, einen Code zur Zurücksetzung Ihres Passworts anzufordern.
3. Befolgen Sie die bereitgestellten Anweisungen, um den Vorgang zur Passwortzurücksetzung abzuschließen.

Anmelden und Code anfordern

Sollten Sie diese Aktion nicht selbst durchgeführt haben oder weitere Unterstützung benötigen, können Sie uns gerne kontaktieren.

Vielen Dank für Ihre prompte Aufmerksamkeit in dieser Angelegenheit.

Das falsche Amazon-Schreiben: Hier sollen Kunden des Online-Händlers in die Falle gelockt werden. verbraucherzentrale.de

Experten warnen jedoch eindringlich davor, den Anweisungen in dieser E-Mail zu folgen. Es handelt sich hierbei um einen klaren Fall von Phishing – einem Versuch von Kriminellen, an sensible persönliche Daten zu gelangen. Bereits das unseriöse Layout und die verschiedenen Schriftarten seien Indizien dafür, dass die Nachricht nicht tatsächlich von Amazon stammt. Die unpersönliche Anrede sowie die fehlerhafte Absenderadresse seien weitere Hinweise auf den betrügerischen Charakter der E-Mail.

Nutzer sollten daher aufmerksam sein und solche E-Mails am besten an den Spam-Ordner weiterleiten, raten die Verbraucherschützer.

++ Wieder angebliche Weintester am Werk (18.04.2024) ++

Schon im Herbst letzten Jahres warnte das Deutsche Weininstitut vor Betrügern, die im Namen der Einrichtung anriefen und sich als Weintester ausgaben. Nun wird die Masche erneut angewandt. Berichtet wird von Anrufen mit einer Berliner Vorwahl (030 31875721). In dem aktuellen Fall, der t-online berichtet wurde, meldete sich ein Mann in gebrochenem Deutsch und erklärte, eine Umfrage für das Deutsche Weininstitut machen zu wollen.

So gehen die Betrüger weiter vor: Sie befragen die Betroffenen zu ihren Weinvorlieben, wie etwa: "Trinken Sie lieber Weißwein, Rosé oder Rotwein?", "Trinken Sie täglich, mehrfach die Woche oder selten?", "Bevorzugen Sie trocken oder lieblich?", warnt das Deutsche Weininstitut. Versuche man die Verbindung zu beenden, werde ein Überraschungsgeschenk versprochen. Schließlich würden die Anrufenden nach dem vollen Namen und der Adresse fragen, um das Geschenk zustellen zu können. Teilweise werden auch Daten der Kreditkarte abgefragt.

Das Deutsche Weininstitut rät:

- Geben Sie in keinem Fall persönliche Daten heraus. "Das Deutsche Weininstitut führt generell keine Umfragen dieser Art durch", sagte ein Sprecher t-online. Und Umfragen von seriösen Instituten erfolgen anonym. Wer Daten weitergibt oder einwilligt, erneut kontaktiert zu werden, kann sich plötzlich mit unzähligen Werbeanrufen konfrontiert sehen.
- Melden Sie die Nummer bei der Bundesnetzagentur, wenn Sie denken, dass es sich um einen Betrüger handelt.
- Berichten Sie Ihrer Familie und Ihren Bekannten über das Vorgehen zu derartigen Anrufen. Die Nummer kann man im Festnetztelefon oder Smartphone blockieren, wenn man sich dauerhaft belästigt fühlt.

Sie wollen Nummern sperren und wissen nicht wie? Lesen Sie hier alles dazu.

++ Lovescamming: Alte Dame betrogen (13.04.2024) ++

Eine Seniorin aus Mecklenburg-Vorpommern ist in einem Fall von Lovescamming (auf Deutsch: Liebesbetrug) um rund 25.000 Euro betrogen worden. Das berichtet die Polizei in Stralsund. Sie schreibt: "Über mehrere Monate erkämpfte sich ein mutmaßlicher Betrüger einen Platz im Herzen der 74-Jährigen." Der Mann habe die alte Dame dazu gebracht, die große Summe in mehreren Schritten an fremde Personen zu überweisen.

Seit Mitte Dezember 2023 hatte der angebliche Verehrer, der sich als Autohändler vorgestellt hatte, die Seniorin umgarnt. Er hatte sie zuvor über eine Dating-Plattform kontaktiert, schickte ihr Blumen und eine Karte, um sich ihr Vertrauen zu erspielen. Dann sprach der Mann plötzlich von Geldsorgen und forderte die Frau auf, ihm Geld zu geben. Die 74-Jährige sei dem nachgekommen, heißt es in der Polizeimeldung. Als der Frau dann doch Zweifel an der Ehrlichkeit des Mannes kamen, erstattete sie Anzeige.

Die Polizei in Stralsund warnt vor der Masche des Lovescamming und mahnt zur Vorsicht.

Wie der Liebesbetrug abläuft und wer gefährdet ist, lesen Sie hier.

++ Vorsicht vor dieser gefälschten Commerzbank-Mail (12.4.2024) ++

Betrüger versuchen zurzeit, Commerzbank-Kunden dazu zu bringen, ihre Kontendaten offenzulegen. In einer E-Mail werden Kunden darüber informiert, dass die Bank aufgrund geltender Gesetzgebung dazu verpflichtet sei, einen Beitrag zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu leisten.

Werde ein Kundenfragebogen nicht sofort ausgefüllt, würden "alle Vertragsbeziehungen" bis zum 13.4.2024 beendet, wird in der E-Mail gedroht. Und sogar noch mehr: Kommen Kunden der Aufforderung nicht nach, werde die Bankkarte für Zahlungen gesperrt, heißt es.

"Gehen Sie dem nicht nach", warnt die Verbraucherschutzzentrale. "Dass es sich hier um einen Betrugsversuch handelt, lässt sich an der fehlenden Anrede, der kurzen Fristsetzung, dem unseriösen Layout und dem fehlenden Logo der Bank erkennen. Fallen Sie nicht auf solche Betrugsmaschen rein." E-Mails dieser Art (sogenannte Phishing-Mails, lesen Sie hier alles dazu) sollten sofort und unbeantwortet in den Spam-Ordner verschoben werden, raten die Experten.

Betrug: Mit dieser Mail sollen derzeit Commerzbank-Kunden eingeschüchtert und abgezockt werden. verbraucherzentrale.de

Tipp: Der Betrugs-Ticker wurde neu aufgesetzt: Den alten Ticker mit weiteren Maschen finden Sie hier.

Quelle: https://www.t-online.de/digital/aktuelles/id_100388342/betrugsmasche-amazon-kunden-sollen-mit-phishing-mails-abgezockt-werden.html

2) Finanzagenten: Vorsicht bei schnellem und leichtverdienten Geld

„Beste Verdienstmöglichkeit mit wenig Arbeit“ - mit solchen Jobangeboten locken Kriminelle ihre Opfer. In Jobbörsen, Internetauftritten oder per E-Mail geben sie sich als Vertreter scheinbar seriöser „Finanzmanagementunternehmen“ oder Ähnliches aus und sprechen in immer größer werdendem Umfang Inhaber von Bankkonten in Deutschland an.

Das Bundeskriminalamt und die Landeskriminalämter warnen nachdrücklich vor dubiosen Stellenangeboten und Nebenverdienstmöglichkeiten, in denen unbekannte Unternehmen nach so genannten Finanzagenten suchen.

Aktuelle Entwicklungen zeigen, dass immer mehr Bürgerinnen und Bürger auf die Betrugsmasche hereinfallen, ohne sich der Folgen bewusst zu sein. Die Finanzagenten werden dabei **nicht nur um ihr eigenes Geld gebracht**, ihnen droht auch eine Strafanzeige wegen des Verdachts auf Geldwäsche.

Ziel der Betrüger ist es, ahnungslose Kontoinhaber für eine **Tätigkeit als so genannte Finanzagenten** zu gewinnen (weitere Bezeichnungen für angebotene Stellen: „Financial Agent“, „Finanzmanager“, „Escrow Agent“, „Treuhandagent“, „Lieferungsmanager“, „Finanztransaktionsmanager“, „Projekt Koordinator“, „Prozessmanager“, „Regional Manager für Zahlungsbearbeitung“).

Der Finanzagent muss nur das eigene Girokonto für Überweisungen zur Verfügung stellen. Darüber soll der Finanzagent dann Geldbeträge, die Dritte auf sein Konto überwiesen haben, möglichst umgehend per Bargeldversand oder über Finanztransferdienstleister (wie z.B. Western Union) an eine im Ausland befindliche Person transferieren. Als Belohnung winkt eine **Provision zwischen fünf und 20 Prozent**, die vom Überweisungsbetrag einbehalten werden darf.

Es kommt auch immer häufiger vor, dass Gelder in Kryptowerte umgewandelt werden sollen und die Finanzagenten dazu gebracht werden, neben ihren eigenen Konten auch Kryptoaccounts auf ihren Namen zu verwenden.

Herkunft der Gelder

Die auf das Konto des Finanzagenten überwiesenen Gelder stammen von Personen, die selbst Opfer u.a. betrügerischer Machenschaften geworden sind. Dies führt dazu, dass die ursprüngliche Überweisung von diesen Opfern widerrufen wird. Weil aber der Finanzagent seinerseits die Geldbeträge weiter überwiesen hat, bleibt er auf dem dadurch entstehenden Schaden sitzen. Die Betrugshandlungen resultieren hauptsächlich entweder

- aus **„Phishing“-Aktionen** - hierbei werden Kontozugangsdaten erschlichen; dann überweisen Betrüger Geldbeträge vom Opferkonto auf Konten von vorher angeworbenen Finanzagenten. Und die wiederum transferieren das Geld weiter ins Ausland. Hierdurch entstehen erhebliche Vermögensschäden;
- oder aus **betrügerischen Internet-Auktionen** - auf Internet-Auktionsplattformen werden Waren zu einem ungewöhnlich niedrigen Preis angeboten. Der Käufer soll den Kaufpreis auf das Konto eines Finanzagenten überweisen; die erstandene Ware wird allerdings nie übersandt.

Wie werben die Betrüger ihre Opfer an?

Durch die Medienberichterstattung, die Warnhinweise von Polizei und Banken sowie die mittlerweile erfolgten Verurteilungen von Finanzagenten haben die Kriminellen Schwierigkeiten, eine angemessene Anzahl von Finanzagenten zu rekrutieren.

Daher greifen die Täter **ständig zu neuen Methoden**. Die Finanztransaktionen verlaufen dabei fast immer nach dem gleichen Grundmuster, allerdings variieren die Legenden zu ihrer Begründung:

Angeblich irrtümlich auf Privatkonten überwiesene Beträge

Die Kriminellen überweisen Geldbeträge, die sie ergaunert haben, an einen Kontoinhaber, der dadurch **ohne sein Wissen in die illegalen Machenschaften eingebunden** wird. Dieser Betrag wird von den Tätern unter einem Vorwand (z.B. Geld wurde irrtümlich auf falsches Konto überwiesen, sei aber für einen Freund im Ausland bestimmt) zurückgefordert, wobei der als Finanzagent missbrauchte Kontoinhaber für die entstandenen Unannehmlichkeiten einen Teil des Geldes behalten darf. Die Rücküberweisung soll allerdings nicht auf das

Ursprungskonto gehen, sondern auf ein anderes Konto, oftmals im Ausland, transferiert werden. Dort verliert sich die Spur.

Vortäuschen eines Arbeitsverhältnisses

Eine Firma sucht per Internetauftritt **„Repräsentanten und Manager“ für „Zahlungsbearbeitung“ und/oder „Warenverkehr“**. Interessenten werden gebeten, sich per E-Mail zu bewerben. Dem Bewerber wird nach einigen Tagen ein Arbeitsvertrag zugeschickt, der dem **Betrug einen offiziellen Anschein geben** soll und der sogar noch bestätigt, dass das Konto nur für seriöse und legale Geschäfte genutzt wird. Nachdem der Bewerber als neuer „Arbeitnehmer“ unterschrieben hat, gehen auf seinem Privatkonto Gelder von angeblichen Kunden der Firma ein. Diese Geldbeträge soll der „Arbeitnehmer“ auf Konten im Ausland weiter transferieren.

Eine Variante besteht darin, dass der „Arbeitnehmer“ von den eingegangenen Geldbeträgen an entsprechenden Verkaufsstellen so genannte „Vouchers“ kaufen soll. Dabei handelt es sich um PIN-Codes, die als elektronische Zahlungsmittel im Internet genutzt bzw. wieder in Geld rückgetauscht werden können. Diese PINs soll der „Arbeitnehmer“ an die E-Mail-Adresse seines „Arbeitgebers“ weiterleiten.

Im Rahmen von anderen Jobangeboten sollen die Angeworbenen, z.B. als App-Tester, Kontoeröffnungen über entsprechenden Online Verfahren durchführen, angeblich um deren Abläufe zu bewerten. Was sie dabei nicht wissen ist, dass sie damit tatsächlich Konten eröffnet haben, die dann ohne eigenen Zugriff für die Abwicklung/Weiterleitung von Geldern aus Straftaten genutzt werden.

Kontoeröffnung durch Finanzagenten für angeblichen Internetversandhandel

Getarnt als Nebenjob, auf den man sich aufgrund einer Internetstellenanzeige bewerben konnte, sollen Interessenten ein Konto eröffnen. Dann müssen sie nichts weiter tun als die **Kontodaten an die Nebenjobfirma weiterleiten** und eingehende Gelder weiter transferieren. Diese Konten der als Finanzagenten angeworbenen Personen werden als **Empfängerkonten für betrügerische Online-Shops angegeben**, die auf Internetseiten mit „unschlagbar günstigen Preisen“ für hochwertige Elektronikgeräte wie z.B. i-Pods oder Spielkonsolen werben. Der Finanzagent wird als Strohmann genutzt. Die eingehenden Geldbeträge werden (nach Abzug einer „Provision“ in Höhe von fünf bis zehn Prozent) auf ein ausländisches Konto weiter überwiesen.

Vortäuschung von Partnersuche

Auf Dating-Seiten im Internet suchen die Betrüger nach Opfern, die für sie **Geldbeträge über das eigene Konto weiterleiten** sollen. Ist ein vertrauensvoller Kontakt hergestellt, bitten die Betrüger das Opfer, sein Konto aus verschiedenen Gründen (z.B. weil sämtliche Papiere und Kontounterlagen gestohlen wurden) für eine Transaktion zur Verfügung zu stellen bzw. eingehende Geldbeträge weiter zu überweisen. So werden Kontoinhaber **unwissentlich als Finanzagenten missbraucht**, z.B. zur Zahlung von Flugkosten, zur Lösung einer Notlage in der Familie etc. Tatsächlich stammen die Beträge aus kriminellen Handlungen und sollen auf diese Weise „gewaschen“ werden.

„Warenagenten“

Personen werden über das Internet geworben, **ihr Konto für die Überweisung von Geldbeträgen zur Verfügung** zu stellen, mit denen sie hochwertige Waren (z.B. TV, Computer, Handys) kaufen und an bestimmte Adressen, die ihnen mitgeteilt werden, gegen Provision weiter verschicken sollen. Bei den überwiesenen Beträgen handelt es sich allerdings um Gelder aus kriminellen Taten.

Persönliche Kontaktaufnahme

Während bei den bisher geschilderten Anwerbungspraktiken die Kommunikation zwischen Anbieter und Kunde per E-Mail erfolgte, gehen die Täter mittlerweile auch dazu über, Finanzagenten **persönlich** zu kontaktieren. Personen werden **auf der Straße oder in öffentlichen Einrichtungen angesprochen** und ihnen wird ein Problem im Zusammenhang mit einer Überweisung ins Ausland geschildert. Der Angesprochene wird dann gebeten, eine Überweisung (von inkriminierten Geldern) gegen eine Belohnung in Form eines Geldbetrags zu veranlassen.

Insbesondere **Personen mit Migrationshintergrund werden von Landsleuten angesprochen** und gebeten, ihr Konto für den Transfer von Geldern - z.B. für einen kranken Verwandten im Ausland - zur Verfügung zu stellen. Die Korrespondenz findet oft in der Muttersprache statt, wobei stets betont wird, dass man sich „unter Landsleuten“ helfe.

- Wenn Ihnen ein lukrativer **Job per unverlangt erhaltener E-Mail** angeboten wird, bei dem Sie unüblich viel Geld verdienen können ohne eine entsprechende Leistung zu erbringen, ist davon auszugehen, dass das Angebot unseriös ist. Antworten Sie nicht auf solche dubiosen E-Mail-Angebote und stellen Sie keinen Kontakt zum Absender her.
- Lehnen Sie Angebote immer ab, bei denen Sie Ihr Konto zur Abwicklung von Zahlungen zur Verfügung stellen sollen. Lassen Sie sich **nicht von verlockenden Provisionsangeboten blenden**.
- Prüfen Sie Ihre Kontoumsätze auf **unerwartete Gutschriften**, die Sie wieder zurück-überweisen sollen. Nehmen Sie Kontakt zu Ihrer Bank oder zur Polizei auf. Rückbuchungen sollten nur auf das Ursprungskonto erfolgen.

Grundsätzlich gilt: Je verlockender ein Angebot ist, desto misstrauischer sollten Sie sein!

Strafrechtliche Konsequenzen

Was Finanzagenten oft nicht ahnen: Statt vermeintlich lukrativer Geschäfte drohen Freiheits-strafen wegen leichtfertiger Geldwäsche (§ 261 Abs. 5 StGB) und Schadensersatzansprüche der Geschädigten. Daneben erwartet sie ein Verfahren der Bundesanstalt für Finanzdienst-leistungsaufsicht (BaFin) wegen des Betreibens unerlaubter Finanzdienstleistungsgeschäfte. Außerdem kündigen Banken regelmäßig das Konto eines Finanzagenten. Dem Finanzagenten **droht ein Strafverfahren wegen Geldwäsche**. Indem er sein Konto zur Verfügung stellt und die eingegangenen inkriminierten Gelder schnell weiter transferiert, hilft der Finanzagent dabei, Herkunft und Transferwege des Geldes zu verschleiern. Damit macht er sich **zumindest der leichtfertigen Geldwäsche schuldig** (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe).

Verwaltungsrechtliche Konsequenzen

Da Finanzagenten für ihre Tätigkeit eine Provision erhalten, betreiben sie gewerbsmäßig ein Finanztransfergeschäft. Sie erbringen damit Finanzdienstleistungen, für die eine Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erforderlich ist. Liegt diese nicht vor, kann die **BaFin gegen Finanzagenten wegen unerlaubten Betreibens** von Finanz-dienstleistungen ein Verwaltungsverfahren einleiten. Der Verstoß kann mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden.

Zivilrechtliche Konsequenzen

Ferner können die Opfer, von denen die überwiesenen Gelder stammen, **zivilrechtlich gegen die Finanzagenten vorgehen** und eine Rückzahlung einfordern.

Quelle: https://www.polizei-beratung.de/themen-und-tipps/betrug/finanzagenten/

3) Aktuelle Betrugsmaschen – Aktuelle Betrugsmaschen: Amazon- und Klarna-Kundschaft im Visier

"Das kann mir nicht passieren": Wenn es um Betrug geht, sollte niemand mehr so denken. Besonders im Internet werden die Maschen immer ausgeklügelter. Damit Sie richtig reagieren, halten wir Sie hier auf dem Laufenden.

Update vom 22. April: Jeder muss zu jeder Zeit mit Phishing-Mails rechnen. Manchmal häufen sich aber die Attacken gegen bestimmte Kundengruppen so deutlich, dass die Verbraucherzentrale gezielte Warnungen ausspricht. Häufig geht es um Phishing-Mails an Kunden bestimmter Bankinstitute, in diesem Monat etwa der ING und der Comdirect. In den vergangenen Tagen erscheint auf dem Phishing-Radar Verbraucherschützer die Kundschaft des Zahlungsanbieters Klarna und verstärkt die des Online-Versandriesen Amazon.

- **Klarna:** Betreff und Überschrift der E-Mail lauten "Lastschriftmandat erneuern", die Adressaten werden persönlich angeredet und dazu gedrängt, zeitnah ihre Daten zu aktualisieren.
- **Amazon:** Die E-Mail dreht sich um "Amazon-Kontosicherheit", denn angeblich seien "ungewöhnliche Anmeldeaktivitäten" festgestellt worden. "Zur Sicherheit" solle der Kunde das Passwort zurücksetzen. Dafür folgt eine Anleitung mit drei Schritten.

Beide E-Mails enthalten einen Button mit einem hinterlegten Link. Am Ende geht es immer darum, dort sensible Daten anzugeben. E-Mails dieser Art sollten immer sofort und unbeantwortet in den Spam-Ordner wandern.

Ein Cent aufs Konto überwiesen? Vorsicht, das ist nicht immer etwas Gutes

Update vom 19. April: Aus aktuellem Anlass ruft die Polizei einmal mehr dazu auf, wachsam zu sein bei eigenartigen Kontobewegungen. Im konkreten Fall wurde ein 70-Jähriger aus Dessau Opfer von Betrügern, nachdem ihm Mitte März genau ein Cent von seinem Konto abgebucht worden war.

Drei Tage später landete der Cent wieder auf seinem Konto. Es dauerte eine Woche, bis es erneut zu einer Abbuchung kam: Diesmal zog eine angebliche Sportstätte aus dem europäischen Ausland unberechtigt 30 Euro von seinem Konto ein.

Ein-Cent-Überweisungen sind ein bekanntes Phänomen. Nicht immer stecke dahinter Betrug, klärt die Verbraucherzentrale Bayern auf Anfrage unserer Redaktion auf: "Eigentlich ist die 1-Cent-Überweisung dazu geeignet, eine funktionierende Kontoverbindung des Vertragspartners zu verifizieren", sagt Sascha Straub, Leiter des Referats Finanzdienstleistungen. Unternehmen nutzen also immer wieder diese Methode, um das Konto eines neuen Kunden zu überprüfen. "In der Praxis wird dies jedoch häufig missbraucht, um kostenlos unerwünschte Werbebotschaften auf Kontoauszügen zu verbreiten oder schlimmer noch, um unbefugt an Kontodaten zu gelangen, um dann Lastschriften einzuziehen oder diese für andere Betrügereien zu nutzen."

Der Rentner aus Dessau handelte genau richtig, indem er gegen die Zahlungen vorging. "Wer unerklärliche Zahlungseingänge bemerkt, sollte umgehend seine Bank informieren", rät Straub.

Kriminelle nutzen EM-Vorfreude aus - Warnung vor unseriösen Angeboten

Update vom 18. April: Nach den Siegen der deutschen National-Elf gegen Frankreich und Niederlande sind in Deutschland die EM-Vorfreude und -Hoffnungen spürbar gestiegen. Und damit bei vielen auch die Versuchung, um jeden Preis noch Tickets zu ergattern. Genau

davor warnen Experten aktuell und raten eindringlich zur Vorsicht: Im Netz tummeln sich unseriöse und betrügerische Angebote. Die Chance, noch auf offiziellem Weg Karten für das Turnier in Deutschland zu bekommen, sind sehr begrenzt. Das Verbraucherschutzportal "Watchlist Internet" weist deshalb auf die Gefahr horrender Preise einerseits und Fake-Angebote andererseits hin.

Kriminelle nutzen besonders soziale Medien wie Facebook, Instagram, Telegam und TikTok gerne für Werbung. "Wenn sie hier auf Angebote für EM-Tickets stoßen, die nicht über die offiziellen Vertriebskanäle laufen, raten wir zu Abstand. Keinesfalls sollten Sie Vorabüberweisungen vornehmen", warnen die Verbraucherschützer.

Vorsicht auch bei Angeboten mit horrenden Preisen: Gemäß den Allgemeinen Geschäftsbedingungen für den EM-Ticketverkauf ist der unautorisierte Weiterverkauf von Tickets verboten. "In den wenigen Ausnahmen, in denen ein Weiterverkauf genehmigt ist, ist außerdem festgelegt, dass keine zusätzliche Gegenleistung, die über den Ticketpreis hinausgeht, von Käufern verlangt werden darf. Ein Verkaufen mit Gewinn bzw. das Verrechnen einer Bearbeitungsgebühr für den Kauf der Tickets ist somit untersagt", stellt "Watchlist Internet" klar.

Die gute Nachricht: Anfang Mai startet noch einmal eine offizielle Vergaberunde für die Tickets! Die letzten verfügbaren Karten werden dann nach der Gruppenphase verteilt, wie die UEFA mitteilt. Fans, deren Nationen es in die K.O.-Phase schaffen, soll das noch einmal Chancen eröffnen.

Vorsicht beim Googeln nach Telefonnummern

Update vom 11. April: Sie googeln die Telefonnummer des Kundendiensts eines Unternehmens und stoßen auf Kontaktdaten, hinter denen sich Betrüger verbergen: Vor dieser Falle warnen Experten von "Watchlist Internet".

Aktuelles Beispiel: Booking.com. "Kriminelle erstellen Fake-Websites mit Booking-Logo und blenden Telefonnummern ein", warnen die Verbraucherschützer des Portals. Wer diese Nummern anruft und den Anweisungen folgt, verliert womöglich hohe Geldsummen.

