30. Cybercrime Newsletter

30.08.2022

1) WhatsApp-Falle: „Hallo Mama“-Betrug im MK gelingt - durch einen doofen Zufall

Ein unglücklicher Zufall: Eine Frau aus Iserlohn ist auf einen WhatsApp-Betrug hereingefallen. Sie glaubte dem „Hallo Mama“-Trick aus einem bestimmten Grund.

Iserlohn - Immer wieder warnt die Polizei vor Betrügern, die ihre Opfer etwa über WhatsApp kontaktieren. Eine beliebte Masche ist der „Hallo Mama“-Trick, bei dem die Betrüger vorgeben, das Kind des Opfers zu sein. Sie erzählen von einem kaputten Handy, einer neuen Rufnummer und einer dringend fällige Rechnung, die beglichen werden muss.

Diese Nachricht via Messenger bekam am Dienstagnachmittag auch eine Frau aus Iserlohn. Ein unglücklicher Zufall sorgte dann dafür, dass die 57-Jährige auf den Betrug hereinfiel: Das Handy ihrer echten Tochter sei tatsächlich kaputt gewesen, schilderte sie der Polizei. Deshalb glaube sie die Geschichte und überwies Geld auf ein Konto in Litauen.

WhatsApp-Falle gelingt: „Hallo Mama“-Betrüger treffen im MK ins Schwarze

Laut Polizei wurde die Mutter erst stutzig, als sie eine weitere Rechnungsforderung bekam. Sie stellte Fragen - und seitens der Betrüger wurde es plötzlich sehr still. Niemand reagierte mehr auf die Nachrichten. Die 57-Jährige informierte ihre Bank und erstattete Anzeige. „Ob es möglich war, die Überweisung noch zu stoppen, ist nicht bekannt“, so die Polizei.

Bei Geldforderungen über Telefon, E-Mail, SMS oder Messenger sollten Betroffene immer die Richtigkeit prüfen, also sicherstellen, dass sie den Anrufer oder Absender kennen. Die Polizei rät etwa beim WhatsApp-Betrug erst einmal die alte Telefonnummer des Kindes anzurufen.

Ist das Handy der Tochter oder des Sohns tatsächlich kaputt, wie im Fall der Iserlohnerin, sollten andere Wege gefunden werden.

Quelle: https://www.come-on.de/kreis-mk/iserlohn-mk-whatsapp-betrug-hallo-mama-polizei-zufall-geld-ueberweisung-warnung-91743458.html

2) Sparkassen-App "Mobiles Bezahlen" erhält starke Neuerung

Sparkassen-Kunden dürfen sich auf eine Neuerung in der App "Mobiles Bezahlen" freuen, die das mobile Bezahlen vereinfacht.

In der Sparkassen-App "Mobiles Bezahlen" und bei Apple Pay schalten die Sparkassen über die kommenden Wochen eine neue Funktion bei der digitalen Sparkassen-Card frei. Diese wird nach "Girocard" nämlich um das Zahlungsverfahren "Debit Mastercard"

erweitert, erhält also ein neues sogenanntes digitales Co-Badge. Damit können die Sparkassen-Kunden mit der neuen digitalen Version der Sparkassen-Card überall in Deutschland und weltweit mobil bezahlen. Die Kombination sei ein klares Bekenntnis "zum beliebten Zahlverfahren Girocard, mit dessen Vorteilen beim Bezahlen und Bargeldbezug in Deutschland", erklärt der Deutscher Sparkassen- und Giroverband.

Das Upgrade der digitalen Sparkassen-Card erfolgt laut der Mitteilung der Sparkassen automatisch, wenn die Kunden bereits von ihrer Bank die neue physische Sparkassen-Card mit den beiden Zahlungsverfahren "Girocard" und "Debit Mastercard" erhalten haben. Entsprechend können sie dann auch über "Debit Mastercard" über die App "Mobiles Bezahlen" (hier für Android im Google Play Store) auf Android-Geräten beziehungsweise über Apple Pay auf iOS-Geräten unterwegs kontaktlos bezahlen.