Bei Kontaktaufnahme geben sich die Betrüger als vertrauenerweckende Booking.com-Mitarbeiter aus und fordern dazu auf, eine Software zu installieren. Vorsicht! "Wenn Sie eine Fernwartungssoftware installieren und Ihrem kriminellen Gegenüber den Zugriff auf Ihr System gewähren, kann Schadsoftware installiert werden und in weiterer Folge könnten beispielsweise Ihre Eingaben über die Tastatur ausgelesen werden. Kriminelle können so unter anderem auf Online-Banking-Daten zugreifen oder sogar Zahlungen auslösen", warnt "Watchlist Internet".

Nicht nur der Name von Booking.com würde für diese Betrugsmasche missbraucht, heißt es. Daher gilt es, immer auf der Original-Website nach dem Kundenservice zu suchen. Zudem sollte man nie Zahlungsdaten am Telefon preisgeben oder Fernwartungssoftware auf dem Computer installieren.

"Dreiecksbetrug" kann jeden Online-Schnäppchenjäger treffen

Update vom 10. April: Misstrauen und hohe Wachsamkeit sind die einzigen Mittel, die vor dieser ausgeklügelten Betrugsmasche schützen. Sie kann letztlich sonst jeden Online-Schnäppchenjäger treffen. Das Verbraucherschutzportal "Watchlist Internet" warnt aktuell davor.

So läuft es ab: Sie stoßen im Internet bei einer beliebten und namhaften Verkaufsplattform auf ein günstiges Produkt und bestellen sowie bezahlen es. Die gewünschte Ware kommt auch - doch nach einigen Wochen flattert Ihnen eine Mahnung ins Haus, da Sie die Ware

angeblich nicht bezahlt hätten. Bei genauem Hinsehen zeigt sich: Die Mahnung stammt von einem Shop, bei dem Sie die Ware gar nicht bestellt haben. Sowohl Sie als auch der Online-Shop, der Ihnen die Ware geliefert hat, sind Opfer von Betrug geworden.

Was dahintersteckt: Die Anzeige, die das Produkt angepriesen hat, war ein Fake. Häufig stecken dahinter gefälschte Nutzerprofile, die Betrüger mit gestohlenen Nutzerdaten erstellt haben. Letztlich haben Sie also bei Kriminellen bestellt und ihnen auch Ihr Geld übermittelt. "Damit Sie den Betrug nicht sofort bemerken, bestellen die Kriminellen das gewünschte Produkt mit Ihren Daten bei einem seriösen Onlineshop – in der Regel bei Shops, die Kauf auf Rechnung anbieten", erklären die Experten von "Watchlist Internet". "Sie erhalten das Produkt also nicht von der Plattform, bei der Sie eigentlich bestellt haben, sondern von einem anderen Shop." Ignorieren Sie die Mahnungen von diesem Shop, folgen Inkassoschreiben. Den Betrügern verschafft all das Zeit, um die Geldflüsse zu verschleiern und ihre Spuren im Internet zu verwischen.

Tipps, wie Sie sich vor dieser Art des "Dreiecksbetrugs" schützen:

- Seien Sie skeptisch, wenn ein Schnäppchen eigentlich zu gut scheint, um wahr zu sein. Verzichten Sie darauf, denn das Risiko, dass es sich um Betrug handelt, ist gewaltig.
- Überprüfen Sie die Absenderadresse, wenn Sie eine Lieferung erhalten: Kommt das Paket nicht von dem Shop, bei dem Sie bestellt haben, nehmen Sie Kontakt zum Absender auf.
- Wählen Sie eine sichere Zahlungsmethode, das heißt: mit Rückbuchungsmöglichkeit beziehungsweise Käuferschutz. Vorsicht: Bei der PayPal-Funktion "Geld an Freunde und Familie senden" haben Sie keinen Käuferschutz.

Mini-Haus oder Wohnmobil zu verschenken? Vorsicht!

Update vom 9. April: "Wir haben 5 Mini-Häuser, die wir aufgrund kleinerer Kratzer nicht verkaufen können". Nun sollen die kleinen Häuser angeblich verlost werden. Wieder einmal verbirgt sich Betrug hinter einem vermeintlich traumhaften Angebot. Wer dahinter steckt, ist nicht ersichtlich. Laut dpa handelt es sich definitiv um einen Fake.

Ebenso bei einem sehr ähnlichen Posting, in dem es heißt: "Aufgrund einiger kleiner Dellen und Kratzer" sei ein Autohaus "nicht in der Lage" gewesen, ein Wohnmobil zu verkaufen - und darum solle es jetzt bei Facebook verschenkt werden, heißt es bei Facebook. Eine "Freude" werde denjenigen gemacht, der den Post kommentiert.

Die offiziellen Facebook-Seiten von Unternehmen erkennt man oft an dem Verifikationsabzeichen, also einem kleinen weißen Häkchen auf blauem Grund. Das Zeichen bedeutet, dass die Seite des Unternehmens von Facebook geprüft und als echt anerkannt wurde. Dieses fehlt jedoch genauso wie Links zu einer Firma oder einem Händler und eine dazugehörige Adresse.

Oft zeigt auch eine Bilderrückwärtssuche bei Google, dass die Bilder von vermeintlichen Traum-Mini-Häusern oder -Wohnmobilen schon Jahre alt sind und nichts mit einem angeblichen Gewinnspiel zu tun haben.

Verbraucherschützer und die Polizei warnen immer wieder davor, bei dubiosen Gewinnspiel-Angeboten die eigene E-Mail-Adresse oder sonstige persönliche Daten weiterzugeben. Ein Motiv der Täter nämlich: Sie sammeln diese Daten und verkaufen sie im Darknet weiter. Dann werden sie für weitere Betrugszwecke missbraucht.

Quelle: https://web.de/magazine/ratgeber/finanzen-verbraucher/aktuelle-betrugsmaschen-amazon-klarna-kundschaft-visier-39464290

4) Die Schattenseite des Fahrradhandels – Betrugsalarm: Diese Fahrradshops sollten Sie meiden

Die Verbraucherzentrale Hamburg hat mehrere Hinweise auf betrügerische Fahrrad-Shops erhalten. Auf diesen Webseiten sollten Sie keinesfalls etwas bestellen.

Die Sonne scheint, Blätter sprießen an den Bäumen – und mit dem Frühling holen viele ihr Fahrrad aus dem Winterquartier. Vielleicht fällt dabei auf, dass der Drahtesel an einigen Stellen so abgenutzt ist, dass Ersatzteile hermüssen. Oder ist das Bike vielleicht so in die Jahre gekommen, dass ein neues ansteht?

Wer derzeit nach einem neuen Zweirad oder nach Zubehör sucht, sollte vorsichtig sein. Denn die Verbraucherzentrale Hamburg warnt vor betrügerischen Online-Händlern in diesem Bereich. Die Shops locken potenzielle Käuferinnen und Käufer mit vermeintlich günstigen Angeboten, etwa für hochwertige Räder und E-Bikes. Auch Ersatzteile und Zubehör wie Fahrradtaschen von Markenherstellern werden angeblich preiswerter angeboten. Das böse Erwachen kommt dann, nachdem Kundinnen und Kunden bezahlt haben.

Vorsicht vor diesen Online-Shops!

Nachdem das Geld geflossen ist, ist der Onlineshop plötzlich nicht mehr erreichbar und liefert die bestellte Ware nicht. Das haben mehrere Menschen der Verbraucherzentrale Hamburg über folgende Shops berichtet:

- eradprofi.com
- gravelbikede.com
- fahrradmeierigm.com
- bikeboys-onlineshop.net

Bei diesen vermeintlichen Händlern sollten Sie also keinesfalls etwas ordern. Denn die Ware wird meist per Überweisung oder Kreditkarte bezahlt. Das macht es schwerer, das Geld schnell zurückzuholen, so wie es zum Beispiel bei Lastschrift oder PayPal möglich ist. Schauen Sie also besser immer sehr genau hin, bevor Sie bei einem Ihnen noch unbekannten Online-Shop etwas bestellen. "Gerade beim Kauf von Saisonware ist Vorsicht geboten. Je attraktiver das Angebot, desto genauer sollte ein Shop geprüft werden", rät Julia Rehberg von der Verbraucherzentrale Hamburg.

So entlarven Sie Fake-Shops

Was sollten Sie tun, um einen Online-Shop als Fake zu erkennen? "Ein kurzer Blick ins Impressum der oft professionell gestalteten Internetseiten reicht leider oft nicht mehr aus", so Rehberg. Meist würden plausible Adressen in Deutschland mit Telefonnummer, Registernummer und Namen der Geschäftsführung angegeben.
Die Verbraucherschützerin empfiehlt, vor einer Bestellung zu kontrollieren, ob das Unternehmen tatsächlich unter der angegebenen Handelsregisternummer im Registerportal geführt wird. Auch die Telefonnummer aus dem Impressum sollten Sie testweise anrufen. Zudem schadet es nicht, einen Blick in die Liste von gefälschten Shops zu werfen, die die Verbraucherzentrale Hamburg führt. Falls Sie bereits Ware in einem Fake-Shop bestellt haben, rät die Verbraucherzentrale: Kontaktieren Sie Ihr Kreditinstitut und versuchen Sie, das Geld wieder zurückbuchen zu lassen. Erstatten Sie zudem umgehend Strafanzeige bei der Polizei. Das ist in Hamburg auch bei der Onlinewache der Polizei möglich.

Quelle: https://www.autobild.de/artikel/die-schattenseite-des-fahrradhandels-25721967.html

5) Betrugsmaschen – Betrugsopfer schildert Masche, bei der Totalverlust droht: "Heute weiß ich all das und es macht mich so wütend"

Psychologische Tricks und immenser technischer Aufwand: Welche Maschinerien Betrüger in Gang setzen, um arglose Menschen in die Falle zu locken, ist kaum zu glauben. Hier erzählt eine Betroffene ihre Geschichte, um andere zu warnen.

Es ist die Hoffnung auf den einen oder anderen unerfüllten Traum. Auf etwas mehr Polster für die Rente. "Ich war immer ein eher misstrauischer Mensch, ich hätte mir nicht mal ein Los auf der Kirmes gekauft", erzählt Eva-Maria Schirmer (*Name von der Redaktion geändert*).

Doch als die 68-Jährige vor wenigen Monaten Lena Meyer-Landrut in einem Online-Video von einer Handelsplattform schwärmen sieht, weckt das bei ihr Vertrauen. Vielleicht gibt es in diesen Zeiten von schlechten Zinsen und hohen Kosten ja doch noch eine Chance, an mehr Geld zu kommen. Wenn eine Prominente von solchen Gewinnen erzählt, warum sollte das nicht funktionieren?

Was Schirmer nicht ahnt: Das Video ist nicht echt, sondern eine mittels künstlicher Intelligenz (KI) erstellte Fälschung. Lena Meyer-Landrut hat nie für die genannte Trading-Firma geworben. Der Satz "Man darf nur glauben, was man selbst sieht und hört" gilt in Zeiten der neuen digitalen Möglichkeiten nicht mehr. Denn auch was man mit eigenen Augen sieht, kann Fake sein. Bereits vor Jahren klärte die Sängerin ihre Fans darüber auf, dass sie nicht mit Bitcoins handele und derlei Werbungen gefälscht seien.

Warnung vor Fake-Werbung

- *Vorsicht ist geboten, wenn Sie Promis im Internet für Handelsplattformen oder beispielsweise Gesundheitsprodukte werben sehen: Künstliche Intelligenz ermöglicht raffinierte Fakes, die oft nicht auf Anhieb als solche zu erkennen sind. In der Vergangenheit wurden dafür schon Fotos oder TV-Interviews von Promis wie Barbara Schöneberger, Judith Williams, Til Schweiger, Eckhart von Hirschhausen und Sandra Maischberger bearbeitet oder mittels einer KI-generierten Stimme synchronisiert. "In Zeiten von künstlicher Intelligenz werden solche Betrügereien vermutlich noch zunehmen", warnt Susanne Punsmann, Rechtsanwältin im Projekt "Faktencheck Gesundheitswerbung" der Verbraucherzentrale. Wer sich unsicher ist, kann Links und Screenshots zur Prüfung and die Verbraucherzentrale schicken.*

Beispiele für solche Fake-Werbung (weitere Artikel sind unter dem u.g. Link abrufbar)

- Finanztipp von Til Schweiger? Vorsicht!
- Judith Williams zeigt dreistes Beispielbild für Betrug

Traumhaft einfache Konditionen und schnelle Gewinne?

Als Schirmer den Online-Clip sieht, zweifelt sie nicht an seiner Echtheit und gibt die Adresse der namentlich genannten Handelsplattform direkt im Browser ein. Sofort landet sie auf einer optisch ansprechenden Seite. Aktienkurse laufen durch einen Ticker, Zitate von Mitarbeitenden und angebliche Auszeichnungen schmücken das Portal.

Es scheint alles so unkompliziert. Kein Vertrag, keine Kündigungsfristen – nur eine Mindestlaufzeit von 14 Tagen und der Einsatz von 250 Euro sind für die Anmeldung nötig. Den Rest, also möglichst schnelle und hohe Gewinne, erledige die Firma für die Anleger.

"Irgendwas hat mich geritten, wenn es auch nur der Gedanke war: 250 Euro zu verlieren, könntest du ja gerade noch verschmerzen. Ich dachte mir, ich mach das mal", erzählt Schirmer. Nach einem Impressum sucht sie nicht. Ein Fehler, wie ihr heute klar ist. "Ich habe mich damit zufriedengegeben, dass unten eine Adresse und ein Support-Kontakt angegeben waren", sagt die Rentnerin aus Köln, die früher als Steuerberaterin tätig war.

Wer solche Warnsignale übersieht und auf Fake-Trading-Plattformen reinfällt, dem drohe der Totalverlust, warnt die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin). Schirmers Erfahrungen seien typisch: Nach ihrer Registrierung gratuliert ihr eine angebliche Mitarbeiterin der Trading-Firma zu ihrer "guten Entscheidung", es folgen telefonische Kontaktaufnahmen. Die Betrüger verstünden es, im Laufe der Kommunikation einerseits Vertrauen, andererseits Druck aufzubauen, um die Anleger zu noch mehr Investitionen zu drängen.

So auch bei Schirmer. Jeder Log-in auf der Seite löst zudem euphorische Gefühle aus, denn der Profit steigt angeblich stetig: Binnen kurzer Zeit liegt ihr angebliches Guthaben schon fast bei 300 Euro. Was sie allerdings beunruhigt: Ihr Startkapital von 250 Euro hat sie zu Beginn nicht an die Firma direkt, sondern auf eine Bank im Ausland überwiesen.

Wie sie sich denn ihre Gewinne auszahlen lassen könne, will sie von ihrem "Kundenbetreuer" wissen, der sie regelmäßig anruft. Jedes Mal von einer anderen Nummer, wie ihr schnell auffällt. Wann immer sie auf solche Ungereimtheiten zu sprechen kommt und Fragen stellt, bricht er unter einem Vorwand das Gespräch ab und vertröstet sie auf einen anderen Tag. Schriftliche Kommunikation findet – auch ein typisches Warnsignal für Betrug - ausschließlich über WhatsApp statt.

Ein mysteriöses Angebot

Nach wenigen Wochen macht er ihr einen ungewöhnlichen Vorschlag: "Da meine Geschäfte doch so prima liefen, würde mir die Firma 20.000 Euro zur Verfügung stellen. So würde sich der weitere Handel für mich, aber auch für ihn als Berater mehr lohnen", erzählt sie.

Was nach diesem vermeintlichen Darlehen wohl passiert wäre: Ihre – fiktiven – Gewinne wären weiter rasant gestiegen. Dann wäre sie aufgefordert worden, ihre Schulden zuerst zu begleichen, bevor ihr der Gewinn ausgezahlt werden könne. Oder es wären Gebühren fällig geworden. Das vermutet Dominika Kula, Sprecherin bei der Bafin, auf Anfrage unserer Redaktion: "Sie wäre statt ihrer anfänglichen 250 Euro dann schnell 20.000 Euro losgewesen. Die Kriminellen gaukeln ihren Opfern vor, eine hohe Summe stünde vor der Auszahlung – vorher sei allerdings noch eine Steuerzahlung oder ähnliches fällig."

Als Schirmer sich nicht auf das Angebot einlässt, reagiert der Betreuer unwirsch. Ihr angebliches Guthaben liegt zu diesem Zeitpunkt – nach nur wenigen Wochen – bereits bei 928 Euro. Ein eindeutiges Kennzeichen für Betrug: Das Bundeskriminalamt und die Landeskriminalämter warnen immer wieder vor solchen unrealistischen Gewinnen.

Für Verbraucher, die ihr Geld anlegen möchten, ist wichtig zu wissen: Wer Finanzdienstleistungen anbietet, benötigt dafür die Erlaubnis der Bafin. Ob diese Lizenz vorliegt, kann jeder online nachschlagen. "Und das muss man vor einer Anlage auch unbedingt tun", betont Kula, "denn wenn Sie es mit jemandem zu tun haben, der in betrügerischer Absicht handelt, hat der logischerweise auch keine Erlaubnis. Vor solchen Fake-Anbietern und ihren zugehörigen Internetseiten warnen wir mehrmals täglich", erklärt sie und verweist auf aktuelle Warnmeldungen, in denen klangvolle Namen auftauchen wie "FX-GlobalMarkets" oder "finanzwelt.pro".

Wer ist die Bafin und welche Links sind für Verbraucher wichtig?

- Bafin steht für Bundesanstalt für Finanzdienstleistungsaufsicht. Für ein stabiles Finanzsystem beaufsichtigt die Behörde Banken, Finanzdienstleistungs- sowie Zahlungs- und E-Geldinstitute, deutsche Zweigniederlassungen ausländischer Kreditinstitute aus dem Europäischen Wirtschaftsraum, Versicherer und Pensionsfonds sowie Kapitalverwaltungsgesellschaften und inländische Fonds. **Link:** Tagesaktuelle Warnungen der Bafin zu unseriösen Plattformen
- Da es aber passieren kann, dass Verbraucher auf betrügerische Websites stoßen, die dort noch nicht erfasst sind, sollten Anleger online nachschlagen, wer die Erlaubnis der Bafin hat und somit seriös ist. **Link:** Unternehmensdatenbank der Bafin

Auch die Telefonnummern erweisen sich als Fake

Bald erlebt Schirmer die nächste Überraschung: Als sie sich in ihren Account einloggen will, ist die Webseite nicht mehr erreichbar. Über eine Google-Suche findet sie die Firma wieder – allerdings unter leicht geänderter Adresse im Internet. Nun schrillen alle Alarmglocken und sie versucht, ihren Kundenberater anzurufen. Über die abgespeicherten Nummern landet sie zuerst bei einer Hausfrau in Österreich, dann auf einem Anrufbeantworter in Belgien, schließlich bei einer offenbar ebenfalls völlig unbeteiligten Person in Frankreich.

Warnung vor Call-ID-Spoofing

- *Es ist möglich, Anrufe zu erhalten, die tatsächlich von einer anderen Nummer stammen als der auf Ihrem Display angezeigten. Man nennt diese Masche Call-ID-Spoofing. "Um eine Rufnummer zu manipulieren und bei Anrufen eine falsche Rufnummer zu übermitteln und anzeigen zu lassen, ist es nicht erforderlich, sich diese Rufnummer auf irgendeine Weise zu verschaffen, d.h. sie zu erwerben oder sie freischalten zu lassen", erklärt die Bundesnetzagentur. "Von der Manipulation betroffen sein können dabei einerseits real existierende – auch ausländische – Rufnummern, obwohl der Inhaber der Rufnummer mit dem Anruf nichts zu tun hat." Auch könnten bei diesem sogenannten Call-ID-Spoofing erfundene Rufnummern verwendet werden, die es also gar nicht gibt. Wer entsprechende Anrufe erhält, möge diese möglichst unverzüglich der Bundesnetzagentur melden, die dann unter bestimmten Voraussetzungen dann ermitteln kann.*

Gefälschte Telefonnummern, veränderte Domains, exorbitante Gewinne – als der Kundenberater wieder anruft, spricht Schirmer ihren Verdacht offen aus, dass das alles Betrug sei: "Er wurde dann sehr ungehalten und verstrickte sich in abenteuerliche Ausreden: Firmen änderten ja öfter ihre Domains - er wollte mir also Schwachsinn verkaufen. Mir reichte es. Ich sagte ihm, ich werde Anzeige erstatten und Himmel und Hölle in Bewegung setzen, um mein Geld zurückzubekommen."

Ein letztes Mal spielt ihr Anrufer auf Zeit und leitet sie am Telefon an, eine Auszahlung zu veranlassen. Das Geld werde nach zwei bis drei Werktagen ankommen. Das ist bis heute nicht der Fall. Schirmer hat inzwischen Anzeige erstattet und ihre Daten im Kundenbereich gelöscht. Ob die Betrüger diese damit nicht mehr zur Verfügung haben, ist mehr als fraglich. Laut Bundeskriminalamt sind Betrugsopfer besonders gefährdet, wieder ins Visier von Betrügern zu geraten. Häufig werden Daten an andere Kriminelle verkauft oder Betrüger melden sich mit vermeintlichen Hilfsangeboten: Sie geben sich als jemand aus, der dabei unterstützen will, das verlorene Geld zurückzuholen.

Hinter dem Betrug stecken riesige Netzwerke

Welche Maschinerie allein hinter Schirmers Fall steckt, was Betrüger also alles in Bewegung setzen, um Menschen zu täuschen, ist erstaunlich. Die Bafin bezeichnet an Schirmers

Erfahrungen als typisch, dass nie erklärt wird, wie die Kapitalanlage eigentlich genau funktioniert. Kein Wunder, sind doch auch die Gewinne viel zu hoch, um wahr zu sein. Eingezahlte Gelder werden nie einer Kapitalanlage zugeführt. Alles ist Fake. Das Geld wird nie ausgezahlt, sondern ist längst auf ausländische Konten verteilt.

Mit 250 Euro Verlust hatte sie noch "Glück im Unglück", weiß Schirmer, denn andere verloren durch Cyber Trading Fraud, wie Anlagebetrug auch genannt wird, schon Zigtausende Euro. Die Dimensionen zeigt auch ein Schlag gegen Anlagebetrug aus dem vergangenen Jahr: Eine einzige Bande hatte allein in Deutschland einen Schaden von 22 Millionen und international 89 Millionen Euro verursacht.

"Es sind gewaltige betrügerische Netzwerke, die da agieren und sich die Arbeit professionell aufteilen", erläutert Kula: "Die einen erstellen die Websites, die anderen agieren aus Telefoncentern, andere sorgen für den schnellen Geldtransfer ins Ausland, wo die Zuständigkeit deutscher Strafverfolgungsbehörden aufhört. Das erschwert die Ermittlungen. Und auch Domains lassen sich nicht so einfach sperren, wie wir uns alle das wünschen würden, wenn sie im Ausland gehostet sind", informiert sie.

Umso wichtiger sei die Aufklärung von Anlegern und immer wieder der Appell, intensiv zu recherchieren, bevor man Geld investiert: Impressum suchen (wer ist der potenzielle Vertragspartner und wo hat er seinen Sitz?), Firmennamen googeln und bei der Bafin eingeben und auch eine Google-Rückwärtssuche der Bilder kann im Handumdrehen aufdecken, dass hier gar keine echten Mitarbeitenden abgebildet sind. Im Zweifelsfall könne man sich auch an die Verbraucherzentrale wenden.

Die psychologischen Tricks der Kriminellen

"Die Betrüger spielen ja mit unserer 'Fear of missing out', der Sorge, etwas zu verpassen: Das Angebot könnte weg sein, wenn ich heute nicht zuschlage. Dieser Trick ist reine Psychologie und erwischt Menschen aus allen Schichten. Schlafen Sie immer darüber, wenn es um Ihr Geld und Ihre Daten geht und recherchieren Sie gründlich", warnt die Expertin der Bafin.

Die betrügerischen Handelsplattformen seien letztlich leere Hüllen im Internet, schnell erstellt und sogar immer wieder gleich unter verschiedenen Domains, deren Unterseiten oft schon ins Leere führten. Doch sie werden immer raffinierter. "Und die Betrüger sind mit ihren Anrufen vehement und hartnäckig. Hier muss man gesunden Menschenverstand walten lassen: Warum sollte mich jemand drängen zu investieren und mich unter Druck setzen, wenn er offenbar selbst die Lizenz zum Gelddrucken entdeckt hat?", gibt Kula zu bedenken.

"Heute weiß ich all das und es macht mich so wütend", sagt Schirmer. Im Internet fand sie weitere unseriöse Plattformen und will nun andere warnen: "Ich war wirklich immer wachsam. Ich habe noch nie so einen Blödsinn gemacht – und dann das. Man sollte nie sagen: Mir kann das nicht passieren."