Sparkassen reagieren so auf Ende von Maestro im zweiten Halbjahr 2023

Bisher geben 50 Sparkassen in Deutschland die neue Sparkassen-Card mit Debit Mastercard-Funktion aus, andere Sparkassen werden folgen. Im 1. Quartal 2023 soll es auch das Debit-Zahlverfahren von Visa namens "Visa Debit" neben "Girocard" auf der digitalen Sparkassen-Card geben. Laut Angaben der Sparkassen sind zwei Bezahlsysteme auf einer digitalen Karte bisher nur in Australien, Neuseeland, Frankreich und Brasilien verfügbar.

Die Sparkassen dürfen selbst entscheiden, welches Kartenprodukt sie ihren Kunden anbieten. Der Deutsche Sparkassen- und Giroverband geht davon aus, dass die Mehrheit aller Sparkassen ab dem zweiten Halbjahr 2023 die Sparkassen-Card mit "Girocard" und einem zweiten Debit-Zahlverfahren von Mastercard oder Visa ausgeben werden.

"Die Einführung der digitalen Sparkassen-Card mit Girocard und Debit Mastercard ist ein wichtiger Baustein für die Neuausrichtung der Kartenstrategie nach der Ankündigung von Mastercard International Inc., sein Debit-Zahlverfahren Maestro ab dem zweiten Halbjahr 2023 in den meisten europäischen Ländern vom Markt zu nehmen", heißt es seitens der Sparkassen.

Quelle: https://www.pcwelt.de/news/Sparkassen-App-Mobiles-Bezahlen-erhaelt-starke-Neuerung-11286022.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3700617&pm_cat%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Urteil: Schon ein "Like" kann strafbar sein in sozialen Netzen

Schon ein "Like" in sozialen Netzen kann strafbar sein und zu einer Hausdurchsuchung führen. Das stellte jetzt ein Landgericht fest. Die Begründung.

Das Landgericht Memmingen hat ein Urteil (vom 05.08.2022, 6 Qs 146/22) gefällt, das alle Nutzer von sozialen Netzen aufmerksam lesen sollten: Schon ein "Like" kann strafbar sein. Ehssan Khazaeli, Rechtsanwalt des Verurteilten, meint dazu: "Danach kann das bloße Liken eines fremden Beitrages auf Facebook strafbar sein und zu einer Wohnungsdurchsuchung führen." Voraussetzung ist, dass der gelikte Beitrag strafbare Inhalte enthält.

Darum geht es

Ein Facebook-Nutzer hatte in Bezug auf die beiden bei Kusel am 31. Januar 2022 ermordeten Polizisten geschrieben: "Keine einzige Sekunde Schweigen für diese Kreaturen". Der von Rechtsanwalt Khazaeli verteidigte Beschuldigte gab diesem pietätlosen Posting ein Like. Daraufhin beantragte die Staatsanwaltschaft Meiningen die Durchsuchung der Wohnung, des Autos und der Person, die den Beitrag gelikt hatte, wie Khazaeli in seinem Blog schreibt .

Die Staatsanwaltschaft meinte, dass das "Like" den Tatbestand der Verunglimpfung des Andenkens Verstorbener nach § 189 StGB und der Belohnung und Billigung von Straftaten nach § 140 StGB erfüllen würde. Bei der Durchsuchung sollen Beweismittel wie Smartphones oder Speichermedien sichergestellt werden. Auch Onlinespeicher sollen durchsucht werden. Die zuständige Ermittlungsrichterin des Amtsgerichts Meiningen erließ den beantragen Durchsuchungsbeschluss und dieser wurde vollzogen.

Die Begründung des Landgerichts

Khazaeli legte im Auftrag des Beschuldigten Beschwerde ein, doch das Landgericht bestätigte nun das Vorgehen. Es begründet seine Entscheidung damit, dass sich der Beschuldigte mit seinem "Like" die fremde Äußerung zu eigen gemacht habe. Das Landgericht führt aus: " *Aus dem Kontext des Posts ist bei objektiver Betrachtung zu entnehmen, dass derjenige, der den Opfern eines Tötungsdelikts i.S.v. § 126 Abs. 1 Nr. 3 StGB jede Würde absprechen will, auch auf den Leitartikel, dessen Kommentierung unternommen wird, Bezug nimmt und letztlich die dort dargestellte Straftat des Mordes in 2 Fällen billigt. Wer demjenigen, der durch ein Verbrechen zu Tode gekommen ist, in der dargestellten Weise jede Anerkennung und Ehrung abspricht, heißt das Verbrechen an sich gut. Bei lebensnaher Betrachtung kann die Zustimmung, den Opfern ohne weiteres ein Mindestmaß an Menschenwürde abzusprechen, nicht anders als die Billigung des Zentralgeschehens verstanden werden, auf das allein das Gedenken Bezug nimmt.* “