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/betrugsopfer-schildert-masche-totalverlust-droht-weiss-all-wuetend-39561564

6) Geld & Shopping – Verbraucherzentrale warnt vor perfidem Comdirect-Betrug

Im digitalen Zeitalter, in dem nahezu jede Transaktion und jeder Bankauftrag online abgewickelt wird, ist Cybersicherheit von höchster Bedeutung. Kriminelle versuchen laufend über betrügerische Maschen an sensible Informationen und das Geld anderer zu gelangen.

In der Vergangenheit waren Phishing-E-Mails oft leicht zu erkennen, da sie entweder unpersönliche Anreden wie "Sehr geehrter Kunde ..." verwendeten oder durch fehlerhaftes Deutsch auffielen. **Doch heutzutage gehen die Kriminellen häufig wesentlich professioneller vor.** Skepsis ist also durchaus angebracht.

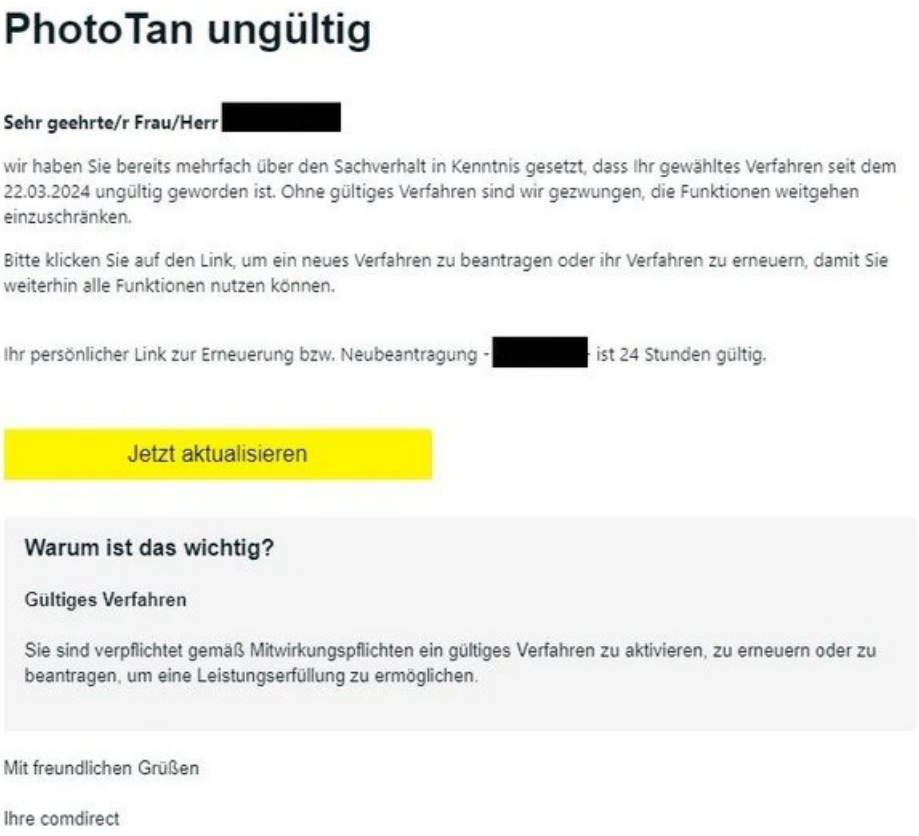
Aktuell kursieren laut der Verbraucherzentrale Phishing-Nachrichten, die sich wieder einmal an Bank-Kund:innen richten. Unter dem Deckmantel einer angeblichen offiziellen Mitteilung der Comdirect zielen sie darauf ab, das Vertrauen der Kundschaft zu missbrauchen und persönliche Daten zu ergattern.

Phishing-Betrug: Vorsicht bei dieser Comdirect-Nachricht

Die Verbraucherzentrale warnt: In einer kürzlich aufgetauchten Phishing-Mail, die angeblich von der Comdirect stammt, wird die Dringlichkeit einer wichtigen Aktualisierung als Grund vorgeschoben. Was diese betrügerische E-Mail besonders gefährlich macht, ist der Druck, den sie damit bei Commerzbank-Kund:innen erzeugt.

Den Empfänger:innen wird suggeriert, dass sie innerhalb eines begrenzten Zeitraums von 24 Stunden handeln müssen, um ihre Kontofunktionalitäten nicht zu verlieren. **Diese knappe Frist soll dazu führen, dass die Opfer in Unruhe geraten und ohne genaue Überprüfung des Links handeln.** Das soll Betrüger:innen Tür und Tor öffnen, um sensible Daten abzugreifen.

Unter dem Betreff "Bitte um Kenntnisnahme - Handlungsbedarf" werden die Kund:innen fälschlicherweise darüber informiert, dass ihr aktuelles PhotoTan-Verfahren seit dem 22.03.2024 nicht mehr gültig sei. Um weiterhin die Kontofunktionen nutzen zu können, werden sie aufgefordert, über einen bereitgestellten Link ein neues Verfahren zu beantragen.



PhotoTan ungültig

Sehr geehrte/r Frau/Herr [redacted]

wir haben Sie bereits mehrfach über den Sachverhalt in Kenntnis gesetzt, dass Ihr gewähltes Verfahren seit dem 22.03.2024 ungültig geworden ist. Ohne gültiges Verfahren sind wir gezwungen, die Funktionen weitgehen einzuschränken.

Bitte klicken Sie auf den Link, um ein neues Verfahren zu beantragen oder ihr Verfahren zu erneuern, damit Sie weiterhin alle Funktionen nutzen können.

Ihr persönlicher Link zur Erneuerung bzw. Neubeantragung - [redacted] ist 24 Stunden gültig.

Jetzt aktualisieren

Warum ist das wichtig?

Gültiges Verfahren

Sie sind verpflichtet gemäß Mitwirkungspflichten ein gültiges Verfahren zu aktivieren, zu erneuern oder zu beantragen, um eine Leistungserfüllung zu ermöglichen.

Mit freundlichen Grüßen

Ihre comdirect

Quelle: Die Verbraucherzentrale hat einen Screenshot einer betrügerischen Mail veröffentlicht. Bild: Verbraucherzentrale

Verbraucherzentrale warnt Kunden vor Betrug

Die Verbraucherzentrale warnt ausdrücklich davor, auf derartige Phishing-Mails zu reagieren. In solchen Fällen sei es ratsam, keine Links in verdächtigen E-Mails zu öffnen. **Im Zweifel wird den Betroffenen angeraten, direkt Kontakt mit der Bank aufzunehmen, um den Sachverhalt zu klären.**

Grundsätzlich aber gilt: **Banken fordern in der Regel keine Aktualisierung von Sicherheitsverfahren über Mail- oder Nachrichten-Links an.** Als zusätzliche Sicherheitsmaßnahme ist es ratsam, verdächtige Mails unbeantwortet in den Spam-Ordner zu verschieben und keinesfalls persönliche Informationen preiszugeben.

Phishing erkennen: Das sind mögliche Anzeichen

Typische Merkmale wie Tippfehler oder ungewöhnliche Umlaute sowie eine unpersönliche Anrede sind mittlerweile selten. Selbst bei gut formulierten Texten sollte man also skeptisch bleiben. **Das Bundesamt für Sicherheit in der Informationstechnik gibt Tipps, woran Phishing zu erkennen ist:**

- Die Nachricht drängt auf sofortige Maßnahmen, indem sie beispielsweise behauptet: "Ohne unverzügliche Aktualisierung Ihrer Daten riskieren Sie deren unwiederbringlichen Verlust ...".
- Es werden Drohungen ausgesprochen, wie etwa: "Wenn Sie dieser Aufforderung nicht nachkommen, wird Ihr Konto bedauerlicherweise gesperrt ...".
- Sie enthält eine Aufforderung, vertrauliche Informationen wie die persönliche Online-Banking-PIN oder Kreditkartennummer preiszugeben.
- Die E-Mail enthält Links oder Formulare, die zur Eingabe sensibler Daten auffordern.
- Obwohl die E-Mail den Anschein erweckt, von einer vertrauenswürdigen Person oder Organisation zu stammen, wirkt das Anliegen des Absenders ungewöhnlich oder fragwürdig.

Wenn eine Nachricht mindestens eines dieser Merkmale aufweist, sollte man skeptisch sein. Denn in solchen Fällen besteht mit hoher Wahrscheinlichkeit die Gefahr, dass es sich um Phishing handelt.

Quelle: https://www.watson.de/leben/geld%20&%20shopping/619319934-comdirect-verbraucherzentrale-warnt-bank-kunden-vor-betrug

7) Vorsicht Geldabzocke Paypal-Betrug mit "Freunde und Familie"-Funktion

Eine Person hat Geld per Paypal überwiesen und bittet darum, es zurückzubekommen. Der Grund: Es sei eine Fehlüberweisung. Wer jetzt falsch handelt, verliert im Ernstfall viele Euros. Worauf sollte man achten?

"Freunde-Bezahlfunktion" hebelt Käuferschutz aus

Paypal soll Schutz bei Online-Überweisungen bieten. Das geht aber nur, wenn man die Regeln dafür befolgt. Hier setzt eine neue Betrugsmasche an: Eine Person meldet sich mit dem Hinweis, sie hätte fälschlicherweise eine Überweisung getätigt und bittet um eine Rücküberweisung über die "Familie und Freunde"-Funktion.

Was unproblematisch klingt, ist ein mieser Trick: Die Betrüger überweisen über die Option "Waren und Dienstleistungen" und "genießen" so den Käuferschutz. Bekommen sie das Geld über die "Familie und Freunde"-Funktion geschickt, hat der Absender keinen Bezahlschutz.

"Persönliche Zahlungen sind nicht vom PayPal-Käuferschutz abgedeckt", erklärt Paypal in seinen AGB.

Opfer stehen aber ohne Käuferschutz da und sind ihr Geld los

Die Betrüger holen sich dann über den Käuferschutz durch die "Waren und Dienstleistungen"-Option das zuvor angeblich fälschlicherweise an ihr Opfer gesendetes Geld über Paypal zurück, mit dem Hinweis, sie hätten eine bestellte Lieferung nicht bekommen. Und: Sie haben noch die Überweisung von ihren Opfern obendrauf. Damit haben sie ihren "Einsatz" verdoppelt. Die Opfer sind ihr Geld los und können nur versuchen, es wiederzubekommen, indem sie bei der Polizei Anzeige erstatten. Vor der aktuellen Betrugsmasche warnt das ZDF-Magazin "Wiso".

Paypal: Was ist der Unterschied zwischen "Zahlungen an Freunde und Familie" und "Zahlungen für Waren und Dienstleistungen"?

Erhaltene Falsch-Überweisung sicher zurücküberweisen

Das falsch überwiesene Geld nicht über die "Familie und Freunde"-Funktion zurücksenden! Wählen Sie die betreffende Zahlung an und nutzen Sie den Button "Rückzahlung senden". Dann sind Sie raus und Paypal übernimmt die Rückabwicklung. Der Bundesverband der Verbraucherzentralen rät dringend von der Freunde-Bezahlfunktion beim "Bezahlen bei Einkäufen und sonstigen geschäftlichen Vorgängen" ab, auch wenn durch die Bezahlfunktion "Waren und Dienstleistungen" Transaktionsgebühren anfallen. Die "Familie und Freunde"-Funktion nur bei vertrauenswürdigen Personen verwenden, die man kennt.

Gut zu wissen Wer online bestellt und die Ware dann bezahlen möchte, sollte sich den Paypal-Link des Verkäufers gut anschauen. Fake-Shops machen Kasse, indem sie die Bezahlfunktion" Familie und Freunde" voreinstellen. Auch hier entfällt dann der Käuferschutz. Ist man auf Kriminelle hereingefallen, hat man dann im Zweifelsfall keine Ware bekommen und dennoch dafür "bezahlt" - und steht dann ohne alles da.

Paypal warnt vor Betrugsanruf: Diese Anrufe sind nicht echt

So funktioniert die Masche

Betrüger haben sich eine neue Masche ausgedacht. Sie überraschen derzeit mit gefälschten Anrufen des Bezahldienstes Paypal. Darin werden die Angerufenen darüber informiert, dass Paypal eine hohe Summe von mehreren hundert Euro abbuchen wird. Um dies zu verhindern, soll eine Taste auf dem Telefon gedrückt werden.

Die Verbraucherzentrale warnt vor diesen Anrufen. Sie würden an andere Betrugsanrufe erinnern. Wer bei diesen nach der Ansage tatsächlich eine Taste gedrückt hat, wurde mit einer Person verbunden und im Gespräch dazu gedrängt, Geld auf ein ausländisches Konto zu überweisen oder in Kryptowährungen zu investieren.

Auch PayPal selbst kennt diese Betrugsmasche. "Wir erhalten derzeit vermehrt Anrufe von Kund:innen zu diesem Thema, darunter leider auch einige, die Opfer dieser Form des Betrugs geworden sind", bestätigt das Unternehmen auf Nachfrage von BRISANT. Betrüger würden dabei mit dem Vertrauen der Menschen spielen. "Häufig werden die Angerufenen unter Zeitdruck gesetzt, um so die Herausgabe von Informationen zu erreichen."

Das sollten Sie tun

Wer einen solchen Anruf bekommt, sollte unbedingt auflegen und keine Taste drücken. Dazu rät auch der Bezahldienst selbst. Das Unternehmen ruft seine Kunden in der Regel nicht an,

"– und schon gar nicht mit der Aufforderung, Zahlungen zu leisten." Um sicher zu gehen, dass es keine ungewöhnlichen Zahlungen auf dem Paypal-Konto gibt, sollte man sich das Konto genauer ansehen. Wichtig dabei: Direkt auf die echte Webseite oder in die App gehen.

Auf seiner Webseite warnt der Bezahldienst Paypal vor den häufigsten Betrugsmaschen und listet diese auf. Zudem weist der Dienstleister darauf hin, dass er seine Kunden in der Regel per E-Mail kontaktiert. Ein erster Hinweis auf einen Betrug ist also bereits der Anruf.

Allerdings berichten laut Verbraucherzentrale bislang alle Betroffenen der neuen Betrugsmasche, dass sie noch während der Bandansage aufgelegt haben. Was passiert, wenn man tatsächlich eine Taste drückt oder einfach in der Leitung bleibt, ist also unklar. Keiner der Angerufenen konnte ungewöhnliche Zahlungen oder Abbuchungen feststellen.

Sollte Ihnen doch ein hoher Betrag abgebucht worden sein oder Sie andere Ungereimtheiten feststellen, kontaktieren Sie unbedingt den Kundenservice - ebenfalls über die App oder die echte Webseite.

Wenn Sie doch getippt haben

Wenden Sie sich unbedingt an den Kundendienst des Bezahldienstes und behalten Sie Ihr Konto im Auge. Lassen Sie sich auf keinen Fall zu einer Zahlung drängen. Unternehmen wie Paypal weisen darauf hin, dass "seriöse Unternehmen ihre Kund:innen nicht anrufen, um persönliche Informationen abzufragen oder mit der Aufforderung, Zahlungen auszulösen." Außerdem sollten Sie den Betrugsversuch oder den Betrug bei der Polizei anzeigen. Wichtig dabei: die Telefonnummer, von der Sie angerufen wurden. Eine Anzeige kann für Entschädigungszahlungen wichtig sein.

Quelle: https://www.brisant.de/haushalt/sicherheit/paypal-betrug-anruf-178.html und https://www.mdr.de/ratgeber/finanzen/betrug-paypal-masche-124.html

8) Sicherheit – Kontodeaktivierung bei Postbank: Neue Phishing-Welle bedroht Kundschaft

Und täglich grüßt das Murmeltier: Kaum ein Tag vergeht ohne eine neue Phishing-Masche. Diesmal haben es die Kriminellen in betrügerischer Absicht auf die Kundschaft der Postbank abgesehen.

Am 25. April 2024 gab es eine neue **Phishing-Welle**, die sich gezielt gegen die **Kundschaft der Postbank** richtet. Mit gefälschten E-Mails, die vorgeben, die Konten der Opfer innerhalb von 24 Stunden zu deaktivieren, versuchen Kriminelle, an persönliche Daten zu gelangen. In diesem Artikel geben wir einen Überblick über die neue Phishing-Methode, den genauen Inhalt der E-Mails und wie man sich davor schützen kann.

Inhalt der Phishing-Mails

Die derzeit im Umlauf befindlichen Phishing-E-Mails tragen Betreffzeilen wie „Servicekommunikation <beliebige achtstellige Zahl>“. In der E-Mail wird behauptet, dass das **Konto des Opfers innerhalb von 24 Stunden deaktiviert wird**. Als Grund werden „routinemäßige Sicherheitsmaßnahmen“ der „Bank“ angegeben. Um die Deaktivierung zu verhindern, wird aufgefordert, sein Online-Profil zu aktualisieren und zu bestätigen.

Zielgruppe und Methoden

Die Phishing-Kampagne richtet sich an die Kundschaft der Postbank. Mit Drohungen und einer kurzen Frist wird versucht, die Opfer unter Druck zu setzen. Die Aufforderung, das

Online-Profil zu aktualisieren und zu bestätigen, dient lediglich dazu, **an sensible Daten zu gelangen**. Wird die Aufforderung ignoriert, wird in der E-Mail behauptet, die Verifizierung sei nur in einer Filiale möglich.

Tipps zum Schutz vor Phishing

Es ist wichtig, sich von solchen E-Mails nicht einschüchtern zu lassen und nicht unüberlegt zu handeln. Phishing-Mails arbeiten oft mit Drohungen oder engen Fristen, um eine schnelle Reaktion zu erzwingen. Am besten ist es, **solche E-Mails unbeantwortet in den Spam-Ordner zu verschieben** und zu ignorieren. Auf keinen Fall sollten Links oder Anhänge in Phishing-Mails geöffnet werden.

Fazit

Die aktuelle Phishing-Welle zeigt, wie wichtig es ist, wachsam zu sein und E-Mails genau zu prüfen. Die Postbank oder andere Banken werden niemals sensible Daten per E-Mail abfragen. Ignorieren Sie verdächtige E-Mails und informieren Sie gegebenenfalls Ihre Bank. Bleiben Sie wachsam und schützen Sie Ihre persönlichen Daten, indem Sie nicht auf Phishing-Mails antworten.

5 Schritte zum Schutz vor Phishing

- **1. Kommunikation überprüfen**
  Bevor Sie handeln, prüfen Sie die Echtheit der E-Mail. Kontaktieren Sie die Postbank über die offiziellen Kontaktdaten, um die Echtheit der Kommunikation zu bestätigen.
- **2. Keine verdächtigen Links anklicken**
  Phishing-Mails enthalten oft Links, die auf betrügerische Webseiten führen, um Daten zu stehlen. Klicken Sie nicht auf Links in E-Mails, an deren Echtheit Sie zweifeln.
- **3. Bleiben Sie auf dem Laufenden**
  nformieren Sie sich über die neuesten Phishing-Techniken und -Taktiken der Betrüger. Mit aktuellen Informationen können Sie ihre Versuche besser erkennen und vereiteln.
- **4. Melden Sie verdächtige E-Mails**
  Wenn Sie eine Phishing-E-Mail erhalten, melden Sie diese Ihrem E-Mail-Anbieter und den zuständigen Behörden. Dies hilft, diese betrügerischen Praktiken zu identifizieren und zu bekämpfen.
- **5. Wachsam bleiben**
  Denken Sie daran, dass die Postbank niemals per E-Mail nach persönlichen Informationen wie Passwörtern oder Finanzdaten fragt. Wenn Sie wachsam und informiert bleiben, können Sie sich und andere davor schützen, Opfer dieser böswilligen Phishing-Versuche zu werden.

Quelle: https://www.connect.de/news/kontodeaktivierung-postbank-kundschaft-neue-phishing-welle-3205322.html?utm_source=nachrichten-NL&utm_medium=newsletter

Anwenderinformationen:

1) Tipp – Verlorenes Smartphone: So sperren Sie Ihr Handy übers Internet oder löschen gleich alle Daten

Für viele Menschen ist das ein Albtraum: Plötzlich ist das Smartphone weg! Was also tun, wenn das Gerät trotz Suche nicht wieder auftauchen sollte - sperren oder alle Daten löschen?

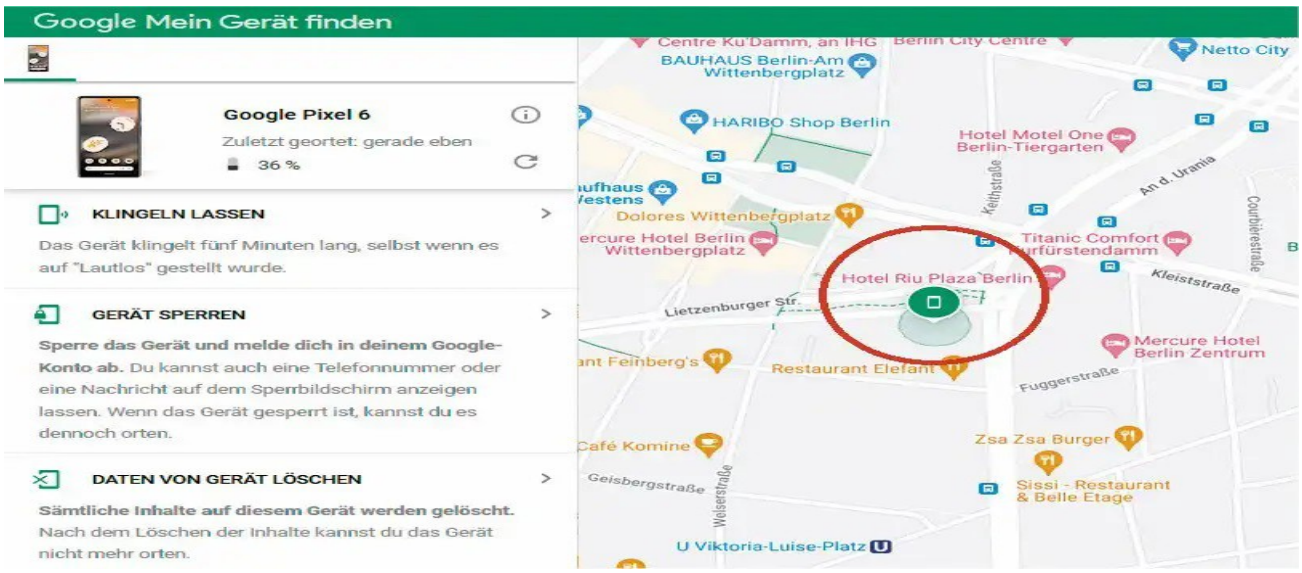
Zunächst einmal sollten Sie versuchen, sich von einem anderen Anschluss selbst anzurufen. Hat jemand Ihr Telefon gefunden oder hört es klingeln, kann der ehrliche Finder den Anruf annehmen. Je nach Einstellung des Sperrbildschirmes ist Ihr Anrufversuch inklusive der Telefonnummer auch nachträglich sichtbar, sodass man Sie gegebenenfalls zurückrufen kann.

Wenn solche Anrufversuche erfolglos sind oder Sie Ihr Telefon lieber sofort sperren möchten, so ist das sowohl bei Android-Geräten als auch bei iPhones ohne irgendwelche vorherigen Vorbereitungen sofort möglich:

Für ein Android-Smartphone loggen Sie sich von einem beliebigen Gerät mit Ihrem Google-Konto im Browser unter www.google.com/android/find ein. Ist das verlorene Telefon eingeschaltet, wird es daraufhin automatisch kontaktiert und Sie sehen den (ungefähren) Standort auf einer Karte. Kann es nicht geortet werden, wird der letzte bekannte Standort angezeigt.

Nun haben Sie drei Möglichkeiten: „Klingeln lassen“ lässt das Gerät fünf Minuten lang bei voller Lautstärke klingeln, selbst wenn es auf lautlos gestellt ist. „Gerät sperren“ sperrt Ihr Smartphone mit Ihrer PIN oder Ihrem Passwort. Falls Sie noch keine Sperre eingerichtet haben, können Sie das an dieser Stelle sogar nachholen!

Zudem können und sollten Sie hier für einen potenziellen Finder eine Nachricht wie „Finderlohn, danke!!!“ oder etwas Ähnliches und eine Rückrufnummer hinterlassen. Diese Nachricht auf dem Sperrbildschirm sieht der potenzielle Finder, über einen speziellen Anruf-Button kann er Sie auf der von Ihnen hinterlegten Telefonnummer anrufen.



Die Google-Funktion „Find my device“ ortet ein verlorengegangenes Android-Telefon und bietet die Möglichkeit, es anzurufen, zu sperren oder sogar komplett zu löschen.

Die dritte Option macht genau das, was die Bezeichnung „Daten von Gerät löschen“ verspricht. Anschließend haben jedoch Sie selbst keinerlei Möglichkeit mehr, das Smartphone aus der Ferne zu kontaktieren. Beim iPhone funktioniert das Prozedere grundsätzlich ähnlich, Apple erläutert das Vorgehen im Onlinehandbuch. Weil das Mobiltelefon mittlerweile sehr viele persönliche Informationen speichert und dabei meistens auch Zugriff auf Mailkonten und so weiter erlaubt, ist es dringend geraten, das Gerät mit einer PIN und für mehr Komfort zusätzlich mittels Fingerabdruck zu sichern.

Lese-Tipp: Android-Handy wieder schnell machen: Cache löschen – das bringt es und so geht’s

Quelle: https://www.pcwelt.de/article/2283806/verlorenes-smartphone-sperren-daten-loeschen.html?utm_source=flipboard&utm_content=PCWELT%2Fmagazine%2FPC-WELT

2) Apps – Sofort löschen: Gleich 5 Apps spionieren dich heimlich aus

Gleich mehrere Apps solltest du löschen. Sie sind mit schadhafter Software versetzt oder stehen mit fragwürdigen Akteuren im Zusammenhang.

Nicht nur im Google Play Store, auch in Apples App Store finden sich hin und wieder gefährliche Applikationen, die Nutzerinnen und Nutzer ernsthafte Probleme bereiten können. Dazu zählen beispielsweise die folgenden **Apps, die du löschen solltest**. Sie können auf verschiedenste Art bedrohlich werden.

App löschen: Achte auf diese 5 Exemplare

Findet sich auf dem eigenen Handy eine fragwürdige App, ist das Löschen immer eine empfehlenswerte Reaktion. Wer ein iPhone oder iPad besitzt, darf sich dabei in der Regel etwas sicherer fühlen, denn Apple prüft die Anwendungen in seinem App Store sehr gründlich und sorgt dafür, dass potenziell riskante Exemplare nicht hinein gelangen.

Android-Benutzer*innen auf der anderen Seite sind stärker durch Malware und Kriminelle gefährdet. Diese können die Sicherheitsvorkehrungen leichter umgehen und Software über Drittanbieterquellen zum Herunterladen in den Play Store schmuggeln. Entsprechend solltest du besonders aufpassen, wenn du ein Smartphone mit dem Google-Betriebssystem verwendest.

Wichtig ist es in jedem Fall, schon vor dem Download Rezensionen und Bewertungen für jede Anwendung, die dein Interesse gewonnen hat, zu lesen. Nur eine bösartige App kann ausreichen, dass du gehackt wirst und deine Daten gestohlen werden. Fachleute empfehlen beispielsweise, sich von diesen fünf Apps zu trennen.

Hinweis: Die genannten Anwendungen wurden aus den App-Stores zwar schon entfernt. Wer die dahinter steckenden Risiken allerdings nicht kennt, hat sie womöglich weiter in Nutzung.

#1 SuperVPN

Nicht zum ersten Mal ist die Anwendung in den Fokus von Expert*innen gerückt. Schon 2020 riet man dazu, die SuperVPN-App zu löschen. Und erst jüngst, 2023, kamen Analysten zu dem Urteil, dass es sich dabei um „eines der gefährlichsten und unzuverlässigsten kostenlosen VPNs [handelt], die wir getestet haben“.

Die Gründe dafür sind vielfältig: So besitzt die Anwendung „invasive Protokollierungsprozesse, schwache Sicherheitsfunktionen, besorgniserregende

Verbindungen nach China und kann keine Webinhalte entsperren“. Man warnte davor, dieses VPN zu verwenden beziehungsweise empfahl, es „sofort zu deinstallieren“.

#2 Noizz

Hinter dieser Anwendung steckt ein beliebter Editor für Videoschnitt und Musik. Im Google Play Store wurde er bereits 2023 rund 100 Millionen Mal heruntergeladen. Später stellte man fest, so Bleeping Computer, dass die Anwendung bösartige Software enthält, die dein Gerät gefährden kann.

Im Detail ist das eine relativ neue Android-Malware, die als „SpinOk“ bezeichnet wird, private, auf den Geräten der Nutzer*innen gespeicherte Daten stehlen und an einen Remote-Server senden kann. Dabei simuliert sie Minispiele, um das Interesse der Nutzer zu wecken.

Während diese in der App angezeigt werden, führt die Malware im Hintergrund bösartige Funktionen aus, darunter das Auflisten von Daten in Verzeichnissen, die Suche nach bestimmten Informationen, das Hochladen von Dateien vom Gerät oder das Kopieren und Ersetzen von Inhalten der Zwischenablage.

#3 Fake-ChatGPT-Apps

Dank der überwältigenden Popularität des KI-Bots ChatGPT war es unvermeidlich, dass gefälschte Varianten davon auftauchen und einige davon schädlichen Code enthalten. Eine Fake-ChatGPT-App brachte vor kurzem erst Schadsoftware auf den PC vieler Nutzerinnen und Nutzer.

Entsprechend wichtig ist es auch, falschen Open AI/ChatGPT-Apps, die sowohl bei Google Play als auch im App Store auftauchen, nicht auf den Leim zu gehen. Oft sehen sie genauso aus wie das Original. Sie können aber sogenannte Fleeceware enthalten, die versucht, dir Geld zu stehlen.

Lesetipp: So kannst du Android- und iOS-Apps löschen

#4 Essential Horoscope

Viele Horoskop-Apps sind für ihre Anwender*innen ein einfacher Spaß. Im Fall von Essential Horoscope für Android kamen unter dieser Annahme mehr als 100.000 Downloads auf Google Play zustande. Dann erst fanden Fachleute von McAfee heraus, dass sie eine Malware namens Xamalicious enthält.

Diese macht sich das Open-Source-Framework Xamarin zunutze, um sich auf befallenen Geräten zu verbergen. Dann kann sie die volle Kontrolle übernehmen, um betrügerische Aktionen ohne Zustimmung der Betroffenen durchzuführen. Dazu zählt beispielsweise die heimliche Installation anderer Apps.

#5 UC Webbrowser

Dieser Browser ist nur für Android verfügbar und gehört über seine Entwicklerfirma UCWeb zum chinesischen Unternehmen Alibaba. Die App schützt allerdings und nach Ansicht von Cybersecurity-Expert*innen Datenübertragungen nicht hinreichend, wie Shefinds erklärt. Dies kann dazu führen, dass persönlichen Informationen anfällig für Kriminelle und Angriffe werden.

Quelle:https://www.futurezone.de/digital-life/apps/article540758/5-apps-loeschen-china-spioniage.html

3) Smart-TVs angreifbar – Schwere Sicherheitslücken in LG-Fernsehern: Diese Geräte sind betroffen

Sicherheitsexperten haben im WebOS für LG-Fernseher vier Schwachstellen entdeckt. Damit Hacker nicht in die Software des TVs eindringen können, gibt es Abhilfe.

In LG-Fernsehern mit dem Betriebssystem WebOS sind vier Sicherheitslücken entdeckt worden. Das teilen die Cybersecurity-Experten des Unternehmens "Bitdefender" mit. Über die Schwachstellen könnten Kriminelle Zugriff auf das Gerät erlangen, heißt es.

Unter anderem sei es den Hackern möglich, über eine Schwachstelle einen zusätzlichen Benutzer zum TV-Gerät hinzuzufügen.

Über eine andere Sicherheitslücke könnten die Angreifer dann den neuen Benutzer mit Root-Rechten (Administratorrechten) ausstatten, um anschließend die vollständige Kontrolle über WebOS und damit über den Fernseher zu bekommen.

Damit können die Angreifer die Zugangsdaten von auf dem Fernseher gespeicherten Streamingdiensten wie Netflix oder Disney+ erbeuten.

Das sind die von den "Bitdefender"-Sicherheitsexperten als anfällig identifizierten Betriebssysteme und Fernseher:

- webOS 4.9.7 - 5.30.40 läuft auf LG43UM7000PLA
- webOS 5.5.0 – 04.50.51 läuft auf OLED55CXPUA
- webOS 6.3.3-442 (kisscurl-kinglake) – 03.36.50 läuft auf OLED48C1PUB
- webOS 7.3.1-43 (mullet-mebin) – 03.33.85 läuft auf OLED55A23LA

"Bitdefender" hat die Schwachstellen laut eigenen Angaben bereits im November 2023 an LG übermittelt. Am 22. März 2024 sei ein Patch des TV-Herstellers veröffentlicht worden. Besitzer der oben genannten Geräte sollten prüfen, ob WebOS auf dem aktuellen Stand ist.

So geht's:

1. Schalten Sie Ihren LG-Fernseher ein und drücken Sie die Taste "Einstellungen" auf Ihrer Fernbedienung. Auf der Taste ist ein Zahnradsymbol dargestellt.
2. Wählen Sie "Software-Update" unter dem Menüpunkt "Kundensupport" oder "Allgemein".
3. Wählen Sie "Nach Updates suchen" unter dem Punkt "Software-Update"
4. Folgen Sie den Anweisungen auf dem Fernseher, um WebOS zu aktualisieren.
5. Fertig.

Quelle: https://www.t-online.de/digital/aktuelles/id_100383070/smart-tvs-schwere-sicherheitsluecken-bei-diesen-lg-fernsehern.html

4) Aus aktuellem Anlass: Vorsicht vor Drückerkolonnen – Verbraucherzentrale warnt vor Haustürgeschäften

Es klingelt an der Haustür, aber einen Termin gibt es nicht? Dann sollten Verbraucherinnen und Verbraucher vorsichtig sein. Denn oftmals handelt es sich auf der anderen Seite der Tür um Verkäufer im Außendienst, die Geschäfte machen wollen. Teilweise bedienen sich diese Vertriebsprofis dabei unmoralischer oder sogar krimineller Methoden. Mit der gesetzlichen Abschaffung des Nebenkostenprivilegs sind aktuell verstärkt solche Drückerkolonnen in Schleswig-Holstein unterwegs.

Hintergrund: Wegfall des Nebenkostenprivilegs:

Das Nebenkostenprivileg ist in § 2 Nr. 15 der Betriebskostenverordnung geregelt und besagt, dass der Kabelanschluss vom Hauseigentümer oder der Hausverwaltung in der Nebenkostenabrechnung auf die Hausbewohner umgelegt werden kann. Damit ist bald Schluss: Denn nach einer Übergangsfrist müssen Verbraucher, die zur Miete wohnen, ihren Kabel-Fernsehanschluss spätestens ab dem 1. Juli 2024 selbst wählen.

Was Verbraucher jetzt wissen sollten:

Wer in einem Mehrfamilienhaus wohnt, sollte seinen Kabelanschluss also jetzt prüfen und sich möglicherweise um eine Alternative kümmern. Anderenfalls könnte der bestehende Anschluss gesperrt oder die TV-Buchse in der Wohnung verschlossen werden. Da die Kabelkosten ab Juli nicht mehr zu den Nebenkosten zählen, müssen auch Bürgergeld-Empfänger die Gebühren für einen neuen Anschluss selbst zahlen. Die Mehrkosten belaufen sich auf zwei bis drei Euro pro Einzelnutzungsvertrag.

Was bei neuen Verträgen zu beachten ist:

Egal, ob das Fernsehen über einen Kabelanschluss bezogen oder anders empfangen wird – wie bei jedem neuen Vertragsabschluss gilt:

- Verbraucher sollten nichts vorschnell oder unüberlegt unterschreiben, sondern das Angebot ausreichend prüfen. Außerdem empfiehlt es sich, Preise zu vergleichen.
- Außerdem sollten Betroffene unabhängige Fachleute fragen, ob in ihrer Wohnung mit ihrem Fernsehgerät die vorgeschlagene Empfangstechnik eingesetzt werden kann.
- Wer einen Vertrag im Geschäft abschließt, habt kein Widerrufsrecht. Hier muss das Angebot also sehr gewissenhaft geprüft werden.

Was bei Haustürgeschäften zu beachten ist:

Verträge, die an der Haus- oder Wohnungstür abgeschlossen werden, sind meist überteuert. Vertreter nutzen dafür häufig Überraschungsmomente aus. Deshalb sollten Verbraucher besondere Vorsicht walten lassen. Die Verbraucherzentrale Schleswig-Holstein empfiehlt diese Tipps:

- Öffnen Sie am besten gar nicht erst die Tür, wenn ein Vertreter unangekündigt an der Tür klingelt.
- Lassen Sie niemals einen Vertreter in die Wohnung, auch nicht, wenn er „nur den Kabelanschluss prüfen“ möchte.
- Bei unerwünschten Werbeanrufen: Sagen Sie nicht „Ja“, geben Sie keine Daten heraus und legen Sie notfalls einfach auf.
- Lassen Sie sich nicht einschüchtern, überrumpeln und einen Vertrag aufschwatzen – Sie müssen gar nichts.
- Unterschreiben Sie nichts, was Sie nicht verstehen. Stimmen Sie nichts zu, das Sie nicht verstehen.
- Haben Sie doch zugestimmt oder bereits unterschrieben, können Sie den Vertrag innerhalb von 14 Tagen widerrufen. Erhalten Sie keine Widerrufsbelehrung, erlischt Ihr Recht auf Widerruf erst zwölf Monate und 14 Tage nach Vertragsschluss.

Alternativen zum Kabelanschluss:

Das Fernsehen ist heute digital und es gibt viele Empfangsmöglichkeiten. Dazu zählen zum Beispiel DVB-T2 HD über Antenne, Satellitenfernsehen über eine Satellitenschüssel oder verschiedene Streaming-Dienste über das Internet.

Quelle: https://www.verbraucherzentrale.sh/pressemeldungen/vertraege-reklamation/aus-aktuellem-anlass-vorsicht-vor-drueckerkolonnen-94374

5) Spam-Liste für April – Diese Telefonnummern sollten Sie sofort blockieren

Betrügerische Anrufe von unbekannten Telefonnummern können mit der Zeit die Nerven strapazieren. Um sich zu schonen, sollten Sie diese Nummern blockieren.

Mit lästigen Spam-Anrufen von unbekannten Nummern versuchen Betrüger oft, an persönliche Daten oder Geld zu kommen. Erfreulich im vergangenen Monat: Die Zahl der Spam-Anrufe ist im März zurückgegangen (-12,9 Prozent), wie die Firma Clever Dialer mitteilt.

Clever Dialer hilft mit seiner App ("cleverdialer.app"), unerwünschte und betrügerische Anrufe zu erkennen und abzuwehren. Jeden Monat verrät das Unternehmen t-online die fünf Spam-Nummern, die den Kunden den meisten Ärger bereiten.

Trotz des Rückgangs der Anrufe wurden auch im vergangenen Monat wieder viele Menschen von dreisten Betrügern am Telefon belästigt. So stieg die Zahl der gemeldeten Sperrungen im März um 13,1 Prozent. "Viele Betroffene gehen schon gar nicht mehr ans Telefon, um brenzlige Situationen von vornherein zu vermeiden", so Clever Dialer.

Die Top 5 der Spam-Nummern März 2024

Um die betrügerischen Anrufe abzuwehren, sind hier die fünf Telefonnummern, die im vergangenen Monat am häufigsten bei Clever Dialer gemeldet wurden. Diese sollten Sie sofort blockieren.

(Quelle: Clever Dialer)

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

- 06987003110 (Kostenfalle)
- 056818090264 (Kostenfalle)
- 022376922894 (Kostenfalle)
- 056818090265 (Kostenfalle)
- +447762833647 (Kostenfalle)

So blockieren Sie eine Telefonnummer

Wie Sie auf Ihrem Handy eine Nummer sperren können, erfahren Sie in dieser Anleitung. Die oben genannten Telefonnummern sollten Sie sofort blockieren. Grundsätzlich sollten Sie niemals persönliche Daten wie Adressen, Kontonummern oder Passwörter am Telefon an unbekannte Nummern weitergeben. Werden Sie danach gefragt, beenden Sie einfach den Anruf. Lesen Sie hier auch: Welches Wort Sie am Telefon niemals zu Fremden sagen sollten.

Quelle: https://www.t-online.de/digital/aktuelles/id_100377990/spam-liste-fuer-april-diese-fuenf-nummern-sollten-sie-blockieren.html

6) Gefahrenpotenzial "hoch" – Google schließt Sicherheitslücken in Chrome – so aktualisieren Sie den Browser

Drei Schwachstellen hat Google in seinem Internet-Browser Chrome geschlossen – alle mit hohem Risiko. Nutzer sollten dringend reagieren.

Google hat für seinen Browser Chrome eine Aktualisierungsdatei veröffentlicht. Damit schließt das Unternehmen drei Sicherheitslücken, wie Google in einem Blogeintrag mitteilt.

Alle drei Schwachstellen stuft Google als "hoch" ein. Es handelt sich um Sicherheitslücken mit den Bezeichnungen "CVE-2024-3156", "CVE-2024-3158" und "CVE-2024-3159". Laut Google wurden die Lücken von externen Sicherheitsforschern entdeckt und gemeldet.

Das Update aktualisiert Chrome auf die Versionen 123.0.6312.105/.106/.107 für Windows und Mac. Der Browser für Linux wird auf die Version 123.0.6312.105 aktualisiert.

Chrome aktualisieren – so geht's

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

Wer die aktuellen Versionen des Internet-Browsers noch nicht nutzt, sollte dringend die neue Version installieren.

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

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

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

Quelle: https://www.t-online.de/digital/aktuelles/id_100377308/google-schliesst-sicherheitsluecken-in-chrome-so-aktualisieren-sie-den-browser.html

7) Android-Malware – Banking-Trojaner tarnt sich als McAfee Security App

Der Banking-Trojaner Vultur ist weiterhin aktiv und wird auf neuen Wegen verbreitet - aktuell in einer gefälschten Sicherheits-App.

Der Banking-Trojaner Vultur war zuerst im März 2021 aufgetaucht. Seitdem ist die Malware auf Android-Smartphones aktiv und wird auch immer weiter entwickelt, um gängige Sicherheitsmechanismen zu umgehen. Aktuell setzen Angreifer auf eine neue Taktik, um den Trojaner zu verbreiten, und verstecken ihn in einer Sicherheits-App.

Bei der aktuellen Version von Vultur setzen die Angreifer auf eine Kombination aus SMS und Telefonanrufen, wie ein Bericht von Fox IT nahe legt. Das Opfer soll dann dazu gebracht werden, eine präparierte App zu installieren, die als Dropper für den Trojaner dient.

Angebliche Sicherheits-App über SMS-Link

Der Angriff beginnt mit einer Phishing-SMS (Smishing), die vor einer nicht autorisierten Transaktion warnt, bei der es um eine große Geldmenge gehen soll. Dabei wird auf eine Telefonnummer verwiesen, die man anrufen soll. Am Telefon melden sich dann die Betrüger und suggerieren, dass das Smartphone von Malware infiziert sei.

Natürlich ist die angebliche Überweisung nicht echt und auch das Smartphone ist zu diesem Zeitpunkt (noch) nicht infiziert. Im Verlauf des Telefongesprächs soll man aber dazu gedrängt werden, eine App zu installieren, um die angebliche Malware vom Smartphone zu entfernen. In einer zweiten SMS erhält man hierfür einen Link. Dieser führt augenscheinlich zum Download der McAfee Security App, bei der es sich aber um eine präparierte App handelt.

Auf den ersten Blick wirkt die App authentisch. Sie soll oberflächlich auch Funktionen ausführen, die man von der echten McAfee Security App erwarten würde. Tatsächlich enthält die gefälschte Version der App aber den Dropper "Brunhilda", der anschließend in mehreren Stufen den Trojaner Vultur herunterlädt.

Vultur kontrolliert das Smartphone

Der Trojaner sichert sich Zugriff auf die Bedienhilfen, aktiviert Fernsteuerungssysteme und baut eine Verbindung zum Command-and-Control-Server (C2) auf. Über Bildschirmaufzeichnungen und Keylogger können Daten und Passwörter ausgelesen werden. In der neuen Version ist Vultur außerdem in der Lage, Dateien zu suchen und herunterzuladen, die Ausführung bestimmter Apps zu blockieren oder Statusanzeigen einzublenden. Somit gibt die Malware den Angreifern weitgehende Kontrolle über das Smartphone und kann gleichzeitig ihre Tätigkeiten verschleiern.

Um sich vor Malware zu schützen, wird grundsätzlich dazu geraten, Apps nur aus vertrauenswürdigen Quellen wie etwa dem Google Play Store zu beziehen. Vermeiden Sie es, auf Links in Nachrichten zu klicken. Außerdem sollten Sie, wenn Sie Hinweise auf verdächtige Bankaktivitäten erhalten, die Telefonnummer Ihrer Bank lieber in Ihren eigenen Unterlagen verifizieren und nicht die in der Nachricht angegebene Nummer wählen.

Quelle: https://www.connect.de/news/android-malware-banking-trojaner-vultur-mcafee-security-app-3205088.html?utm_source=connect-NL&utm_medium=newsletter

8) E-Mails adressieren – BCC und CC in E-Mails: So nutzen Sie die Funktion richtig

Wer E-Mails an mehrere Empfänger gleichzeitig schreiben möchte, setzt sie in "CC" oder "BCC". Das gibt es bei der Anwendung zu beachten.

Kommunikation per E-Mail ist sowohl im privaten als auch geschäftlichen Umfeld weit verbreitet. Funktionen wie Dateianhänge, Verlinkungen oder Termineinladungen bieten E-Mails unbegrenztes Potenzial. Mithilfe der CC- und BCC-Funktionen können Sie darüber hinaus eine Vielzahl von Empfängern gleichzeitig erreichen.

Doch diese Freiheiten bringen auch Risiken mit sich. Ein falscher Klick kann schwerwiegende Konsequenzen haben – von zerstörten Beziehungen bis hin zu Betriebsgeheimnissen, die versehentlich preisgegeben werden. Daher ist es wichtig, die Unterschiede zu kennen und die Felder richtig einzusetzen.

CC in E-Mails: Empfänger sind für alle sichtbar

Die Abkürzung "CC" steht für "carbon copy" (auf Deutsch: "Durchschlag") und bedeutet, dass jeder Empfänger die Mailadressen aller weiteren Empfänger sehen und bei Bedarf für eigene Zwecke verwenden kann. Die CC-Funktion nutzen Sie am besten, wenn Sie Rundmails mit gleichem Inhalt an eine Gruppe senden möchten, deren Mitglieder sich untereinander kennen und bei denen die Weitergabe und die Sichtbarkeit der E-Mail-Adressen kein Problem darstellt.

Wenn Sie möchten, dass die Empfänger wissen, an wen die E-Mail versendet wurde, sollten Sie sie in "CC" setzen – zum Beispiel bei Rundmails an Freunde oder der Familie. Genutzt wird die CC-Funktion auch häufig, um dem in das CC-Feld gesetzten Empfänger zu zeigen, dass er die Mail nur zur Kenntnisnahme erhält.

Gehen Sie allgemein vorsichtig mit dieser Funktion um. Es gilt als unhöflich, anderen unerlaubt die Mailadressen weiterzuvermitteln, gerade wenn Sie sich nicht sicher sind, ob auch alle Empfänger mit der Weitergabe einverstanden sind. Manchen Kollegen reagieren zum Beispiel auch pikiert, wenn die Adresse des Chefs in CC angegeben ist.

BCC in E-Mails: Empfänger sind verborgen

"BCC" steht für "blind carbon copy" (auf Deutsch: "blinder Durchschlag") und ist von der Funktionsweise identisch mit CC – auch hier geht die gleiche E-Mail an alle Empfänger. Die Adressen, die in der BCC-Zeile stehen, werden den anderen Empfängern jedoch nicht angezeigt. Die Personen, deren Adresse in der Adresszeile und in CC stehen, können nicht erkennen, ob die Mail auch an andere Empfänger gegangen ist, die in BCC stehen.

Diese Funktion ist immer dann sinnvoll, wenn die Empfängerliste sehr umfangreich ist. Die Funktion sollte vor allem genutzt werden, wenn die Empfänger einer Weitergabe der eigenen E-Mail-Adresse nicht zugestimmt haben oder niemand wissen soll, an wen die Mail noch gegangen ist.

So schützen Sie die Privatsphäre der einzelnen Empfänger. Auch um zu verhindern, dass die Mail-Adressen der Empfänger von Rundmails für Spam-Mails missbraucht werden, ist die Verwendung der BCC-Funktion zu empfehlen. Andernfalls könnten die E-Mails missbraucht werden oder ungefragt im Verteiler irgendwelcher Newsletter landen.

Wie Sie die Funktionen nutzen

Die Funktionen CC und BCC sind in jedem Mailprogramm vorhanden. Teilweise müssen Sie diese jedoch erst aktivieren, bevor Sie eine Nachricht als sichtbare- oder als Blindkopie versenden können. In Outlook sind die Funktionen zum Beispiel hinter dem Reiter "Optionen" zu finden. Alternativ können Sie das Feld CC anklicken und finden dort die Möglichkeit, Empfänger auch in BCC zu setzen.

Kleiner Tipp: Es kommt vor, dass Sie nicht alle Adressen einfach ins BCC-Feld schreiben können. Für den Fall, dass der Maildienst mindestens eine E-Mail-Adresse im Adressfeld verlangt, schreiben Sie dort einfach Ihre eigene hinein – meist ist das jedoch nicht notwendig. Je nach Mailprogramm können Sie die verschiedenen E-Mail-Adressen durch ein Komma oder ein Semikolon trennen und ein Leerzeichen in das jeweilige Feld eingeben.