Das Gericht fährt fort: " *Voraussetzung ist weiter, dass die Äußerung geeignet ist, den öffentlichen Frieden zu stören. Die Bezugnahme auf die Friedensschutzklausel ermöglicht es, das weit gefasste abstrakte Gefährdungsdelikt restriktiv auszulegen. Angesichts einer unkontrollierten Verbreitung der Billigung über das Medium Facebook ist dies – wie auch der Verlauf der hiesigen Ermittlungen selbst zeigt – ganz offensichtlich der Fall.* "

So geht es weiter

Khazaeli will nun Verfassungsbeschwerde gegen beide Entscheidungen einlegen. Damit soll grundsätzlich die Frage geklärt werden, "ob das bloße Liken auf sozialen Medien strafbar sein kann und zu Hausdurchsuchungen führen kann".

Quelle: https://www.pcwelt.de/news/Urteil-Schon-ein-Like-kann-strafbar-sein-in-sozialen-Netzen-11285419.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700601&pm_cat%5B0%5D=Social+Web&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Betrugsmaschen: Vorsicht bei Abholung durch angebliche Kurierdienste bei Kleinanzeigen-Apps

- **Betrüger am Telefon, im Internet oder an der Haustür gehen immer geschickter vor.**
- **Mit immer neuen Tricks versuchen sie, Daten oder Geld ihrer Opfer zu erbeuten.**
- **Aktuelle Betrugsmaschen im Überblick.**

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

Kleinanzeigen: Phishing bei Abholung durch angeblichen Kurierdienst

Update vom 26. August: Jemand kann die Kleinanzeigen-Ware angeblich nicht selbst abholen und bietet an, einen Kurierdienst zu schicken? Wenn einem so ein Vorschlag bei einem Deal unterkommt, sollte der Kontakt besser gleich abgebrochen werden. Denn dahinter steckt wahrscheinlich ein ausgeklügelter Phishing-Angriff auf Kreditkarten- oder Bankdaten, warnt das Verbraucherportal "Watchlist Internet"..

Die typische Vorgehensweise: Um die Sicherheitsvorkehrungen der Kleinanzeigen-Anbieter zu umgehen, werden User aufgefordert, auf einen anderen Kommunikationsweg zu wechseln, etwa auf Messenger, Kurznachricht oder Mail. Wer sich darauf einlässt, wird dann gebeten, die Abholung der Ware per Kurier zu akzeptieren. Es folgt ein Link zu einer gefälschten Website, die den vermeintlichen Kurierdienst erklärt. Dann schicken die Kriminellen einen weiteren Link, der zur ebenfalls gefälschten Seite eines Zahlungsdienstes führt. Dort sind Infos wie die angebotene Ware, die eigene Adresse und der Kaufpreis bereits angelegt.

Wer dann weiter klickt, wird aufgefordert, Kreditkarten- oder Kontoinformationen einzugeben – angeblich um das Geld zu erhalten. Tatsächlich geht es den Angreifern nur darum, die sensiblen Daten abzugreifen.

Verbraucherschützer raten deshalb, ausschließlich über das Nachrichtensystem des jeweiligen Kleinanzeigen-Anbieters zu kommunizieren sowie als Verkäuferin oder Verkäufer niemals Geld zu überweisen und keine angeblichen Vermittler zu akzeptieren. Zahlungsbestätigungen sollte man genau kontrollieren und angebliche Zahlungseingänge immer nur direkt am eigenen Bankkonto abgleichen. Zudem gilt: Verkäufe ins Ausland vermeiden, Waren am besten immer abholen lassen und Geld in bar entgegennehmen. (dpa)

Betrügerische Mail im Namen der Bundesregierung

Update vom 19. August: Vorsicht vor einer Mail im Namen der Bundesregierung, die zur Verifizierung von Kreditkartendaten aufruft. Hierbei handelt es sich um einen Betrug, warnt das Landeskriminalamt (LKA) Niedersachsen. Der Betreff der Mail lautet "Verifizierung ihrer Kredit- oder Debitkarte ist erforderlich, um eine Sperre zu vermeiden".