Tipp: Freemail: Kostenlose E-Mail-Adresse bei t-online.de – so geht's

- Inhalte immer professioneller: Anzahl von gefälschten E-Mails nimmt zu
- E-Mail-Ratgeber: Mit diesen Tricks bleibt das Postfach frei von Spam-Mails

Quelle: https://www.t-online.de/digital/internet/id_65642652/e-mail-adresse-cc-und-bcc-so-nutzen-sie-die-funktion-richtig-internet.html

9) Perfide Betrugsmasche – So viele Menschen sind von Identitätsdiebstahl betroffen

Mit ausgeklügelten Tricks locken Cyberbetrüger ahnungslose Opfer in die Falle – und stehlen mitunter sogar ihre Identität. Wer besonders gefährdet ist.

Mehr als jeder zehnte Erwachsene in Deutschland (elf Prozent) ist bereits Opfer von Identitätsdiebstahl im Netz geworden. Das geht aus einer repräsentativen Umfrage des Meinungsforschungsinstituts YouGov im Auftrag der Initiative Sicher Handeln (ISH) hervor, die am Mittwoch in Berlin veröffentlicht wurde.

Fast jeder fünfte Befragte (19 Prozent), der selbst bisher verschont geblieben ist, kennt aber einen oder gar mehrere Menschen, die zu Opfern wurden. Fünf Prozent haben beides erlebt, sind also selbst Opfer geworden und kennen weitere Betroffene.

In der Online-Umfrage von YouGov wurden Anfang März 2.058 Personen befragt. Die Ergebnisse wurden gewichtet und sind repräsentativ für die deutsche Bevölkerung ab 18 Jahren.

Darum ist Identitätsdiebstahl so gefährlich

Identitätsdiebstahl sei eine besonders perfide Betrugsmasche, erklärte die Initiative. Kriminelle nutzten dabei Daten wie den Namen, das Geburtsdatum, die Anschrift oder Kreditkarten- oder Kontonummern ihrer Opfer, um sich mithilfe dieser Daten Nutzerkonten bei Onlinediensten anzulegen und auf fremde Kosten einzukaufen oder Verträge abzuschließen. "Die Opfer bekommen das meistens erst mit, wenn es zu spät ist und die Überweisungen auf dem Konto verbucht sind oder Rechnungen eintrudeln."

Aktuell nutzen viele Cyberkriminelle den angespannten Wohnungsmarkt aus. So werden etwa Wohnungssuchende mit einer gefälschten Anzeige dazu verleitet, ein Post-Ident-Verfahren für eine Bewerbung um eine angebliche Wohnungsbesichtigung zu absolvieren. Oft merken die Betroffenen dabei nicht, dass sie mit den Angaben den Betrügern lediglich dabei helfen, in ihrem Namen ein Bankkonto zu eröffnen, das für kriminelle Zwecke verwendet werden soll, etwa für Geldwäsche.

Junge Menschen gehen sorglos mit dem Thema um

"Obwohl die Gefahr steigt, nehmen viele das Thema offensichtlich noch immer auf die leichte Schulter", sagte eine Sprecherin der Initiative. Vor allem die junge Generation agiere besonders sorglos. In der Umfrage sagte jeder dritte 18- bis 24-Jährige, für mehrere Nutzerkonten im Netz dasselbe Passwort zu verwenden.

Im Schnitt handelt gerade einmal jeder Fünfte so. 16 Prozent der jungen Erwachsenen räumten ein, bereits eine Kopie ihres Personalausweises über das Internet mit einer fremden Person geteilt zu haben. Innerhalb der gesamten Stichprobe trifft das nur auf elf Prozent der Befragten zu.

Ältere Menschen sind oft vorsichtiger

Auch bei den Sicherheitsmaßnahmen handeln die älteren Befragten deutlich gewissenhafter als die jüngste Generation. 70 Prozent der über 55-Jährigen sagen, dass sie regelmäßig ihre Kontoauszüge prüfen. Bei den 18- bis 24-Jährigen sind das lediglich 39 Prozent.

Sicher Handeln ist eine gemeinsame Initiative der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK), der Stiftung Deutsches Forum für Kriminalprävention (DFK), Deutschland sicher im Netz e. V. (DsiN), Risk Ident und Kleinanzeigen (ehemals eBay Kleinanzeigen), die 2023 ins Leben gerufen wurde.

Quelle: https://www.t-online.de/digital/aktuelles/id_100373256/betrugsmasche-identitaetsdiebstahl-mehr-als-jeder-zehnte-deutsche-opfer.html

10) Amazon: Ab morgen deutlich kürzere Rückgabefrist für diese Geräte – darauf müssen Sie achten

Amazon verkürzt ab dem 25.4.2024 für eine Reihe von Produkten die Rückgabefrist von bisher 30 Tagen auf dann nur noch 14 Tage. Das müssen Sie wissen und das sind die Ausnahmen.

Amazon-Kunden müssen ab dem 25. April 2024 bestimmte Geräte schneller als bisher zurückschicken, wenn sie diese nicht behalten wollen. Denn Amazon reduziert die Rückgabefrist für ausgewählte Gerätegruppen von bisher 30 Tagen auf dann nur noch 14 Tage. Das berichtet Spiegel Online. Ein Amazon-Sprecher bestätigte die Reduzierung der Rückgabefrist auf unsere Nachfrage. Amazon schrieb uns:

Wir werden das Rückgabefenster für ausgewählte Produkte im Elektronik-Bereich anpassen. Das Rückgaberecht und Rückgabedatum werden weiterhin deutlich gekennzeichnet unter dem Produktpreis zu finden sein. Wir bieten auch weiterhin kostenlose und bequeme Rückgaben für die meisten innerhalb Deutschlands gelieferten Artikel an.

Amazon teilte die verkürzten Rückgabefristen den Marketplace-Verkäufern bereits am Mittwoch letzte Woche mit (6.3.2024), hier finden Sie den Eintrag in Seller Central. Die neuen verkürzten Rückgabefristen gelten aber nicht für alle Produktkategorien, sondern nur für elektronische Geräte wie zum Beispiel Fernseher, Kameras, Router und PCs. Aber auch Blu-Ray-Filme und Videospiele sowie Musik-CDs müssen Sie ab dem 25. April 2024 bei Nichtgefallen schneller zurückschicken. Ebenso gilt die neue verkürzte Rückgabefrist von 14 Tagen auch für Büroartikel. 14 Tage entsprechen übrigens der gesetzlich vorgeschriebenen Rückgabefrist.

Händler, die über Amazon verkaufen, können aber freiwillig auch längere Rückgabefristen einräumen.

Die neue Rückgabefrist gilt übrigens grundsätzlich schon seit dem **25. März 2024**. Amazon schreibt aber:

Für Artikel, die ab dem 25. März 2024 gekauft werden, verkürzt Amazon in den folgenden Kategorien die Rückgabefrist für Kunden von 30 auf 14 Tage, beginnend mit dem Tag der Lieferung des Produkts. Um eine reibungslose Umstellung für Kunden sicherzustellen, können sie zwischen dem 25. März 2024 und dem 25. April 2024 weiterhin über das Online-Rücksendezentrum eine Rücksendung mit einer Rückgabefrist von 30 Tagen beantragen. Wie bisher müssen diese Rücksendeanträge im Rahmen der Richtlinien für Warenrücksendungen und Erstattungen von Amazon genehmigt und erstattet werden. Ab dem 25. April 2024 können Kunden 14 Tage nach dem Tag der Lieferung keine Rücksendung mehr beantragen.

Seine eigenen Produkte wie Amazon-Fernseher, –Streamingboxen und Tablets der Fire-Serie nimmt Amazon von der Verkürzung der Rückgabefrist aber aus, für diese gelten weiterhin die 30 Tage. Ebenso gilt die Rückgabefrist von 30 Tagen auch weiterhin für runderneuerte Elektronik aus dem "Renewed"-Angebot.

Achten Sie genau auf die Rücksendeangaben unter dem Preis

Auf Nachfrage des Spiegel bestätigte Amazon die verkürzten Rückgabefristen. Kunden sollten also künftig besonders genau auf die bei jedem Produkt genannten Rückgaberechte und Rückgabedaten achten. Diese befinden sich auch nach dem 25. April 2024 unter dem Produktpreis. Amazons Rücksendebedingungen finden Sie hier.

Marktbeobachter vermuten, dass Amazon mit der Senkung der Rückgabefrist die Retourenquote verringern will. Je weniger Zeit man zur Verfügung hat für die Rücksendung, desto geringer dürfte die Zahl der Rücksendungen sein. Amazon dürfte damit also seine Kosten für Rücksendungen reduzieren.

Tipp: Neue Amazon-Seite informiert über alle Gefahren, Rückrufe und Warnungen

Quelle: https://www.pcwelt.de/article/2261610/amazon-verkuerzt-ruckgabefrist.html

11) iPhone entsperren: Dieser Trick begeistert Nutzer – „einfach nur darauf drücken"

Auf Reddit teilte jemand einen Tipp wie sich das Apple-Gerät schneller freischalten lässt, wenn FaceID das Gesicht nicht erkennt. Viele kennen ihn noch nicht.

Es ist inzwischen für jede*n essentiell, das eigene Smartphone gut gegen den Zugriff von Fremden zu schützen. Dazu gehört beim **iPhone** unter anderem die Funktion FaceID, die das Gerät durch Gesichtserkennung entsperrt. Funktioniert diese allerdings nicht, gibt es einen kleinen Trick.

iPhone: So kannst du es schneller entsperren

Auf Reddit postete der oder die Nutzer*in rickpickel vor wenigen Tagen ein Problem, das vielen wahrscheinlich äußerst bekannt sein dürfte: „Ich fahre oft mit Sonnenbrille… wenn ich nach oben wische, versucht Face ID, mich zu erkennen… und es hält für etwa 5 volle

Sekunden, bevor es aufgibt und mir erlaubt, meinen Pin einzugeben. Ist es nicht in der Lage, sofort zu erkennen, dass es sich um eine Person mit Sonnenbrille handelt, und einfach die millionenfache Neueintragung zu überspringen?“

Auf die anschließende Frage „Oder gibt es eine andere Abkürzung, um die Gesichtserkennung zu überspringen und direkt zur PIN zu gelangen (vorzugsweise eine einhändige Methode)?“ antwortete jemand mit dem Account itsradii mit besagtem Trick: „Du kannst nach oben wischen und auf den Text ‚Face ID‘ in der Mitte des Bildschirms tippen, um direkt zur PIN zu gelangen. Ich weiß nicht, warum das so unintuitiv ist, aber es ist da.“

iPhone-Nutzer*innen sagen „danke“

Wie wenig bekannt die versteckte Funktion ist, zeigen die Reaktionen auf den Kommentar. Gleich mehrfach bedankte man sich für den anscheinden sehr nützlichen Tipp: „Vielen Dank, die ganze Zeit habe ich das Telefon von mir weggedreht und 5 Sekunden gewartet, bis es zur PIN wechselt“, erklärte eine Person.

Eine andere zeigte sich noch überraschter: „Was?!! Du sagst mir, dass ich all die Jahre darauf gewartet habe, dass Facetime eine Zeitüberschreitung hat und ich einfach darauf drücken konnte! Ich danke dir vielmals.“ Aber auch „Danke! Ich habe ehrlich gesagt nicht einmal daran gedacht, das zu versuchen…“, war eine der Reaktionen.

Tipp: Diese iPhones erhalten kein iOS 18

Quelle: https://www.futurezone.de/digital-life/article544611/iphone-schneller-entsperren-trick.html

12) Manipulation von Kunden – Verbraucherzentrale mahnt Billig-Shop Temu ab

Die Verbraucherzentrale mahnt das Onlineshop-Unternehmen Temu wegen mehrerer Verstöße ab. Das sind die Hintergründe.

Den Online-Shop Temu gibt es erst seit knapp zwei Jahren – trotzdem hat sich die Plattform innerhalb kürzester Zeit zu den bekanntesten ihrer Art gemausert. Einer Umfrage vom Dezember 2023 zufolge landete Temu auf Platz vier der am meisten frequentierten Onlineshops in Deutschland. Toppen konnten das nur Amazon, Ebay und Otto.

Der Marktplatz steht aber auch oft in der Kritik. Denn so verlockend die günstigen Preise der zahlreichen Artikel aus allen möglichen Bereichen auch sind, die Qualität der Billigware lässt oft zu wünschen übrig. Und das ist nicht der einzige Kritikpunkt. Der Verbraucherzentrale Bundesverband (vzbv) hat die Plattform jetzt sogar abgemahnt, weil er mehrere Verstöße festgestellt hat.

Design der Temu-Webseite ist "manipulativ"

Konkret geht es dabei unter anderem um die intransparente Preisgestaltung und das manipulative Design der Webseite. Wie der vzbv in einer Pressemitteilung erklärt, weist Temu etwa hohe Rabatte von bis zu 70 Prozent aus – ohne Kundinnen und Kunden einen Referenzpreis zu nennen.

Potenzielle Käufer erhalten auf der Website zahlreiche Pop-ups und Hinweise, die sie zum Kauf bewegen sollen. Temu verspricht Rabatte, wenn eine bestimmte Anzahl von Produkten gekauft oder der Newsletter abonniert wird. Warnungen, dass ein Artikel bald ausverkauft ist oder der angebliche Rabatt bald abläuft, setzen die Verbraucher ebenfalls unter Druck.

Solche manipulativen Designs, auch "Dark Patterns" genannt, sind in der EU laut Digital Services Act seit dem 17. Februar 2024 verboten, wie der vzbv in seiner Mitteilung erklärt. Der Verband kritisiert zudem, dass Temu nicht ausreichend darüber informiert, wie die Authentizität von Produktbewertungen sichergestellt werden soll. Bereits in der Vergangenheit habe es den Verdacht gegeben, dass Bewertungen des Shops – auch auf Seiten wie Trustpilot – gefälscht seien.

Temu gaukelt Nachhaltigkeit vor

Es fehlen auch Informationen über die Identität der Produktanbieter. Temu agiert als Online-Marktplatz. Das bedeutet, dass das Unternehmen eine Art Vermittler zwischen Kunden und Händlern ist. Letztere sind sehr oft in China ansässig.

Und es gibt noch einen weiteren Marketingtrick, den die Verbraucherzentrale beanstandet. Denn Temu wirbt damit, dass Kunden ihren CO_2-Fußabdruck reduzieren können, wenn sie sich ihre Bestellung an eine Abholstation statt direkt nach Hause liefern lassen. Da aber viele Artikel aus China oder anderen fernen Ländern kämen, "haben die Produkte bereits weite Wege hinter sich, bevor sie ausgeliefert werden", so der vzbv.

Zu der Abmahnung erklärt die vzbv-Vorständin Ramona Pop, dass "Verbraucher und Verbraucherinnen vor derartigen Geschäftspraktiken geschützt werden müssen". Die Verbraucherzentrale rät generell zu Vorsicht beim Shoppen bei Temu. Hier können Sie nachlesen, warum.

Tipp: Chinesischer Versandhandel: "LightInTheBox": Seriöser Onlineshop oder Abzocke?

Quelle: https://www.t-online.de/digital/aktuelles/id_100372548/temu-kassiert-abmahnung-von-verbraucherzentrale-wegen-manipulation.html

13) Streaming-Dienst – Netflix: Neue Preiserhöhung gilt auch für Bestandskunden

Der Streaming-Anbieter Netflix erhöht seine Abo-Preise für Bestandskunden: Die vor Kurzem für Neukunden eingeführte Tarifanpassung gilt ab sofort auch für bestehende Abonnenten.

Vor wenigen Wochen passte der Streaming-Dienst Netflix die Preise für Neukunden an. Für das Standard-Abo, das für zwei Geräte in HD-Bildqualität gedacht ist, werden künftig 14 statt 13 Euro im Monat fällig. Premium-Abonnenten zahlen für 4K-Auflösung 20 statt 18 Euro monatlich, während das nur noch für Wechselkunden verfügbare Basis-Abo von 8 auf 10 Euro im Monat angehoben wurde.

Ursprünglich galt diese Preisanpassung nur für Neukunden ab dem 13. April - knapp zwei Wochen später setzt Netflix diese Änderung auch für Bestandskunden um. Wie das Portal Heise berichtet, werden betroffene Kunden derzeit per E-Mail über die gestiegenen Preise informiert. Immerhin bleibt das werbefinanzierte Abonnement vorerst unberührt und kostet weiterhin rund fünf Euro im Monat.

Damit diese Preiserhöhung wirksam wird, müssen Netflix-Kunden dieser explizit zustimmen. Im vergangenen Herbst sorgte ein Urteil des Kammergerichts Berlin dafür, dass Netflix und weitere Streaming-Anbieter die Preise nicht einseitig zulasten der Kunden anpassen dürfen. Allerdings ist man dennoch gewissermaßen dazu gezwungen, die Zustimmung zu geben: Wer der Anpassung nicht zustimmt, wird seitens Netflix automatisch gekündigt.

Quelle: https://www.connect.de/news/netflix-preis-erhoehung-mai-2024-bestandskunden-3205289.html?utm_source=nachrichten-NL&utm_medium=newsletter

14) Kabel-TV-Nebenkosten: Übergangsfrist endet am 30. Juni 2024 – Kabelfernsehen: Das müssen Mieter nach der Abschaffung des Nebenkostenprivilegs wissen

Das „Nebenkostenprivileg“ für Kabelgebühren ist zwar schon seit gut zwei Jahren aufgehoben, die Übergangsfrist endet aber erst am 30. Juni 2024. Für Kabel-TV-Kunden ergeben sich daraus nicht nur Vorteile.

Vielleicht haben auch Sie wie rund 12,5 Millionen andere Mieter in Deutschland schon Post von Ihrem Vermieter oder der Hausverwaltung erhalten oder Werbung von einem Kabelfernsehanbieter. Was hat es mit dem Wegfall des „Nebenkostenprivilegs“ auf sich, von dem darin die Rede ist?

Das **Nebenkostenprivileg** wurde in den 1980er-Jahren eingeführt, um die Verbreitung des damals noch neuen Kabelfernsehens zu fördern. Die Idee dahinter: Zwischen Hauseigentümer beziehungsweise Hausverwaltung und dem Kabelanbieter (ursprünglich ausschließlich Deutsche Bundespost) konnte ein Sammel- oder Mehrnutzervertrag geschlossen werden, sofern ein Mehrfamilienhaus einen gemeinsamen Kabelanschluss besaß.

Üblicherweise wurden die Kosten für den **Kabelanschluss** im Mietvertrag gemäß § 2 Nr. 15 der Betriebskostenverordnung (BetrKV) auf die **Mieter umgelegt**. Meist waren es Beträge unter 10 Euro monatlich. Der Haken: Das mussten die Mieter selbst dann bezahlen, wenn sie den Kabelanschluss gar nicht nutzten.

Entsprechend klagten mehrere betroffene Mieter, die Fernsehen auf anderen Wegen empfingen. Das Bundesverfassungsgericht sah in der üblichen Abrechnungspraxis einen Verstoß gegen die Rundfunkfreiheit und den Gleichbehandlungsgrundsatz. Das entsprechende Urteil vom Dezember 2018 zugunsten der Kläger mündete in der **Novellierung des Telekommunikationsgesetzes** (TKG). Es trat bereits am 1. Dezember 2021 in Kraft, die Übergangsfrist endet am 30. Juni 2024.

Von dieser Änderungen sind alle Mieter betroffen, in deren jährlicher **Nebenkostenabrechnung** ein Betrag für den Kabel-TV-Anschluss ausgewiesen ist. Die Umlage über die Betriebskostenverordnung endet automatisch – spätestens zum 30. Juni 2024. Eine gesonderte Kündigung ist nicht notwendig.

Was bedeutet der Wegfall des Nebenkostenprivilegs für Mieter?

Von der Änderung spätestens ab 1. Juli profitieren in erster Linie die Mieter, die den Kabelanschluss nicht genutzt haben, weil sie keinen Fernseher haben oder andere Empfangsmöglichkeiten wie Antenne, Satellit oder Internet bevorzugen. Wer weiterhin Kabelfernsehen empfangen will, kann einfach auf einen Werbebrief oder Anruf reagieren und einen neuen Vertrag bei dem regional zuständigen Kabelnetzanbieter abschließen. Wer das ist, hängt vom Wohnort ab.

In Deutschland gibt es über 50 verschiedene Anbieter für Kabel-TV beziehungsweise Internet über Kabel. Die beiden großen Kabelanbieter **Vodafone** und **Tele Columbus** mit seiner Marke PYUR haben ihre zuständigen Regionen weitgehend aufgeteilt. Die wichtigsten regionalen Anbieter finden Sie auf www.kabelfernsehen.info/regional. Sie wollen beim Kabel-TV bleiben? Gut so. Denn dann können Sie Ihre Empfangsgeräte weiter verwenden.

Welche Alternativen zu Fernsehen ohne Kabel-TV gibt es?

Sie sollten allerdings die Gelegenheit nutzen und mögliche Alternativen zum TV-Empfang via

Kabelnetz prüfen. Moderne Smart-TVs besitzen Triple-Tuner und sind von Haus aus für den Empfang von **DVB-T2 (Antenne)**, **DVB-C (Kabel)** oder **Satellit (DVB-S2)** vorbereitet. Ein zusätzlicher Receiver ist nicht notwendig.

Mit **DVB-T2 HD** haben Sie über eine Zimmerantenne oder eine Außenantenne Zugriff auf rund 40 öffentlich-rechtliche und private TV-Sender in HD-Qualität. Der größte Teil der HD-Programme privater Veranstalter ist ausschließlich im Programmpaket von freenet TV gegen eine Jahresgebühr von 85 Euro oder im Abo für 6,99 Euro monatlich empfangbar.

IPTV steht für Internet Protocol Television und bezeichnet die Übertragung von Fernsehsignalen über das Internet. IPTV liefert eine hohe Bild- und Tonqualität, interaktive Funktionen wie Video on demand und zeitversetztes Fernsehen sowie eine große Auswahl an Programmen. Für den Empfang können Sie bei vielen Internetprovidern IPTV-Pakete buchen. Bei der **Telekom** ist das MagentaTV. Sie benötigen dazu einen IPTV-fähigen Receiver, den Sie vom Anbieter mieten oder kaufen können, sowie einen Router und eine schnelle Internetverbindung.

Alternativ nutzen Sie für IPTV die **Apps der TV-Sender** auf Smart-TVs und Tablets oder einen kostenpflichtigen Anbieter wie **waipu.tv** (www.waipu.tv) oder **Zattoo** (zattoo.com/de), die bis zu 200 Sender ab 6,49 Euro monatlich bieten.

Satellitenempfang ist eine weitere Möglichkeit. Dafür wird eine Parabolantenne auf dem Dach oder an der Fassade eines Gebäudes installiert, die die Signale von einem Satelliten im Weltraum empfängt. Mit dieser Variante können Sie mehr als 400 deutschsprachige und internationale Sender in digitaler Qualität sehen, viele davon sogar in HD oder Ultra HD.

Die öffentlich-rechtlichen Sender sind kostenlos, für die Privaten brauchen Sie ein Abo bei HD Plus (www.hd-plus.de), für das 75 Euro pro Jahr fällig werden. Die Installation einer Satellitenschüssel ist allerdings nicht immer erlaubt oder möglich, zum Beispiel wenn Sie zur Miete oder in einem denkmalgeschützten Haus wohnen.

Schwarzseher: Kabel-TV auch ohne Vertrag empfangen

Wer zukünftig ohne Vertrag Fernsehen über Kabel empfängt, ist „Schwarzseher“. Möglich wird dies durch die antiquierte Hausverkabelung („**Baum-Struktur**“) in deutschen Wohnhäusern. Üblicherweise geht bei der Baum-Struktur vom Hausübergabepunkt (Verteiler) im Keller eine Leitung nach oben und verzweigt sich in den Stockwerken in die Wohnungen zur Kabeldose. So werden alle Wohnungen mit demselben Signal versorgt.

Das bedeutet: Nach aktuellem Stand der Technik lässt sich das TV-Signal **nicht für einzelne Wohnungen** abschalten. Um den unbezahlten Empfang zu unterbinden, müsste der Anbieter die Kabeldose mit einer Sperrvorrichtung versehen. Das muss der Mieter aber erlauben. Ohne Zustimmung darf der Techniker die Wohnung nicht betreten.

In neueren oder modernisierten Häusern besteht meist eine **Stern-Struktur**. Sie führt vom Hausübergabepunkt zu jeder Wohnung eine eigene Leitung. Diese kann ein Techniker im Verteiler für Nicht-Kabel-TV-Kunden vor Ort abklemmen, sofern der Kunde keinen Internetzugang über das Kabelnetz hat. Ob sich dieser Aufwand rechnet? Wohl kaum.

Darum werden die Kabelnetzanbieter die möglichen **Schwarzseher** tolerieren – zumindest so lange, bis andere technische Möglichkeiten als das manuelle Abklemmen existieren. Vodafone hat eine Lösung angekündigt, verrät allerdings weder den Termin noch Details der Umsetzung. Ohne gültigen Vertrag kann man in den meisten Wohnungen zwar weiterhin das TV-Signal über das Kabelnetz empfangen, legal ist das aber natürlich nicht.

Das **Strafgesetzbuch** definiert es unter § 265a als „Erschleichung von Leistungen“: „Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden

Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Der Versuch ist strafbar."

Das Problem dürfte die Beweislast des Kabelnetzanbieters sein. Denn ein TV-Gerät allein reicht nicht aus als Beweis für eine unbefugte Nutzung des nicht bezahlten Kabelnetzes, da es auch andere Empfangsmöglichkeiten gibt. Anders liegt der Fall, wenn der Mieter eine bereits angebrachte Sperrdose entfernt, um den Anschluss weiter zu nutzen. Das ist strafrechtlich relevant.

Fazit: Ruhe bewahren

Auch wenn der 1. Juli nicht mehr fern ist, besteht kein Grund, hektisch zu werden, sofern Sie vom Wegfall des Nebenkostenprivilegs betroffen sind und noch nicht gehandelt haben. Vielleicht ist ein Wechsel zu einer anderen TV-Empfangsart für Sie sinnvoll und spart sogar noch Geld. Es gibt immer wieder interessante Angebote.

Info: Vorsicht vor unseriösen Medienberatern

Die Änderungen beim Kabelanschluss rufen zahlreiche freiberufliche Verkäufer auf den Plan, die im Auftrag des Kabelnetzbetreibers als Medienberater unterwegs sind. Sie werden von diesen bei erfolgreichen Vertragsabschlüssen auf Provisionsbasis bezahlt.

Dabei geht es oft nicht mit rechten Dingen zu. Entsprechend gibt die Verbraucherzentrale wichtige Hinweise:

- Lassen Sie niemanden in die Wohnung – auch die unangekündigte Überprüfung des Kabelanschlusses wird meist nur als Vorwand zum Abschluss neuer Verträge genutzt.
- Lassen Sie sich nicht überrumpeln, und unterschreiben Sie nichts an der Haustür!
- Fragen Sie nach dem Dienstausweis der Medienberater und notieren Sie sich den Namen und gegebenenfalls die Kontaktdaten.
- Lassen Sie sich nicht einschüchtern: Niemand wird Ihnen von heute auf morgen den Fernsehanschluss wegnehmen!
- Erteilen Sie – falls notwendig – dem Medienberater Hausverbot.
- Falls die Medienberater ohne Erlaubnis in Ihre Wohnung kommen: Gehen Sie zur Polizei, und erstatten Sie eine Anzeige wegen Hausfriedensbruchs.
- Falls Sie (auch ohne Unterschrift) plötzlich eine Auftragsbestätigung im Briefkasten finden: Melden Sie den Fall der Verbraucherzentrale, und widerrufen Sie den Vertrag.
- Bei unerwünschten Werbeanrufen: Sagen Sie im Gespräch niemals „ja". Legen Sie im Zweifelsfall einfach auf – auch wenn es Ihnen unhöflich erscheint.
- Widersprechen Sie gegebenenfalls der postalischen Werbung (auch teiladressiert zum Beispiel „An die Bewohner des Hauses") und auch der Werbung per Telefon.

FAQ: Wegfall der Kabelfernsehen-Nebenkosten für Mieter

Was ist das Nebenkostenprivileg und warum wird es abgeschafft?

Das Nebenkostenprivileg wurde in den 1980er-Jahren eingeführt, um die Verbreitung des Kabelfernsehens zu fördern. Es ermöglichte, die Kosten für den Kabelanschluss im Mietvertrag über die Nebenkosten zu verteilen. Aufgrund eines Urteils des Bundesverfassungsgerichts, das diese Praxis als verfassungswidrig erklärte, endet das Privileg am 30. Juni 2024.

Wer ist vom Wegfall des Nebenkostenprivilegs betroffen?

Betroffen sind alle Mieter, in deren jährlicher Nebenkostenabrechnung ein Betrag für den Kabel-TV-Anschluss enthalten ist. Diese Umlage endet automatisch – spätestens zum 30. Juni 2024.

Was bedeutet der Wegfall des Nebenkostenprivilegs für Mieter?

Mieter, die den Kabelanschluss nicht genutzt haben, profitieren von der Änderung, da sie keine Gebühren mehr für einen Dienst zahlen müssen, den sie nicht in Anspruch nehmen. Wer weiterhin Kabelfernsehen empfangen will, muss einen individuellen Vertrag mit einem Kabelanbieter abschließen. Die Kosten variieren je nach Anbieter und Region.

Welche Alternativen gibt es zum Kabelfernsehen?

Es gibt mehrere Alternativen:

- **DVB-T2**: Empfang von Fernsehprogrammen über eine Antenne. Bietet rund 40 HD-Kanäle, erfordert jedoch eine Gebühr für einige private Sender.
- **IPTV**: Fernsehen über das Internet, oft als Teil von Internetpaketen erhältlich. Bietet eine breite Auswahl an Kanälen und interaktive Funktionen.
- **Satellitenempfang**: Ermöglicht Zugang zu mehr als 400 deutschsprachigen und internationalen Kanälen. Erfordert jedoch eine Satellitenschüssel, die möglicherweise nicht überall erlaubt ist.

Was passiert, wenn man ohne Vertrag weiterhin Kabelfernsehen empfängt?

Ohne gültigen Vertrag gilt der Empfang von Kabelfernsehen als "Schwarzsehen", was illegal ist und als "Erschleichung von Leistungen" betrachtet wird. Zwar ist die Beweislast für Kabelnetzanbieter hoch, jedoch könnten rechtliche Konsequenzen drohen, insbesondere wenn technische Sperrvorrichtungen entfernt werden.

Sollte ich sofort handeln oder kann ich mir Zeit lassen?

Auch wenn der 1. Juli nicht mehr weit ist, besteht kein Grund zur Eile. Überlegen Sie sich in Ruhe, ob Sie einen neuen Kabelvertrag abschließen oder auf eine andere Empfangsart umsteigen möchten. Ein Wechsel könnte sogar kostensparend sein. Suchen Sie nach Angeboten und vergleichen Sie die Kosten der verschiedenen Empfangsarten.

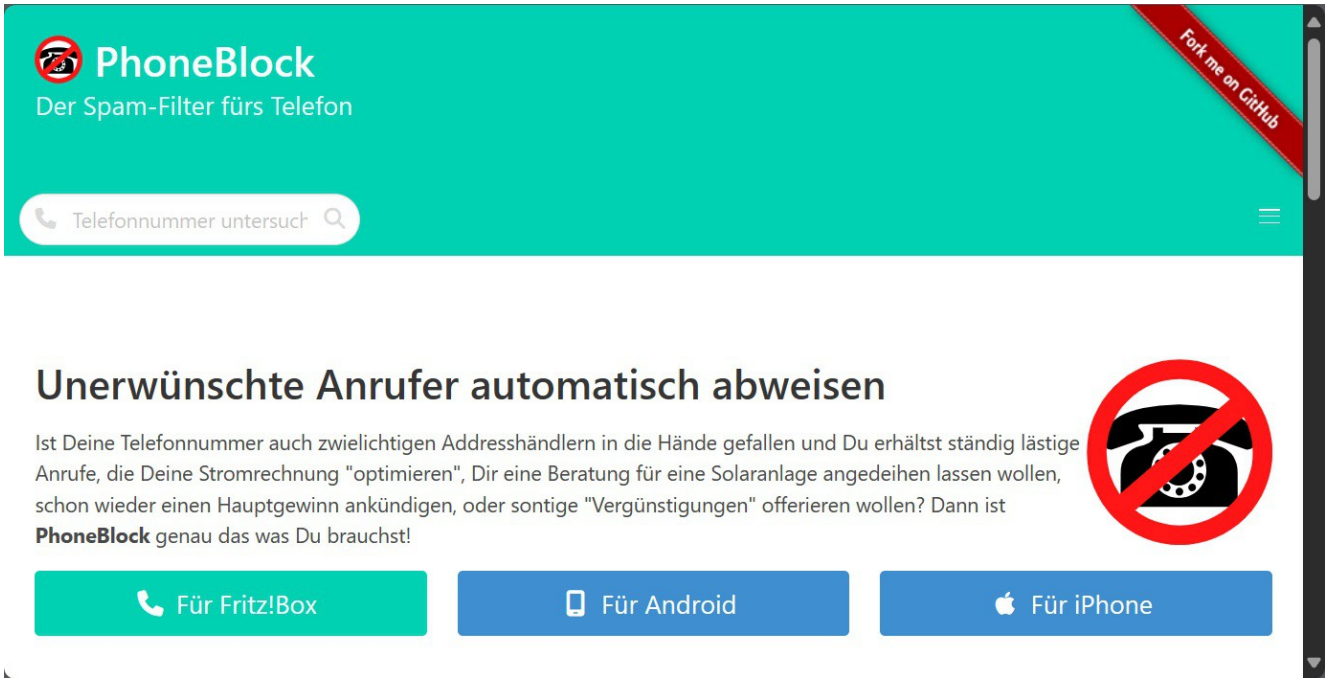
Quelle: https://www.connect.de/ratgeber/kabelfernsehen-abschaffung-nebenkostenprivileg-kabel-tv-nebenkosten-neue-regelung-mieter-infos-faq-3205249.html?utm_source=connect-NL&utm_medium=newsletter

15) Ratgeber – Genialer Gratis-Dienst blockt Spam-Anrufe auf der Fritzbox

Sie ärgern sich über nervige Spam-Anrufe? Als Besitzer einer Fritzbox mit angeschlossenen Telefonen weisen Sie Werbeanrufe künftig ganz automatisch ab. Möglich macht das der kostenlose Anrufschutz Phoneblock.

Sie werden ständig von Unbekannten angerufen und sind nach einiger Zeit wahrscheinlich ziemlich genervt von Werbetreibenden, Versicherungen, Marktforschern und Stromanbietern. Ist Ihre Festnetznummer erst einmal in den Datenbanken von Werbern und Kriminellen gelandet, beginnt der Telefonterror.

Klar – Sperrlisten kann man in der Fritzbox mit wenigen Mausklicks selbst anlegen. Doch komfortabler ist ein automatischer Anrufschutz, wie ihn Phoneblock kostenlos anbietet. Und das nicht nur für die Fritzbox, sondern auch für Smartphones (Android & iOS).



Quelle: Bild Christoph Hoffmann

Tipp: Hier geht's zur Phoneblock-Webseite

Nach kostenfreier Registrierung erhalten Sie Zugriff auf ein externes Telefonbuch, das Sie als Anrufschutz in die Fritzbox-Oberfläche einbinden. Das funktioniert ganz einfach, wie die folgende Schritt-für-Schritt-Anleitung zeigt.

Das Telefonbuch von Phoneblock enthält als unseriös eingestufte Rufnummern und erkennt unerwünschte Anrufer schon vor dem ersten Klingeln. Gesperrte Anrufe werden in der Anrufhistorie der Fritzbox als abgewiesen angezeigt.

Dank der automatischen Updates bleibt die Anrufsperrliste immer auf dem neuesten Stand. Ihr Vorteil: Nach der einmaligen Einrichtung sind keine weiteren Konfigurationen notwendig.

Phoneblock auf der Fritzbox einrichten

Beginnen Sie mit der kostenfreien Registrierung auf der Phoneblock-Webseite. Sie können sich mit Ihrem Google- und Facebook-Konto sowie einer Mail-Adresse anmelden. Tragen Sie diese in das entsprechende Feld ein und klicken Sie auf „Registrieren".

Sie erhalten eine E-Mail mit einem Code, den Sie auf der Webseite einfügen und mit einem Klick auf „Account erstellen" bestätigen. Sie erhalten dann auf der folgenden Webseite eine Zusammenfassung der benötigten Daten. Übernehmen Sie diese in einem Texteditor und speichern Sie die Datei, falls Sie die Installation wiederholen müssen.

Öffnen Sie nun die Fritzbox-Oberfläche über die Adresse „fritz.box" beziehungsweise „192.168.178.1" im Browser und melden sich mit Benutzername und Passwort (falls eingerichtet) an. Gehen Sie links in der Leiste zu „Telefonie", klicken Sie danach auf den Menüpunkt „Telefonbuch" und dann auf den Link „Neues Telefonbuch".

Benennen Sie das Telefonbuch mit „Blocklist". Darunter aktivieren Sie „Telefonbuch eines Online-Anbieters nutzen" und wählen als Anbieter im Aufklappfeld „CardDAV-Anbieter" aus.

Ihre persönlichen Daten ergänzen Sie unter „Internetadresse des CardDAV-Servers",

„Benutzername“ und „Passwort“. Weisen Sie das neue Telefonbuch dann noch einem oder mehreren Telefonen zu und bestätigen Sie mit einem Klick auf „OK“.

Hat alles funktioniert, lädt die Fritzbox alle Nummern aus der Phoneblock-Sperrliste und Sie sehen das neue Telefonbuch „Blocklist“ in der Rubrik „Telefonie > Telefonbuch“. Ein Klick auf das Register „Blocklist“ zeigt alle Nummern von aktuell hinterlegten Spam-Anrufern.

Unter „Telefonie > Rufbehandlung“ binden Sie das neue Telefonbuch „Blocklist“ als gesperrter Rufnummernbereich ein. Scrollen Sie nach unten bis zu dem Unterpunkt „Rufnummernbereiche sperren“ und klicken Sie auf „Bereich hinzufügen“.

Als Bereich wählen Sie „Gesamtes Telefonbuch“ und darunter „an alle Telefonnummern“. Als „Telefonbuch“ übernehmen Sie „Blocklist“ und bestätigen mit einem Klick auf „Übernehmen“.

Das war es. Die Einrichtung ist abgeschlossen. Ihre Telefone sollten jetzt deutlich weniger häufig wegen eines unerwünschten Anrufers klingeln. Und wenn doch, dann können Sie den Spammer ganz einfach blockieren und melden.

In der Fritzbox-Oberfläche sehen Sie die eingegangenen Anrufe. Unbekannte Nummern können Sie mit einem Klick auf das kleine Icon am Ende der Zeile im nächsten Schritt zum Telefonbuch „Blocklist“ hinzufügen.

Anmerkung der Redaktion: weitere Illustrationen sind unter dem u.g. Link abrufbar.

Tellows als kostenpflichtige Alternative

Mit über sieben Millionen monatlichen Nutzern in 50 Ländern ist Tellows die größte Community zur Rufnummernsuche und -bewertung in Deutschland. Die Tellows-Datenbank enthält rund zwei Millionen Bewertungen von Telefonnummern. Zu jeder Nummer werden Details wie Anrufertyp, Anrufername, Risikoeinschätzung, Herkunft, Anzahl der Suchanfragen und Bewertungen erfasst.

Den Anrufschutz gibt es als Telefonbuch zum Einbinden in die Fritzbox-Oberfläche sowie als App für Android-Smartphones und iPhones.

Quelle: https://www.pcwelt.de/article/2312412/phoneblock-fritzbox-spam-anrufe.html?utm_date=20240426140950&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Genialer%20Gratis-Dienst%20blockt%20Spam-Anrufe%20auf%20der%20Fritzbox&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

16) Feature – Seltsamer Bug: iPhone 15 lädt nicht per Kabel – das können Sie tun

In der aktuellen iPhone-Generation hat Apple Lightning duchrch USB-C als Port ersetzt. Doch offenbar gibt es damit Probleme – wir haben eine Lösung gefunden.

Die Bewegung gehört fast schon zur Abendroutine – zwischen dem Zähneputzen und Zubettgehen noch kurz das iPhone an das Netzteil anschließen. Diejenigen, die unseren Ratgeber “Das erledigt iPhone in der Nacht” gelesen haben, wissen, dass das Gerät wichtige Hintergrundaufgaben wie Indizieren der Fotos oder Synchronisierung mit der Cloud des Nächtens erledigt. Manche Aufgaben absolviert es aber nur, wenn es am Netzteil hängt.

So pflege ich das vor dem Schlafengehen auch: Das iPhone kurz ans Netzteil, bei mir ist ohnehin die Einstellung “80 %” bei der Batterie aktiviert, heißt, mein Smartphone lädt nur bis 80 Prozent und speichert keine weitere Energie mehr. Das lief ein halbes Jahr wunderbar, bis ich eines Abends bemerkt habe, dass bei Batteriesymbol kein Blitzzeichen aufgeleuchtet hat, als ich das Gerät an das Kabel ansteckte.

Am nächsten Morgen war das iPhone bis unter 20 Prozent entladen, ich habe dann das gleiche Kabel mit einem anderen Netzteil (vom Macbook Pro) ausprobiert, auch in der Kombination wollte das iPhone nicht laden. Eine halbe Stunde später im Büro habe ich das gleiche Experiment mit einer anderen Ausstattung ausprobiert, mit dem gleichen Ergebnis. Zwei USB-C-Kabel und drei unterschiedliche Netzteile, alle Originale von Apple, konnten mein iPhone nicht zum Laden bewegen. Der Grund musste das Gerät selbst sein, nicht das Zubehör.

Ich habe schon einen Support-Termin in einem naheliegenden Apple Store vereinbart, als der Kollege Müller einen Tipp gegeben hat: Das iPhone herunterfahren (Power- und Lauter-Taste einige Zeit drücken und danach ausschalten) und dann neu starten. Sein iPhone 15 hat nämlich das gleiche Verhalten an den Tag gelegt, nur zwei Monate früher. Wenn in einer recht kleinen Redaktion zwei Mitglieder das gleiche Problem erfahren, sollte dieses Problem höchstwahrscheinlich noch mehr Nutzer betreffen als uns.

Und tatsächlich, vor allem auf Reddit finden sich Berichte, dass das iPhone 15 plötzlich aufgehört hat zu laden. Der drahtlose Weg über Magsafe hat jedoch funktioniert (wie bei mir übrigens).

Auch in Apples Diskussions-Foren tauchen seit einigen Monaten die gleichen Berichte auf: Das iPhone 15 lädt nicht per Kabel, dafür über Magsafe (1, 2, 3, 4). Die ältesten Beiträge mit der Problembeschreibung sind von Ende Oktober bis Anfang November, so ist es mit großer Wahrscheinlichkeit anzunehmen, dass das Problem gleich vom Beginn bestand und nicht durch ein späteres iOS-Update verursacht wurde.

Quelle: https://www.macwelt.de/article/2315765/iphone-15-ladt-nicht-per-kabel.html?utm_date=20240426144000&utm_campaign=Macwelt%20Daily&utm_content=Title%20Story%3A%20Seltsamer%20Bug%3A%20iPhone%2015%20l%C3%A4dt%20nicht%20per%20Kabel%20%E2%80%93%20das%20k%C3%B6nnen%20Sie%20tun&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

17) FritzBox nicht erreichbar: Die Notfall-IP bringt Zugriff auf den WLAN-Router zurück

Ist der WLAN-Router nicht mehr erreichbar, hilft in vielen Fällen die sogenannte Notfall-IP. Über diese fest vergebene Adresse können Sie die WLAN-Zentralen verschiedener Hersteller immer erreichen.

Die meisten Nutzer werden nicht jeden Tag die Konfigurationsoberfläche des WLAN-Routers ansteuern, warum auch? Doch ab und an will man vielleicht doch Einstellungen anpassen, manuell auf Updates prüfen oder Infos auslesen. Bei der FritzBox tippen Sie im Browser nur **http://fritz.box** ins Adressfeld. Das kann man sich einfach merken und bringt Sie in der Regel zur Konfigurationsoberfläche.

Doch kürzlich hat jemand kurzerhand genau diese Box-Domain registriert. Statt auf der Router-Oberfläche landen Nutzer dann bei Fernzugriffen auf einer anderen Webseite. Besser ist es deshalb, auf den WLAN-Router über dessen IP-Adresse zuzugreifen. Doch die dürften die wenigsten Nutzer auswendig parat haben.

Wenn Sie die Standardeinstellungen nicht geändert haben, können Sie eine FritzBox auch immer über die IP-Adresse **192.168.178.1** erreichen. Bei den meisten FritzBoxen dürfte diese Einstellung unangetastet sein. Wenn Sie einen Reset ausführen, ist das immer die vorgegebene IP-Adresse. Doch Sie können die IP-Range auch anpassen, sodass diese Adresse ins Leere läuft.

Bei Fehlkonfigurationen oder wenn Sie die IP-Adresse vergessen haben, gibt es auch immer

noch eine **Notfall-IP**. Diese ist für alle FritzBoxen gleich. Standard ist so eine Notfall-IP in der Router-Welt zwar nicht, der ein oder andere Hersteller baut sie aber auch ein.

FritzBox Notfall-IP nutzen

Wenn die Benutzeroberfläche der FritzBox nicht erreichbar ist, gibt AVM Tipps und rät schließlich dazu, die Notfall-IP zu probieren. Die unterscheidet sich von der Standard-Adresse und gilt immer, egal, welche Netzwerkeinstellungen Sie selbst gesetzt haben. Tippen Sie im Browser **http://169.254.1.1** ein, dann sollten Sie die Konfigurationsoberfläche der FritzBox erreichen.

Das kann zum Beispiel dann nützlich sein, wenn Sie mit FritzBox und Repeatern ein Mesh-Netzwerk aufgebaut haben und die Konfiguration Probleme macht. Über die Notfall-IP sollten Sie dann immer bei der FritzBox oder dem angedockten FritzRepeater landen. Außerdem ist die Notfall-IP nützlich bei DNS- oder DHCP-Fehlern.

Notfall-IP für andere WLAN-Router

Dass FritzBoxen keine schlechte Wahl sind, sehen Sie in unserer Bestenliste WLAN-Router. Doch nicht jeder hat ein AVM-Gerät als WLAN-Router zu Hause stehen. Wir zeigen in der Tabelle unten, wie Sie die Konfigurationsoberflächen anderer WLAN-Router per URL und Standard-IP erreichen.

Notfall-IPs gibt es für:

- **1&1 Homeserver:** 169.254.1.1
- **Telekom:** 192.168.2.254
- **Synology:** 10.0.4.1

WLAN-Router Konfigurationsoberflächen

WLAN-Router	URL	Standard-IP
Telekom Speedport	http://speedport.ip	192.168.1.1, 192.168.2.1
Asus	http://router.asus.com	192.168.1.1
Netgear	http://routerlogin.net, http://routerlogin.com	192.168.0.1, 192.168.1.1
TP-Link	http://tplinkwifi.net	192.168.0.1, 192.168.1.1, 192.168.0.254
Synology	http://router.synology.com	192.168.1.1
Zyxel	http://myrouter.local	192.168.1.1
D-Link	http://dlinkrouter.local	192.168.0.1
Linksys	http://myrouter.local	192.168.1.1
Huawei	-	192.168.8.1
Edimax	http://edimax.setup, http://edimax.go	192.168.1.1, 192.168.2.1, 192.168.8.1
Vodafone EasyBox	http://easy.box	192.168.2.1

Quelle: https://www.chip.de/news/FritzBox-nicht-erreichbar-Die-Notfall-IP-bringt-Zugriff-auf-WLAN-Router-zurueck_184311389.html?utm_source=chip_1001311&utm_medium=email&utm_campaign=1012914&utm_content=26.04.2024

18) Tipp – USB-C: Vorsicht vor No-Name-Zubehör

Nachrüstbare magnetische USB-C-Adapter könnten Ihre Hardware beschädigen. Deshalb ist Vorsicht angesagt.

Herunterhängende oder locker am Boden liegende Netz- und Ladekabel für Smartphones, Tablets und Laptops können schnell zu Stolperfallen werden. Wenn Sie darin hängenbleiben, riskieren Sie, dass Ihr angeschlossenes Gerät vom Tisch gezogen wird.

Verhindern ließe sich das mit magnetischen USB-C-Anschlüssen, die eine Verbindung schnell lösen. Apple und Microsoft haben magnetische Anschlüsse für ihre Macbooks und Surface-Laptops. Diese Technik trennt die Verbindung zwischen Netzkabel und USB-C-Anschluss zuverlässig, bevor ein Gerät herunterfallen kann.

Sie könnten Ihr USB-C-Kabel natürlich mit einem magnetischen Adapter aufrüsten. Solche Adapter gibt es günstig im Internet – aber Vorsicht: Experten warnen, dass Sie damit Ihre Hardware schädigen könnten.

Viele über Amazon verkaufte Kabel und Zubehörteile werden in China hergestellt und erfüllen oft nicht annähernd die für Europa geltenden Sicherheitsbestimmungen, selbst dann nicht, wenn sie die CE-Kennzeichnung tragen.