Demnach würde die Bezahlkarte des Empfängers nicht mehr den PSD2-Richtlinien der Europäischen Union entsprechen. Bis zum 31. August müsse die Kredit- oder Debitkarte deshalb verifiziert werden, andernfalls würde das Konto gesperrt. Wer dem beigefügten Link "Identität bestätigen" folgt, landet auf einer gefälschten Website mit Eingabemaske.

Haben Sie Ihre Kreditkartendaten hier bereits eingegeben, sollten Sie unverzüglich Ihre Bank informieren und die betroffene Karte sperren lassen, rät das LKA. Das ist jederzeit unter der Telefonnummer 116 116 möglich. Erstatten Sie außerdem Anzeige bei der örtlichen Polizei oder der Onlinewache, wenn verfügbar.

Warnung vor neuer Betrugsmasche mit Kryptowährungen

Update vom 26. Juli: Vor einer neuen Betrugsmasche mit Kryptowährungen warnt die Berliner Polizei. Die mutmaßlichen Täter nehmen dabei nach bisherigen Erkenntnissen zunächst telefonisch Kontakt zu Menschen auf, die im Kryptowährungshandel Verluste gemacht haben, wie die Polizei am Montag mitteilte.

Später werde die Kommunikation per E-Mail fortgesetzt. Dabei geben sich die Betrüger als Beschäftigte der Zentralen Ansprechstelle Cybercrime der Polizei Berlin (ZAC) aus, wie es hieß. Den Betroffenen werde dann vorgegaukelt, sie könnten die eingefahrenen Verluste im Kryptowährungshandel gegen Zahlung in Vorkasse wettmachen.

Nach den Angaben werden in dem per E-Mail verschickten Schreiben die Logos des Bundeskriminalamtes und der Berliner Polizei verwendet. Die geforderte Zahlung

bezeichneten die Betrüger als Darlehen, das in einer Kryptowährung gezahlt oder in bar übergeben werden könne. Die Verdächtigen sollen sich als "Wiederherstellungs-Agenten" bezeichnen und mit einem Foto einer Schweizer Identitätskarte legitimieren, wie es hieß.

Nach Angaben einer Polizeisprecherin liegt dem Landeskriminalamt bislang zwar keine Vielzahl solcher Fälle vor. Es sei den Ermittlern aber wichtig, "die Masche zu benennen, damit die Betrüger gar nicht erst die Chance haben, damit das große Geld zu machen." Möglichen Betroffenen rät die Polizei nicht auf Zahlungsaufforderungen zu reagieren und Anzeige zu erstatten.

Falscher Paketdienst-Chatbot greift Daten ab

Update vom 12. Juli: Eine neue Phishing-Variante mit vermeintlichen Nachrichten vom Paketdienst ist im Umlauf. In den E-Mails mit Betreff wie "Track and Trace DHL" ist die Rede von angeblichen Paketen mit beschädigtem Adressaufkleber. Empfängerinnen und Empfänger werden gebeten, fehlende Angaben per Chatbot zu ergänzen. Bei einem Chatbot handelt es sich um eine Anwendung, die das Chatten beziehungsweise einen Dialog mit einem technischen System erlaubt.

Aktuell warnt die Verbraucherzentrale Nordrhein-Westfalen davor, auf die genannten Nachrichten zu reagieren. Die Mails sollten direkt in den Spamordner verschoben werden.

Wer nämlich über den Link in der Mail den Chatbot ("virtueller Guide Suzy") öffnet, spielt das miese Spiel der Betrüger bereits mit. Mail und Chatbot haben natürlich nichts mit irgendeinem Paketdienst zu tun, sondern sind frei erfunden, um Nutzerinnen und Nutzern Adressen und weitere persönliche Daten abzujagen.

Der Chatbot tritt wirklich in einen Dialog mit den Nutzerinnen und Nutzern, zeigt Nummern zur Sendungsverfolgung und sogar Fotos der vermeintlichen Pakete an. Die Gefahr ist den Experten zufolge daher sehr groß, auf diese Masche hereinzufallen.