Risiken beim Einsatz eines magnetischen Adapters

Das sind die Risiken, die Sie mit der Verwendung eines magnetischen Adapters eingehen:

- Gefahr elektrostatischer Entladung
- Datenverluste und Leistungseinbußen aufgrund elektromagnetischer Störungen durch die freiliegenden Pogo-Pins (die winzigen Metallstifte, die zur Herstellung des Kontakts herausragen)
- Gefahr von Lichtbogenschäden an den Pins in Umgebungen mit hoher Luftfeuchtigkeit
- Schmutz könnte zum Kurzschluss freiliegender Magnetstifte führen
- Magnetische Adapter sind nicht Teil der USB-C-Spezifikation

Vor allem der letzte Punkt sollte Sie davon abhalten, einen magnetischen No-Name-Adapter zu kaufen.

Bei der Entwicklung von USB-C ging man davon aus, dass ein USB-C-Kabel auch in einen USB-C-Anschluss eingesteckt wird. Die Ingenieure haben nicht erwartet, dass die Verbindung per Magnet erfolgen könnte.

USB-C ist unter anderem so konzipiert, dass bei einem Laptop mit einer Leistungsaufnahme von 65 Watt das Kabel plötzlich aus der Steckdose gezogen werden kann. Dabei wird das Risiko eines Lichtbogens minimiert, indem der Strom in einer bestimmten Zeitspanne abgeschaltet wird.

Eine Kabelverbindung per Magnet lässt sich viel schneller lösen. Wenn aber dann noch Strom durch das Kabel fließt, erhöht sich das Risiko eines Lichtbogens.

Apple und Microsoft verwenden sichere magnetische Anschlüsse an ihren Laptops (Microsoft hat sogar ein Patent auf einen magnetischen USB-C-Anschluss angemeldet), die Hardwareschäden und Datenverlust durch eine plötzlich auftretende Verbindungsunterbrechung verhindern sollen.

Es ist eher unwahrscheinlich, dass Sie diese Qualität auch bei einem kleinen Anbieter finden, der Magnetadapter für um die 10 Euro anbietet. In diversen Foren berichten Leute von Schäden an ihren Geräten, die durch den Einsatz solcher Adapter entstanden sind.

Und diese Berichte decken sich mit den Warnungen vor Interferenzen und Lichtbögen, die durch Metallteile, die in die magnetischen Anschlüsse gesaugt werden, die Ladeanschlüsse zerstören.

Es ist natürlich Ihre Entscheidung, ob Sie sich mit der Verwendung eines günstigen magnetischen Adapters und dem damit verbundenen Risiko wohlfühlen. Wägen Sie ab, was Sie mehr schmerzen würde – dass einmal ein Gerät herunterfällt, weil Sie über ein Kabel gestolpert sind, oder dass Sie Ihr Gerät durch die ständige Verwendung eines Billig-Adapters beschädigen.

Tipp:

- Die besten USB-C-Kabel im Test: Optimales Lade- und Datentempo
- USB-C: Vermeiden Sie diese Missverständnisse
- USB-C: Lösungen für 6 typische Probleme

Quelle:https://www.pcwelt.de/article/2313544/usb-c-vorsicht-vor-no-name-zubehor.html?utm_date=20240429102527&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20USB-C%3A%20Vorsicht%20vor%20No-Name-Zubeh%C3%B6r&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

19) News – Vorsicht vor Update KB5036979: Windows 10 drängt danach zum Erstellen eines Microsoft-Kontos

Microsoft erhöht den Druck auf Windows-10-Nutzer, sich mit einem Microsoft-Konto einzuloggen und das lokale Benutzer-Konto aufzugeben. So geht Microsoft vor und so stoppen Sie das Ganze.

Microsoft stellt ab sofort KB5036979 als optionalen Download für Windows 10 bereit. KB5036979 ist aus der Testversion/Preview Build 19045.4353 entstanden (siehe weiter unten). Doch aufgepasst: Wer KB5036979 freiwillig auf seinem Windows-10-Rechner installiert, bekommt einen nervigen Hinweise-Banner angezeigt, der zur Anmeldung mit einem Microsoft-Konto anstelle des lokalen Kontos drängen.

Sie können KB5036979 entweder über die Windows-Update-Funktion als optionales Update installieren oder direkt hier vom Microsoft-Update-Katalog herunterladen. Die Windows-10-Build-Nummer ändert sich dann zu 19045.4355.

Zum nächsten Patchday im Mai 2024 wird das jetzt noch optionale Update KB5036979 dann als Pflicht-Update im Rahmen des kumulativen Updates auf allen Windows-10-Rechnern installiert.

Wie der neue Hinweis-Banner aussieht, mit dem Microsoft Windows-10-Nutzer zum Einrichten eines Microsoft-Kontos drängt, lesen Sie im Folgenden.

So drängt Microsoft Windows-10-Nutzern plötzlich das Microsoft-Konto auf – so wehren Sie sich

Die Benutzung von Windows 11 setzt ein Microsoft-Konto voraus (Windows ohne Microsoft-Konto nutzen – so geht's). Anders ist es dagegen bei Windows 10, das man durchaus noch nur mit einem lokalen Benutzer-Konto und ohne Microsoft-Konto nutzen kann. Doch das will Microsoft offensichtlich ändern – sicherlich auch vor dem Hintergrund, dass Windows 10 mit deutlichem Abstand vor Windows 11 bei der Verbreitung liegt.

Denn wie Nutzer seit einigen Tagen berichten, führt Microsoft in der Testversion/Preview Build 19045.4353 des nächsten Windows-10-Updates einen unübersehbaren Hinweis in den Windows-Einstellungen ein, der die Nutzer zum Erstellen eines Microsoft-Kontos drängen soll. Diesen Hinweis blendet Windows 10 in Form eines großen Banners ein. Der Nutzer wird aufgefordert, sich mit einem Microsoft-Konto einzuloggen und zugleich nennt das Banner die Backup-Möglichkeit für Dateien und Fotos auf dem Onedrive-Speicher als Vorteil dafür.

Klickt man auf den prominent platzierten "Sign in now"-Button, so öffnet Windows 10 demnach die Windows-Backup-App. Um seine Dateien darüber auf dem Onlinespeicher Onedrive zu sichern, benötigt man eben ein Microsoft-Konto. An dieser Stelle kann man sich nun aber dagegen entscheiden und nicht auf den "Back Up"-Button klicken und somit kein Microsoft-Konto erstellen beziehungsweise sich nicht mit einem vorhandenen Microsoft-Konto anmelden. Sondern stattdessen zurück zu den Einstellungen gehen.

Es gibt also keinen Zwang dazu, ein Microsoft-Konto für Windows 10 zu benutzen, sondern Microsoft empfiehlt das nur sehr deutlich. Der Hinweis-Banner ist dann erst einmal weg. Bis zum nächsten oder übernächsten Neustart – dann erscheint der Banner erneut in den Windows-10-Einstellungen.

Microsoft erklärt diesen neuen Banner im Support-Dokument zur Windows 10 Build 19045.4353 für den Release Preview Channel folgendermaßen:

> *Neu! Dieses Update beginnt mit dem Rollout von kontobezogenen Benachrichtigungen für Microsoft-Konten in Einstellungen > Home. Ein Microsoft-Konto verbindet Windows mit Ihren Microsoft-Anwendungen. Das Konto sichert auch alle Ihre Daten und hilft Ihnen bei der Verwaltung Ihrer Abonnements. Sie können auch zusätzliche Sicherheitsschritte hinzufügen, um zu verhindern, dass Sie aus Ihrem Konto ausgesperrt werden. Diese Funktion zeigt Benachrichtigungen im Startmenü und in den Einstellungen an. Sie können Ihre Einstellungsbenachrichtigungen unter Einstellungen > Datenschutz und Sicherheit > Allgemein verwalten.*
>
> *Deutsche Übersetzung des englischen Originaltextes*

Dort müssen Sie dann die Option "Vorgeschlagene Inhalte in der Einstellungen-App anzeigen" abschalten. Danach sollten Sie von diesem Werbebanner verschont bleiben.

Bisher ist dieser Werbebanner für das Microsoft-Konto nur in der Preview Build 19045.4353 von Windows 10 zu sehen. Es ist aber damit zu rechnen, dass Microsoft dieses "Feature" zum nächsten Patchday am 14. Mai 2024 standardmäßig an alle Windows-10-Rechner ausliefert.

Quelle: https://www.pcwelt.de/article/2308865/windows-10-microsoft-konto-statt-lokalem-konto.html?utm_date=20240429104636&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Windows%2010%20dr%C3%A4ngt%20Nutzern%20pl%C3%B6tzlich%20Microsoft-Konto%20auf%20%E2%80%93%20so%20wehren%20Sie%20sich&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

20) Blitzer-Apps – Die besten Radarwarner-Apps für Android und iPhone

Mit Radarwarner-Apps sparen Sie Bußgelder und vermeiden Punkte in Flensburg. Wir sagen, was für und was gegen den Einsatz dieser Apps spricht und welche richtig gut sind.

„Piep, piep, piep“ und das Display des Handys leuchtet rot auf. Keine Frage, ein paar Meter weiter muss eine Radarfalle sein. Ein kurzer Blick auf den Tacho zeigt: 5 km/h müssen runter. Den Fuß vom Gas - und wieder ist alles gut gegangen. In Zeiten, in denen immer neue Radarfallen wie Pilze aus dem Boden schießen, ist die Nutzung von Radarwarner-Apps, kurz Blitzer-Apps, zu einem der beliebtesten Einsatzgebiete für Smartphones im Auto geworden.

Doch nicht alle Apps funktionieren zuverlässig, und so mancher beliebte Dienst ist inzwischen wieder eingestellt worden. Und wie sieht es überhaupt mit der rechtlichen Situation aus? Wir erklären, wie Radarwarner auf dem Smartphone funktionieren und welche guten Apps es für Android und iOS gibt. Außerdem fassen wir zusammen, ob und wann Blitzer-Apps in Deutschland verboten sind.

Die besten Radarwarner-Apps für Android und iPhone

In der folgenden Bildergalerie stellen wir Ihnen empfehlenswerte Blitzer-Warn-Apps vor. Wie Blitzer-Apps funktionieren, erklären wir weiter unten.

Auflistung Blitzer-Apps: https://www.connect.de/bildergalerie/blitzerwarner-apps-1505240.html

So funktionieren Radarwarner-Apps

Dank seines GPS-Empfängers weiß Ihr Handy immer, wo es sich gerade befindet. Diese Positionsinformation kann aber nicht nur zur Navigation genutzt werden. Auch Radarwarner-Apps greifen darauf zu und gleichen den aktuellen Standort mit Informationen über Radarfallen ab. Bewegt man sich auf eine Radarfalle zu, erscheint eine Warnung auf dem Display. Das System hat Stärken und Schwächen.

Fest installierte Radarfallen ändern sich selten

Die Standorte fest installierter Blitzer ändern sich nur selten. Deshalb werden sie besonders zuverlässig erkannt. Die in der App enthaltene Blitzerdatenbank veraltet entsprechend langsam.

Apps, die nur vor fest installierten Blitzern warnen, gehen daher in der Regel etwas sparsamer mit dem mobilen Datenvolumen um. Sie aktualisieren sich zu Hause per WLAN und kommen dann unterwegs ohne mobile Internetverbindung aus.

Meldesystem für mobile Radargeräte

Mobile Blitzer können innerhalb weniger Stunden auf- und abgebaut werden. Entsprechend schwierig ist es für Apps, vor diesen Geräten zu warnen. Hier setzen die meisten Anbieter auf die Community. Wer eine Radarfalle entdeckt, kann sie per Knopfdruck in der App melden und auf diese Weise andere Nutzer warnen. Dazu ist eine mobile Internetverbindung nötig, der Datenverbrauch hält sich aber in unmerklichen Grenzen.

Problematisch ist eher, dass Apps mit kleiner Community nur über wenige Meldungen verfügen. Entsprechend lückenhaft sind die Warnungen.

Schutz vor Falschmeldungen

Gegen digitale Vandalen, die aus Spaß eine Meldung absetzen, sind die Systeme recht gut geschützt - vermutlich, weil ein Standort erst von mehreren Fahrern gemeldet werden muss, bevor Warnungen an andere Fahrer in der Region verschickt werden.

Lesetipp: Handy mit altem Autoradio verbinden

Allerdings sind die Daten auch schnell veraltet. Manche Systeme fragen deshalb später vorbeifahrende Autofahrer, ob die Radarfalle noch steht. Das lenkt aber vom Verkehr ab.

Fehlalarme möglich

Da die Apps nur den Standort überwachen und bestenfalls mit einer Straßenkarte abgleichen, erkennen sie zwar zuverlässig, ob man auf eine Falle zufährt. Es kann aber auch zu Fehlalarmen kommen, etwa wenn man über eine Autobahnbrücke fährt und die Falle auf einer Straße unter der Brücke steht. In der Praxis ist das aber nur lästig und kein wirkliches Problem.

Smartphones, auf denen eine App installiert ist, die vor Blitzern warnt, gelten rechtlich als Radarwarngeräte. Dementsprechend gilt für sie § 23 Abs. 1c StVO, der die Benutzung durch Fahrzeugführer verbietet. Das Verbot betrifft sowohl reine Radarwarn-Apps wie auch Navigations-Apps mit entsprechendem Funktionsumfang.

Radarwarner-Apps für Beifahrer erlaubt?

Während der Fahrt darf der Fahrer entsprechende Apps also nicht nutzen, weder als Informationsquelle noch um neue Blitzer zu melden. Im Umkehrschluss bedeutet dies, dass man sich vor Fahrtantritt in der App über stationäre und mobile Blitzer informieren darf.

Inzwischen ist auch die Frage geklärt, was diese Regelung für Beifahrer bedeutet. Nach einem Urteil des Oberlandesgerichts Karlsruhe (AZ 2 ORbs 35 Ss 9/23) ist es auch Beifahrern untersagt, Blitzer-Apps zu nutzen und den Fahrer zu informieren. Das Urteil erfolgte im Hinblick auf eine Verkehrskontrolle, in deren Rahmen die Beifahrerin mit laufender Blitzer-App auf dem Handy erwischt wurde.

Ein Verstoß wird mit einem Punkt und einem Bußgeld von 75 Euro geahndet. Im europäischen Ausland drohen deutlich höhere Bußgelder und teilweise sogar Freiheitsstrafen. Eine Übersicht über die Regelungen in verschiedenen Ländern finden Sie beim ADAC.

Tipp: Schon die Installation einer Blitzerwarner-App auf dem Handy des Fahrers kann einen Verstoß gegen die Straßenverkehrsordnung darstellen. Ohne begründeten Verdacht darf die Polizei das Handy aber nicht beschlagnahmen oder überprüfen, welche Apps installiert sind.

Quelle: https://www.connect.de/ratgeber/radarwarner-blitzer-apps-legal-illegal-stvo-1505251-7320.html?utm_source=connect-NL&utm_medium=newsletter

21) Gratis, aber gefährlich: Diese VPN-Apps können Ihr Smartphone infizieren

VPN-Apps sind eine beliebte Wahl für sicheres Online-Surfen und Streaming. Jedoch meint es nicht jede dieser Anwendungen gut mit Ihrem Smartphone. Sicherheitsexperten haben nämlich 15 Apps im Play Store entdeckt, die Ihr Handy zum Zombie mutieren lassen können.

VPNs sind aus zwei Gründen sehr beliebt: Erstens kann man mit entsprechenden Apps sicher in unsicheren Netzen surfen und zweitens lassen sich damit Geoblockaden überwinden. Letzteres ist besonders für Streaming-Fans interessant, die ausländische Inhalte anzapfen wollen.

CHIP testet immer wieder Bezahl-VPNs und listet auch eine Auswahl seriöser kostenloser VPN-Dienste auf, aber wer im Play Store einfach so nach einem kostenlosen VPN sucht, kann Pech haben.

Eine Untersuchung von Sicherheitsexperten hat **15 kostenlose VPN-Apps** im Play Store gefunden, die bösartige Software enthalten. Die kann Ihr Handy zu einem Werkzeug für Cyberkriminelle machen.

Diese Apps sollten Sie sofort löschen

Android-Handys mit den betroffenen Apps können **zum Proxy für Kriminelle** werden – sozusagen ein Zombie, der von Fremden gesteuert wird. Grundsätzlich sind zwar auch seriöse Einsatzmöglichkeiten denkbar, doch auch Anzeigenbetrug, Spamming, Phishing oder Passwort-Spraying sind mit infizierten Geräten möglich.

Heimlich installierte Proxys knappsten Teile Ihrer Internet-Bandbreite ab, denn sie führen im Hintergrund Anweisungen von Kontroll-Servern aus und leiten Webanfragen an E-Mail-Seiten, Online-Händler, Twitch-Streaming-Plattformen und mehr weiter. Wenn Sie eine der aufgeführten VPN-Apps auf dem Handy haben, sollten Sie diese sofort löschen.

- Lite VPN
- Anims Keyboard
- Byte Blade VPN
- Fast Fly VPN
- Fast Fox VPN
- Fast Line VPN
- Oko VPN
- Quick Flow VPN
- Sample VPN
- Swift Shield VPN
- Turbo Track VPN
- Turbo Tunnel VPN
- Yellow Flash VPN
- VPN Ultra
- Run VPN

Nach dem Report hat Google reagiert und die VPN-Apps aus dem Play Store entfernt. Auch Google Play Protect, der eingebaute Virenschutz, sollte jetzt auf die verwendete Software anschlagen und entsprechende Apps blockieren. Erste Apps scheinen aber in neuer Version zurück zu sein. Ob sie dieses Mal sicher sind, darf man zumindest bezweifeln.

Quelle: https://www.chip.de/news/Gratis-aber-gefaehrlich-Diese-VPN-Apps-koennen-Ihr-Smartphone-infizieren_185208545.html?utm_source=chip_1001310&utm_content=29.04.2024&utm_medium=email&utm_campaign=1012842

Allgemeines:

1) Verbraucher – Sparkasse: Millionen Kunden betroffen – das kommt jetzt auf dich zu

Über tausend Kundinnen und Kunden haben eine Sammelklage gegen die Sparkasse eingereicht. Nun wurde das Urteil bekannt geben.

Wer sein Geld bei der **Sparkasse** anlegt, muss für gewöhnlich eine monatliche Kontoführungsgebühr zahlen. Weil diverse Banken diese in der Vergangenheit erhöht haben, ohne ihre Kund*innen zu informieren, hatte der Verbraucherzentrale Bundesverband (vzbv) kürzlich eine Musterklage eingereicht.

Berliner Sparkasse verliert vor Gericht

Das Berliner Kammergericht hat nun entschieden, dass Stillschweigen keine Zustimmung ist. Das Bankhaus hätte sich das Einverständnis ihrer Kund*innen holen müssen, um Kosten für Girokonten zu erhöhen oder einzuführen. Es erklärte die einseitigen Gebührenänderungen der Berliner Sparkasse seit dem Jahr 2016 für unwirksam, wie auf der offiziellen Seite des vzbv berichtet wird.

Für die Kostenerhöhung hat das Bankunternehmen zahlreiche Tricks angewandt. Zum Beispiel wurde Ende 2016 das „Girokonto Comfort“ auf „Giro Pauschal“ umgestellt und damit die monatliche Gebühr um drei Euro gesteigert. Die Sparkasse lehnt es bislang ab, diese Mehrbeträge zurückzuzahlen. Deshalb hat der vzbv eine Musterfeststellungsklage eingereicht. Knapp 1.200 Kund*innen haben sich angeschlossen und können, sobald das Urteil rechtskräftig ist, ihr Geld zurückfordern.

So bekommt ihr euer Geld zurück

Wegen dieses Urteils können derartige Preisänderungen durch andere Banken und Sparkassen ebenfalls keinen Bestand haben. Um herauszufinden, ob man von solchen unerlaubten Kostenerhöhungen ebenfalls betroffen ist, muss ein Blick auf die Kontoauszüge ab dem 01. Januar 2018 geworfen werden.

Wer ab 2018 eine Steigerung der Kontoführungsgebühr findet, kann einen Anspruch auf Rückzahlung haben. Die Verbraucherzentrale stellt dazu ein Musterschreiben zur Verfügung, diese müssen Kunden brieflich an ihre Bank schicken, um das zu viel gezahlte Geld zurückzufordern.

Quelle:https://www.futurezone.de/digital-life/verbraucher/article540880/sparkasse-millionen-kunden-betroffen-das-kommt-jetzt-auf-dich-zu.html?utm_source=flipboard&utm_content=Futurezone_de%2Fmagazine%2FFuturezone+News

2) Nach Starkregen, Sturm, Feuer – Unwetter oder Brand: Schäden dokumentieren für Versicherungen, Vorsicht beim Aufräumen

Mit dem Klimawandel steigt das Risiko für Stürme und Starkregen. Was tun bei Schäden, auch nach Feuer? Fotografieren für die Versicherung, dann wegräumen. Gefahren beim Aufräumen.

In Baden-Württemberg und Rheinland-Pfalz müssen sich die Menschen auf Sturm, Gewitter und Starkregen einstellen. Dann heißt es unter anderem, Gefahren vermeiden, lose

Gegenstände an Haus und im Garten sichern und das Auto möglichst sicher parken.

Viele fragen sich auch für den Brandfall: Passt mein Versicherungsschutz, und an was muss ich alles denken, wenn doch etwas passiert?

Gefahren nach Unwetter oder Brand: Strom, Heizöl, Dachziegel, Äste

- **Vorsicht Einsturzgefahr:** Wenn das Gebäude stark beschädigt ist, müssen Sie draußen bleiben. Verständigen Sie telefonisch die 112 und betreten Sie das Gebäude erst wieder, wenn es von Fachleuten freigegeben wurde.
- **Vorsicht Stromschlag:** Bei überfluteten Kellern besteht die Gefahr eines Stromschlags, wenn der Hausanschlusskasten im Keller untergebracht ist. Und: Nehmen Sie elektrische Geräte nur in Betrieb, wenn sie nicht feucht geworden sind.
- **Vorsicht Heizöl**: Wenn durch eine Überflutung im Keller Heizöl oder andere gefährliche Substanzen freigesetzt worden sind, rufen Sie ebenfalls die 112 an.
- **Vorsicht herabfallende Dachelemente:** Wenn das Dach stark beschädigt ist, zum Beispiel Dachpfannen, -ziegel oder -steine lose sind und herabzustürzen drohen, halten Sie sich fern. Verständigen Sie die Feuerwehr, damit die Gefahr abgesperrt oder beseitigt werden kann.
- **Vorsicht Astbruch:** Wurden beim Unwetter oder durch Feuer Bäume beschädigt, besteht auch noch danach die Gefahr, dass sie umkippen oder Äste herabstürzen. Im Zweifelsfall gilt auch hier: Informieren Sie die Feuerwehr und lassen Sie die Gefahr abklären.

Die Schäden und die Versicherung: Erst dokumentieren, dann aufräumen

Bevor es ans Aufräumen geht, sollten Sie sich zuerst mit der Schadensmeldung bei der Versicherung beschäftigen und gleichzeitig ihrer Schadensminderungspflicht nachkommen.

Unverzügliche Schadensmeldung:

Informieren Sie unverzüglich alle Versicherungen, die möglicherweise betroffen sind - möglichst noch am selben Tag. Bei Unwettern sind das in den meisten Fällen:

- die Gebäudeversicherung,
- die Hausratversicherung,
- die Elementarversicherung für Gebäude bzw. Hausrat
- und gegebenenfalls die Autoversicherung.

Wenn Sie mit der Schadensmeldung zu spät kommen, könnten Sie leer ausgehen. Wichtig ist es erstmal, den Schaden grundsätzlich zu melden und dabei eine Schadensnummer vom Versicherer zu erhalten.

Eine genaue Auflistung aller Schäden im Detail ist später noch möglich. Die Meldung geben Sie am besten schriftlich weiter oder über ein Formular des Versicherers im Internet. Aber Vorsicht: Achten Sie darauf, dass Sie eine Kopie des ausgefüllten Formulars bekommen.

Eine ausführliche Liste für den Versicherer mit den erforderlichen Angaben zu Wert und Kaufzeitpunkt der Gegenstände ist binnen zwei Wochen nötig. Nach mehr als zwei Wochen kann es eng werden. Das Landgericht Oldenburg etwa fand drei Wochen zu lang. Nachdem ein Kunde sich so viel Zeit ließ, durfte der Hausratversicherer seine Zahlung um 40 Prozent kürzen (Az. 13 O 3064/09).

Folgeschäden vermeiden:

Geschädigte sind verpflichtet, den Schaden so klein wie möglich zu halten. Das heißt, Sie müssen alles unternehmen, was möglich und zumutbar ist, um Hausrat und Gebäude vor

weiteren Schäden zu bewahren.

Decken Sie beispielsweise kaputte oder undichte Dachbereiche direkt nach dem Unwetter oder Brand mit einer Plane gegen Regen ab. Kommen Sie ihrer sogenannten Schadensminderungspflicht nicht nach, muss die Versicherung möglicherweise Folgeschäden daraus nicht bezahlen.

Beweise sichern:

Fotografieren oder filmen Sie den Schaden - am besten aus verschiedenen Blickwinkeln und gut beleuchtet. Und achten Sie bei dieser Dokumentation darauf, dass unstrittig zu erkennen ist, wann Sie die Fotos aufgenommen haben.

Aufbewahrungspflicht:

Lassen Sie die Schadensstelle aber bis zur Besichtigung durch den Versicherer ansonsten möglichst unverändert.

Bewahren Sie die beschädigten Sachen möglichst so lange auf, bis die Versicherung sie begutachten konnte oder ausdrücklich darauf verzichtet.

Rücksprache vor Auftragsvergabe und Neukauf:

Müssen Sie zur Abwehr von Schaden unverzüglich handeln, nehmen Sie trotzdem vorher Kontakt mit der Versicherung auf.

Auch wenn Sie Reparaturaufträge vergeben oder Gegenstände neu kaufen wollen, sollten Sie vorher Rücksprache mit der Versicherung halten und auch die Höhe der Versicherungsleistung erfragen.

Regulierer vertritt Interessen der Versicherung:

Oft wird der Versicherer einen so genannten "Regulierer" vorbeischicken, der sich den Schaden anschaut. Dabei handelt es sich nicht um einen unabhängigen Gutachter. Der Regulierer wird vom Versicherer bezahlt und vertritt dessen Interessen.

Es ist daher ratsam, sich die angebotene Regulierung genau anzuschauen und im Zweifelsfall kritisch zu hinterfragen.

Fristen für die Zahlung:

Viele Versicherungen zahlen nicht sofort - sie dürfen ihre Leistungspflicht und die Höhe des Schadens eingehend prüfen.

Einen Monat nach der Schadensmeldung haben Sie jedoch Anspruch auf eine Abschlagszahlung in Höhe des Betrags, der zu diesem Zeitpunkt bereits unstrittig feststeht. Setzen Sie notfalls eine Frist.

Nachfragen und Kontakt halten mit der Versicherung hilft:

Gibt es viele Geschädigte und ist die Situation unstrittig, ergeben sich daraus manchmal auch unkonventionelle Lösungen, und bei so mancher Versicherung kann ein Handwerker beispielsweise direkt mit der Versicherung abrechnen. Nachfragen lohnt sich also.

Erst rechnen, dann Schaden begleichen lassen:

Es lohnt sich nicht bei jedem Schaden, ihn von der Versicherung begleichen zu lassen. Denn nach einem Schadensfall haben sowohl Sie als auch der Versicherer ein Sonderkündigungsrecht.

Es lohnt sich daher zu prüfen, ob man einen Bagatellschaden einreicht oder lieber selbst begleicht. Dies gilt insbesondere, wenn man schon mehrere Schäden bei der Versicherung gemeldet hat und befürchten muss, keine gleichwertige Versicherung mehr zu bekommen.

Gutachten und Ombudsmann helfen bei Ärger mit der Versicherung

Wenn die Summe feststeht und die Zahlung ausbleibt, fordern Sie hartnäckig die Schadenssumme ein. Hilft das nicht, kann man sich beim Ombudsmann für Versicherungen, derzeit die Ombudsfrau für Versicherungen, beschweren. Sie überprüft den Fall als neutrale Stelle - kostenlos.

Kommt ihnen die angebotene Summe zu niedrig vor, sollten Sie über ein unabhängiges Schadensgutachten oder ein Privatgutachten nachdenken.

Wie kommt man an ein unabhängiges Schadensgutachten?

Es ist sinnvoll, beim Amtsgericht vor Ort einen Antrag auf ein sogenanntes "Selbständiges Beweisverfahren" zu stellen. Dann beauftragt das Gericht einen Sachverständigen, der den Schaden begutachtet.

Ab einer Streitsumme von 5.000 Euro braucht man einen Rechtsanwalt, der diesen Antrag stellt. Die Ergebnisse des Gutachtens können in einem etwaigen Gerichtsprozess verwendet werden. Oft lenken die Versicherer aber ein, wenn ein solches Gutachten vorliegt.

Außerdem kann man sich mit den Ergebnissen auch an den Versicherungsombudsmann wenden.

In welchen Fällen hilft der Versicherungsombudsmann?

Der Versicherer sollte Mitglied beim Versicherungsombudsmann e.V. sein. Dann können Streitigkeiten bis zu 100.000 Euro außergerichtlich geschlichtet werden. Bei Schäden bis zu 10.000 Euro muss sich das Versicherungsunternehmen an die Entscheidung halten.

Gibt es allerdings nur ein Gutachten der Versicherung, entscheidet der Ombudsmann auf dieser Grundlage. Er lässt keine eigenen Gutachten erstellen.

Lohnt sich ein Privatgutachter?

Ein Privatgutachten auf eigene Faust in Auftrag zu geben, ist riskant. Die Kosten von oft mehreren tausend Euro, müssen Sie häufig auch tragen, falls Sie später einen Prozess gewinnen.

Wer entsprechend rechtsschutzversichert ist oder einen Versicherungsvertrag hat, der auch einen selbstgewählten Gutachter bezahlt, kann selbst ein Privatgutachten in Auftrag geben. Am besten ist ein gerichtlich vereidigter Sachverständiger.

Aber Achtung: Die Ergebnisse werden mitunter vor Gericht nicht verwertet. Deshalb ist ein "Selbständiges Beweisverfahren" häufig vorzuziehen.

Nach den meisten Versicherungsverträgen ist ein sogenanntes Sachverständigenverfahren möglich, bei dem beide Parteien eigene Gutachter beauftragen können. Leider zahlen bei diesem Verfahren die Auftraggeber ihre Gutachter meist selbst. Außerdem hat der Versicherte anschließend schlechte Karten, wenn es doch noch zu einem Rechtsstreit vor Gericht kommt.

Tipp: Wem das alles zu kompliziert ist, der kann sich auch an eine Verbraucherzentrale wenden. Dort werden spezielle Beratungen im Schadensfall angeboten.

Sorgen Sie vor: Überprüfen Sie ihren Versicherungsschutz!

Noch mal glimpflich davongekommen? Das kann sich schnell ändern, denn Orkane, Tornados, Wirbelstürme, heftige Gewitter, Schneechaos oder Starkregen sowie Brände gehören auch in unseren Breiten zum Jahreslauf.

Durch den Klimawandel könnten sich Unwetterereignisse häufen. Die dadurch verursachten immensen Schäden können Jeden treffen.

Daher unser Tipp: Betrachten Sie das Unwetter als Warnung und überprüfen Sie ihren Versicherungsschutz.

Quelle: https://www.swrfernsehen.de/marktcheck/unwetter-hochwasser-sturm-schaeden-richtiges-vorgehen-100.html

3) Deal – Wozu Makita oder Einhell? Dieser 2-in-1 Akku-Rasentrimmer & Kantenschneider zum Bestpreis erleichtert die Gartenpflege

Der Worx WG163E.1 20V Akku-Rasentrimmer gehört zu den Bestsellern auf Amazon. Er ist derzeit im Angebot so günstig wie schon lange nicht mehr.

Ein Garten pflegt sich leider nicht von selbst. Ein Mähroboter kann dabei eine erhebliche Hilfe sein – die kommen bei hohem Gras oder Rasenkanten aber an ihre Grenzen. Um nicht mit der Schere in der Hand alle Ecken perfekt auf eine Höhe bringen zu müssen, eignen sich leistungsstarke Akku-Rasentrimmer. Obwohl die Geräte von Einhell und Makita sehr gefragt sind, macht Worx hier gerade Konkurrenz.

So gibt es für kurze Zeit den Worx WG163E.1 20V Akku-Rasentrimmer inklusive Akku und Ladestation dank 13 Prozent Preisreduzierung für nur 81,36 Euro. Dabei handelt es sich um den aktuellen Bestpreis – noch günstiger gab es das Bundle zuletzt im Juli letzten Jahres. Wer nicht so lange warten und hoffen mag, sollte beim befristeten Angebot auf Amazon zuschlagen, denn die Rabattaktion kann auch enden, sobald der Vorrat aufgebraucht ist. Bereits 21 Prozent des Kontingents seien laut Amazon vergriffen.

Das hat der Worx WG163E.1 20V Akku-Rasentrimmer und Kantenschneider zu bieten

Das Gartenwerkzeug Worx WG163E.1 ist Rasentrimmer und Kantenschneider in einem, dank des um 90 Grad drehbaren Trimmkopfes. Dadurch sei er praktisch für schwierige Ecken. Eine Schnittbreite von 30 cm im Durchmesser sorge für einen möglichst gleichmäßigen Schnitt des Rasens. Zudem verfügt er über eine automatische Fadenverlängerung auf Knopfdruck mit dem “Command-Feed-Feature”.

Das vielleicht praktischste an Akku-Rasentrimmern: Es wird kein Kabelsalat im Garten angebaut. Dank des Worx-PowerShare-Akkus mit 2 Ah kann man sich frei im Garten bewegen. Kompatibel ist er zudem mit allen 20 Volt-, 40 Volt- und 80 Volt-Geräten aus dem Worx-Kosmos – das bietet sich an, wenn man ohnehin schon elektrische Werkzeuge der Firma besitzt.

Zur einfachen Bedienung ist der Griff des Rasentrimmers verstellbar, ebenso wie die Länge, die je nach Körpergröße in der Höhe angepasst werden kann. Die robusten Inline-Räder helfen laut Worx dabei, bessere Kontrolle über das gerade mal 2,4 kg schwere Gerät zu behalten. Mit dem integrierten Pflanzenschutzbügel ist ein präzises und schonendes Trimmen um Pflanzen herum möglich, sodass man keine Angst haben muss, das Blumenbeet zu zersäbeln.

Aktuell bietet Amazon das Set bestehend aus dem 20V Akku-Rasentrimmer, einem 2Ah Li-Ion-Akku, Ladegerät und Spule zum Bestpreis von nur 81,36 Euro an. Für das Gerät sprechen nicht nur die Verkaufszahlen von 500 Stück allein im letzten Monat, sondern auch die Bewertung von 4,6 von 5 Sternen bei über 5.700 Kundenrezensionen. Das Feedback innerhalb der Kommentarspalte ist zudem durchweg positiv. Ist der Garten bislang nicht auf Vordermann gebracht, leistet der Worx-2-in-1-Rasentrimmer zuverlässige Arbeit, damit die nächste Grillparty zeitig stattfinden kann.

Das sollten Sie beim Kauf eines Akku-Rasentrimmers beachten

Beim Kauf eines Rasentrimmers sollten Sie verschiedene Faktoren berücksichtigen, um sicherzustellen, dass das Gerät Ihren Anforderungen entspricht. Hier sind einige wichtige Punkte, die Sie in Betracht ziehen sollten:

1. **Akkuleistung und -typ:** Überprüfen Sie die Akkukapazität, die in Amperestunden (Ah) angegeben wird, da diese die Laufzeit des Trimmers beeinflusst. Ein höherer Ah-Wert bedeutet in der Regel eine längere Betriebsdauer. Achten Sie auch auf die Art des Akkus; Lithium-Ionen-Akkus sind leichter, haben keine Memory-Effekte und bieten eine konstante Leistungsabgabe.
2. **Motorleistung und Schnittbreite**: Die Motorleistung beeinflusst die Effektivität, mit der der Trimmer Gras und Unkraut schneiden kann. Die Schnittbreite bestimmt, wie viel Bereiche Sie auf einmal bearbeiten können; größere Schnittbreiten reduzieren die Arbeitszeit auf größeren Flächen.
3. **Lärmpegel:** Akku-Rasentrimmer sind in der Regel leiser als benzinbetriebene Modelle, aber es gibt Unterschiede zwischen den verschiedenen Akkumodellen. Ein leiser Betrieb ist besonders wichtig in lärmsensiblen Bereichen.
4. **Verstellbare Funktionen und Zubehör:** Suchen Sie nach Modellen mit verstellbaren Teleskopstielen oder Griffen, die sich an verschiedene Körpergrößen anpassen lassen. Zusätzliche Aufsätze oder austauschbare Köpfe für verschiedene Schneidarbeiten können auch sehr nützlich sein.
5. **Kompatibilität mit anderen Akku-Werkzeugen**: Wenn Sie bereits andere Akku-Werkzeuge besitzen, prüfen Sie, ob die Akkus untereinander kompatibel sind. Dies kann die Gesamtkosten reduzieren und die Flexibilität erhöhen.

Durch die Berücksichtigung dieser Faktoren können Sie einen Akku-Rasentrimmer auswählen, der zuverlässig ist und Ihre Gartenpflege effizient und komfortabel macht. Laut der Kommentarschreiber auf Amazon ist dafür der Worx 2-in-1 Rasentrimmer und Kantenschneider bestens geeignet. Für einen unbekannten Zeitraum ist der Gartenhelfer für nur 81,36 Euro zu ergattern – jedoch kann das Angebot vorzeitig enden, wenn alle vorrätigen Artikel vergriffen sind.

Wer sich neben dem Worx WG163E.1 20V Akku-Rasentrimmer für weitere Spar-Angebote interessiert, der findet in der Aktions-Übersicht bei Amazon alle Rabattaktionen und Blitzangebote.

Tipp: Vor einem Kauf lohnt sich immer der Blick in: www.mydealz.de

Quelle:https://www.pcwelt.de/article/2314519/akku-rasentrimmer-bestpreis.html?utm_date=20240426134033&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Wozu%20Makita%20oder%20Einhell%3F%20Dieser%202-in-1%20Akku-Rasentrimmer%20%26amp%3B%20Kantenschneider%20zum%20Bestpreis%20erleichtert%20die%20Gartenpflege&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Neues Betreuungsrecht – Patientenverfügung und Vorsorgevollmacht: Die aktuelle Rechtslage

Welche Dokumente sollte jeder von uns vorbereiten? Alles Wichtige zu Betreuungsrecht, Vorsorgevollmacht und Patientenverfügung.

Inhalt:

Niemand denkt gerne darüber nach, es kann aber jeden treffen: Durch einen Unfall, eine Krankheit oder altersbedingt ist man plötzlich nicht mehr in der Lage, die eigenen Angelegenheiten zu erledigen.

Um festzulegen, wer diese Angelegenheiten dann für einen übernehmen soll, ist es prinzipiell für jeden ab 18 ratsam, sich um eine **Vorsorgevollmacht** zu kümmern. Sollten Sie beispielsweise nach einem Unfall im **Koma** liegen und es gibt keine Vorsorgevollmacht, muss erst vom Betreuungsgericht ein **Betreuer** bestellt werden – bis dahin kann niemand für Sie entscheiden. Mit einer Ausnahme: Sie sind **verheiratet** oder in einer eingetragenen Lebenspartnerschaft.

Ehegattennotvertretung: Begrenztes Vertretungsrecht

Seit Januar 2023 gibt es die sogenannte **Ehegattennotvertretung.** Ehegatten und eingetragene Lebenspartner haben im Notfall ein gegenseitiges **Vertretungsrecht** in **Gesundheitsangelegenheiten** sowie bei „kurzfristig freiheitsentziehenden Maßnahmen“ – wenn keine Vorsorgevollmacht oder Patientenverfügung anderen Inhalts vorliegt.

Mit kurzfristig freiheitsentziehenden Maßnahmen sind etwa die Fixierung des Patienten, ruhigstellende Medikamente, aber auch beispielsweise ein Bettgitter gemeint.

Die Neuerung im Betreuungsrecht erleichtert sicherlich für viele Paare zunächst einmal einiges. Dennoch haben Vorsorgevollmacht, Patientenverfügung und Betreuungsverfügung nichts an ihrer Wichtigkeit eingebüßt. Hier die Gründe:

Vorsorgevollmacht und Patientenverfügung: nach wie vor essenziell

- Das Notvertretungsrecht **läuft nach sechs Monaten aus**. Bin ich dann immer noch nicht wieder geschäftsfähig, wird vom Gericht ein Betreuer bestellt.
- Das Notvertretungsrecht bezieht sich **nur auf Ehegatten und eingetragene Lebenspartner**. Andere nahe Angehörige - wie beispielsweise Eltern oder Kinder - haben in solchen Fällen nach wie vor keine Rechte.
- Das Notvertretungsrecht betrifft **nur gesundheitliche Angelegenheiten**. Der gesunde Ehegatte oder Lebenspartner ist nicht befugt, Verträge des handlungsunfähigen Partners zu kündigen, finanziellen Forderungen, zum Beispiel von Behörden, in seinem Namen nachzukommen oder seinen Besitz zu verkaufen.

Ausnahmen beim Notvertretungsrecht durch Ehegatten

Wenn das Ehepaar oder die Lebenspartner **getrennt leben**, greift das Notvertretungsrecht

nicht. Personen, die **ausschließen** wollen, dass der Partner oder die Partnerin sie im Ernstfall vertritt, können dem Notvertretungsrecht widersprechen und den Widerspruch beim Zentralen Vorsorgeregister (ZVR) hinterlegen.

Wann kommt es zu einer rechtlichen Betreuung?

Wenn eine Person auf Dauer nicht mehr in der Lage ist, rechtliche Angelegenheiten allein zu regeln, kommt das Betreuungsgericht ins Spiel. Das Gericht legt fest, wer die rechtliche Betreuung der betreffenden Person übernehmen wird. Es gibt die Möglichkeit eines **ehrenamtlichen Betreuers** aus dem eigenen Umfeld, zum Beispiel der Partner, die Kinder oder gute Freunde. Wenn sich kein ehrenamtlicher Betreuer finden lässt, kommen **gesetzliche Betreuer** ins Spiel.

Aufgaben der gesetzlichen Betreuung

Eine gesetzliche Betreuung kümmert sich um **rechtliche Zuständigkeiten**, unter anderem um die **Kündigung** und **Organisation von Verträgen**. Sie ist nicht dazu da, im Alltag zu helfen oder Aufgaben einer Pflege zu übernehmen.

Neues Betreuungsgesetz seit 2023: Mehr Selbstbestimmung

Seit Januar 2023 gibt es ein **neues Betreuungsgesetz**. Im Fokus steht dabei das Recht auf Selbstbestimmung, das zu betreuende Personen haben sollen. Bis auf Ausnahmefälle, in denen sich Betroffene mit ihren Wünschen massiv selbst schaden, hat die Selbstbestimmung oberste Priorität.

Die betroffene Person kann einen **Betreuer vorschlagen oder ablehnen**. Ist der Betreute mit dem Betreuer unzufrieden, muss auch hier seinem Wunsch nachgekommen werden – das Gericht muss einen anderen Betreuer bestimmen oder die gewünschte Bezugsperson (Verwandte, Freunde etc.) einsetzen.

Zudem sieht die neue Rechtslage vor, dass Betreuer nach den **Wünschen der Betroffenen** handeln, auch wenn andere Maßnahmen aus wirtschaftlicher Sicht sinnvoller wären. Zum Beispiel kann ein Betreuer die Wohnung eines betreuten Menschen nur aufgeben, wenn die betroffene Person zustimmt. Damit sollen **Missbrauchsfälle** durch Betreuer künftig **verhindert** werden.

Abschotten und isolieren nicht mehr so einfach möglich

Seit 2023 ist es nicht mehr so einfach möglich, eine Person zu **isolieren** und beispielsweise von Freunden und Familie abzuschotten. **Besuchsverbote** sind nach der neuen Gesetzgebung nur noch möglich, wenn der Betreute explizit sagt: Ich will meinen Sohn, meine Tochter oder Person XY nicht mehr sehen.

Die **Familie** des Betreuten hat ab sofort auch einen **Anspruch auf Auskünfte**, beispielsweise was Diagnosen der Ärzte anbelangt.

Unterschied Vorsorgevollmacht, Betreuungsverfügung, Patientenverfügung

Mit einer **Vorsorgevollmacht** sorgen Sie dafür, dass eine von Ihnen bestimmte Person Ihre Angelegenheiten regeln kann, wenn Sie selbst nicht mehr dazu in der Lage sind. Als Bevollmächtigte sollte nur eine Person ausgewählt werden, der Sie **zu 100 Prozent vertrauen**. Es ist außerdem sinnvoll, die Vollmacht mit der oder dem Bevollmächtigten zu besprechen und sie oder ihn das Dokument ebenfalls unterzeichnen zu lassen.

Die Vollmacht kann auch auf **mehrere Personen** verteilt werden, ebenso können einzelnen Personen bestimmte Befugnisse zugeordnet werden. Wenn mehrere Personen eine Aufgabe wahrnehmen können, sollten Sie jedoch darauf achten, dass jede Person **auch alleine**

entscheidungsbefugt ist – ansonsten müssen immer alle Bevollmächtigten einig sein und entscheiden. Sind sie uneins oder ist jemand nicht erreichbar, kann nicht gehandelt werden.

Tipp: Das Bundesjustizministerium hat eine Broschüre zum Betreuungsrecht zusammengestellt, wo Sie alles Wichtige zum Thema nachlesen können inklusive Vorsorgevollmacht und der zugehörigen Formulare.

Mit einer **Betreuungsverfügung** kann man dem Betreuungsgericht bestimmte Personen als Betreuer vorschlagen. Im Grunde ist eine Betreuungsverfügung nicht unbedingt notwendig, wenn eine Vorsorgevollmacht existiert, schreibt die Verbraucherzentrale. Enthält sie jedoch Regelungslücken – beispielsweise, weil es Änderungen im Recht gab – muss für einzelne Entscheidungen möglicherweise doch ein Betreuer bestellt werden. Um diesen Fall sicher auszuschließen, sollte man trotzdem ergänzend eine Betreuungsverfügung verfassen.

In einer **Patientenverfügung** legt man fest, wie man in medizinischer Hinsicht behandelt werden möchte und welche Maßnahmen – vor allem am Lebensende – auf keinen Fall oder auf jeden Fall getroffen werden sollen.

Wenn Sie eine Patientenverfügung erstellen oder ändern wollen, sollten Sie sich im besten Fall mit ihrem Hausarzt oder ihrer Hausärztin besprechen – er oder sie sollte Ihren Gesundheitszustand am besten kennen. Ärzte können auch darüber aufklären, was einzelne Regelungen in der Realität tatsächlich bedeuten können. **Leider übernehmen die Krankenkassen die Kosten solcher Beratungsgespräche nicht.**

Wie sollte eine Vorsorgevollmacht aussehen?

Die Vorsorgevollmacht muss schriftlich mit Namen, Geburtsdatum und Anschrift des Vollmachtgebers abgefasst werden. Dieser unterschreibt sie mit Angabe von Ort und Datum.

Die Verbraucherzentrale bietet hier die Möglichkeit, kostenlos online eine Vorsorgevollmacht zu erstellen. Hier kann man sich auch beraten lassen.

Vorsorgevollmacht: beglaubigen lassen?

Die Vollmacht muss **nicht zwingend** beglaubigt werden. Sie erhält damit aber unter Umständen eine höhere Akzeptanz im Rechtsverkehr. Wenn allerdings auch Grundstücksgeschäfte mit der Vollmacht abgedeckt werden sollen, ist eine Beglaubigung notwendig.

Die **örtlichen Betreuungsbehörden** beglaubigen für 10 Euro Unterschriften auf Vorsorgevollmachten und Betreuungsverfügungen. Allerdings erlischt diese Beglaubigung mit dem Tod des Vollmachtgebers – auch das ist eine **Neuerung seit 2023**.

Unter Umständen – wenn zum Beispiel großes Vermögen vorhanden ist – ist eine notarielle Beglaubigung sinnvoll.

Bankvollmacht trotzt Vorsorgevollmacht?

Eigentlich deckt die Vorsorgevollmacht Bankgeschäfte mit ab. Dennoch kommt es hier immer wieder zu Problemen. Um dem vorzubeugen, sollte man überlegen, zusätzlich zur Betreuungsvollmacht bei der jeweiligen Bank eine Bankvollmacht ausstellen zu lassen.

Welche Betreuungsbehörde ist für mich zuständig?

Wer rund um das Thema Betreuung Unterstützung benötigt, sollte sich am besten an eine örtliche Betreuungsbehörde in der Nähe wenden. Betreuungsbehörden unterstützen die Vormundschaftsgerichte und helfen bei der Suche eines geeigneten ehrenamtlichen oder beruflichen Betreuers. Sie beraten außerdem Betreuer und Bevollmächtigte und helfen bei

Fragen zu Vorsorgevollmachten und Betreuungsverfügungen.

Außerdem gilt: **Ehrenamtliche Betreuer**, die der oder die Betreute nicht persönlich kennt, müssen an einen anerkannten Betreuungsverein oder die Betreuungsbehörde angebunden werden. So soll die Qualität der ehrenamtlichen Betreuung gesichert werden.

Die örtlichen Betreuungsbehörden sind bei den **Bürgermeisterämtern** der Stadtkreise und bei den **Landratsämtern** angesiedelt. Am einfachsten findet man die zuständige Behörde, wenn man den entsprechenden Landkreis plus „Betreuungsbehörde“ in eine Suchmaschine eingibt.

Für Baden-Württemberg gibt es auch diese Übersichtsseite.

Quelle: https://www.swrfernsehen.de/marktcheck/betreuungsrecht-vorsorgevollmacht-betreuungsverfuegung-patientenverfuegung-108.html