Jeder E-Mail-Nutzer muss von diesen Erpressermails mit erfundenen Druckmitteln gehört haben

Update vom 27. Juni: Das Vorgehen ist simpel und trotzdem raffiniert: Betrüger versuchen per E-Mail, Geld zu erpressen. Und zwar mit Druckmitteln, die sie oft frei erfinden und kombinieren, in der Hoffnung, dass ihre potenziellen Opfer darauf anspringen, warnt das Landeskriminalamt (LKA) Niedersachsen. Häufige Maschen im Überblick:

- **Passwort-Trick:** In der Mail behaupten die Kriminellen, sie hätten den Empfänger oder die Empfängerin gehackt. Sie nennen ein schwaches, unsicheres Passwort, das der oder die Angeschriebene tatsächlich nutzt oder genutzt hat. Es stammt aber mit großer Wahrscheinlichkeit aus anderen Hacker-Angriffen und ist ohnehin meist frei im Netz auffindbar, so das LKA.

Bislang seien keine Fälle bekannt, in denen in Erpresser-Mails auch komplexe, sichere und tatsächlich genutzte Passwörter gestanden hätten. Die Täter sind also meist Trittbrettfahrer.

Nach dem Passwort-Aufhänger folgt in der Mail etwa ein Fantasie-Text. Beschrieben wird, in welche Geräte, Konten und Lebensbereiche die Angreifer angeblich schon vorgedrungen seien und welche Geheimnisse sie angeblich schon herausgefunden haben wollen. Natürlich gilt hier, falls nicht bereits geschehen: Das kompromittierte Passwort ändern.

- **Absender-Trick:** Es sieht so aus, als ob man eine Mail von seinem eigenen Account bekommen hat - und schlussfolgert daraus, dass die Erpresser wirklich Zugriff darauf haben. Doch dahinter steckt ein einfacher technischer Trick namens Mail-Spoofing, erklärt das LKA.

Auf diese Weise könne man - wie auf einem Briefumschlag - einen beliebigen Absender der jeweiligen E-Mail nennen. Ziel sei es, die Angeschriebenen zu verwirren, um den Inhalt glaubhafter wirken zu lassen. Tatsächlich haben und hatten die Kriminellen zu keinem Zeitpunkt Zugriff auf das Mail-Konto.

- **Pornoseiten-Trick:** In diesem Fall wird in den Mails behauptet, man habe Beweise für den Besuch pornografischer Webseiten und wolle diese Bekannten und Verwandten zukommen lassen. Dabei setzen die Täter auf das Zufallsprinzip. Da Pornoseiten zu den am häufigsten besuchten Webseiten im Netz gehören, ist die Wahrscheinlichkeit hoch, jemanden anzuschreiben, der tatsächlich mehr oder weniger oft solche Seiten aufruft. Die behaupteten Beweise existieren aber natürlich gar nicht.
- **Webcam-Trick:** Es kann auch sein, dass die Kriminellen behaupten, Zugriff auf die eigene Webcam zu haben und insbesondere auch intime Bilder gesammelt zu haben. Auch hier wird mit einer Weitergabe gedroht. Ein Webcam-Zugriff ist laut LKA nicht völlig abwegig, solche Fälle habe es schon gegeben, etwa wenn der Rechner mit Schadsoftware befallen ist. Im Kontext der Erpressermail-Welle halten die Ermittler die Drohungen aber für frei erfunden. Es seien keine Fälle bekannt, in denen die Erpresser "Beweisbilder" mitgeschickt hätten.

Bei allen Maschen, egal ob allein oder in Kombination, verlangen die Kriminellen eine bestimmte Summe, etwa per Kryptowährung, damit sie kein vermeintlich kompromittierendes Material weitergeben oder damit sie ihre vermeintliche Überwachung einstellen.

- **Wichtiger Tipp:** Das LKA rät unbedingt dazu, jedwede Erpressung bei einer Polizeidienststelle vor Ort oder bei der Onlinewache der zuständigen Landespolizei anzuzeigen und keinesfalls auf Geldforderungen einzugehen. Ebenso warnen die Ermittler davor, den Erpressern zu antworten: Im schlimmsten Fall könnten Kriminelle diese Mails gegen den Absender oder die Absenderin einsetzen.

Proaktiv können Nutzerinnen und Nutzer zudem regelmäßig prüfen, ob die von ihnen für Log-ins genutzten E-Mail-Adressen und Passwörter vielleicht Hackerangriffen oder Datenlecks zum Opfer gefallen und im Netz auffindbar sind. Und zwar mit Hilfe des Identity Leak Checkers des Hasso-Plattner-Instituts oder auf der Seite Haveibeenpwned.com. Denn dort werde solche Datensätze gesammelt.

Kriminelle fordern per Mail Zollgebühren für Paket

Update vom 20. Juni: Wer dieser Tage eine Mail erhält mit der Aufforderung, eine Zollgebühr per Paysafecard zu zahlen, kann diese getrost ignorieren. Es handelt sich um Betrugsversuche. Eine Forderung auf diesem Wege und dann noch über einen Prepaid-Bezahldienst sei untypisch für Behörden, warnt das Verbraucherschutzportal "Watchlist Internet". Derzeit häuften sich solche Betrugsfälle.

- **Die Zoll-Masche funktioniert so:** In der Mail heißt es, ein Paket könne erst zugestellt werden, wenn man eine Zollgebühr beglichen habe, etwa in Höhe von 50 oder 75 Euro, und zwar per Paysafecard. Man soll bei dem Bezahldienst einen Guthaben-PIN-Code im Wert der geforderten vermeintlichen Gebühr kaufen.

Wer darauf eingeht und den Betrügern den PIN-Code übermittelt, sieht sein Guthaben meist nicht wieder. Mit dem Code können die Kriminellen sofort frei über den jeweiligen Betrag verfügen und damit im Netz bezahlen oder sich das Guthaben auszahlen lassen.

Falls man in die Falle getappt ist, sollte man sofort versuchen, den PIN-Code sperren zu lassen. Das ist über ein Online-Formular des Bezahldienstes möglich. Den Verbraucherschützern zufolge benutzen die Zoll-Betrüger als Absender derzeit häufig die

Fantasie-Mailadressen "noreply@zoll-post.de" oder "Zoll-Paket-Dienste@Osterreichischer-Zoll.at".

Phishing-Betrüger auf Paypal-Raubzug

Update vom 3. Juni: Mit meinem Paypal-Konto ist auf einer Glücksspiel-Seite bezahlt worden? Aber die Zahlung lässt sich noch stoppen, wenn ich mich jetzt gleich hier über diesen Link bei meinem Paypal-Konto anmelde! So ein Glück, möchte man meinen - wenn die Mail nicht gefälscht wäre.

Wer aktuell so eine oder ähnliche E-Mails erhält, dürfe keinesfalls auf Links darin klicken, warnt das Verbraucherschutzportal "Watchlist Internet". Hinter der Nachricht steckten Kriminelle, die versuchten, Nutzerinnen und Nutzern ihre Zugangsdaten zum Paypal-Konto sowie ihre Kreditkartendaten abzujagen. Dazu werden die Opfer auf eine gefälschte Paypal-Seite geleitet, die bei genauem Hinsehen an ihrer seltsamen Internetadresse zu erkennen ist. So verhalten Sie sich richtig:

- Generell: Wer sich bei Nachrichten, die Kontosperrungen oder dubiose Transaktionen suggerieren, unsicher ist, sollte sich einfach in Ruhe auf gewohntem Wege beim betreffenden Konto anmelden und nachsehen. So lässt sich schnell klären, dass die Behauptungen aus E-Mails frei erfunden sind.
- Wer auf die Betrüger hereingefallen ist und auf den Phishing-Seiten seine Daten preisgegeben hat, sollte direkt das Paypal-Passwort ändern und seine Bank wegen der Kreditkarte informieren.
- Bei etwaigen bereits abgebuchten Beträgen, sollte man versuchen, diese von der Bank zurückholen zu lassen. Lässt sich entstandener finanzieller Schaden nicht rückgängig machen, bleibt nur eine Anzeige bei der Polizei.

Keine fremden Nummern bei WhatsApp anrufen

Update vom 2. Juni: Wer beim Messengerdienst WhatsApp Nachrichten erhält, die dazu auffordern, eine spezielle Nummer anzurufen, sollte vorsichtig sein, warnt Computer Bild. Erkennen ließen sich die betrügerischen Rufnummern an einer Ziffernfolge, die mit einem Sternchen angegeben werden, warnt das Fachmagazin. Für Deutschland lautet die Kombination **21*, in bisherigen Fällen - vor allem in Indien - waren der Rufnummer **67* oder *405* vorangestellt.

Bei den zunächst harmlos erscheinenden Zeichen handelt es sich aber um einen sogenannten GSM-Code, der als Steuerbefehl für Smartphones dient. Damit können Betrüger Rufumleitungen und Rufsperren einrichten - und letztlich alle Anrufe auf die Geräte der Betrüger umleiten.

Laut Computer Bild übernehmen nach einem Anruf bei dieser Nummer Kriminelle die WhatsApp-Accounts ihrer Opfer und hinterlegen ihr eigenes Smartphone als neues Gerät. Da sich ein neues Gerät bei WhatsApp meist durch einen Kontrollanruf bestätigen lasse, sei die Verifizierung mittels Rufumleitung kein Problem. Das Fachmagazin warnt, dass Betrüger sich als Nutzer des Accounts legitimieren und womöglich auch die Rufnummern ändern und so volle Kontrolle über das Konto erlangen können.

Das bedeutet: Es wird schwer, sich den eigenen Account wieder zurückzuholen, da Betrüger sich nun einloggen können. Das Fachmagazin mahnt, dass Betrüger den Umstand nutzen und im Namen der Opfer Nachrichten an die eigenen Kontakte verschicken oder die manipulierte Rufnummer weiter verbreiten, um andere Accounts zu übernehmen.

DRV warnt vor neuer Betrugsmasche per Anruf

Update vom 20. Mai: Die Deutsche Rentenversicherung (DRV) warnt vor einer neuen Masche am Telefon, bei der eine Bandansage einer angeblichen Strafverfolgungsbehörde abgespielt wird. Darin heißt es, dass die Sperrung der Sozialversicherungsnummer drohe.

"So kontaktieren wir unsere Kundinnen und Kunden nie", betonte eine Sprecherin der DRV. Im Falle eines solchen Anrufs sollte man sich nicht zu einem persönlichen Ansprechpartner verbinden lassen. Es sei ausgeschlossen, dass die Sozialversicherungsnummer oder gespeicherte Daten zum Rentenkonto aufgrund einer telefonischen Ansage gesperrt oder gar gelöscht werden, warnt die DRV weiter. Genauso unwahrscheinlich sei die Forderung nach sofortigen Überweisungen von Geldbeträgen. Auf keinen Fall sollten persönliche Informationen wie Kontodaten preisgegeben werden.

Phishing-Seite greift wohl Kreditkartendaten ab

Update vom 6. Mai: Betrüger versuchen derzeit, mit Fake-Profilen und Links zu falschen Bezahlseiten die Kunden der Mitfahr-App BlaBlaCar übers Ohr zu hauen und an die Kreditkartendaten der Nutzer zu gelangen. Davor warnt das österreichische Verbraucherschutzportal "Watchlist Internet".

Wer bei den Betrügern eine Mitfahrgelegenheit über die Plattform bucht, wird via Messenger-Dienst kontaktiert und per Link auf eine betrügerische Zahlungsplattform gelockt. Schon im Voraus sollen die User dann einen geringen Betrag an eine angebliche "BlaBlaCar-Kommission" zahlen. Da die Website so wirke, als würde sie zu BlaBlaCar gehören, sei der Betrug für viele Nutzer nicht sofort erkennbar, berichtet "Watchlist Internet". Auch die Internetadresse der betrügerischen Website gleiche der echten. "Watchlist Internet" geht davon aus, dass die Betrüger hierüber Kreditkartendaten erbeuten möchten, etwa um die Opfer anschließend zur Freigabe von Zahlungen zu drängen.

Wer sich schützen möchte, sollte vor allem bei neuen Anbietern auf der Plattform vorsichtig sein, die nur wenige Bewertungen haben, gleichzeitig aber sehr viele Fahrten anbieten - oft mehrmals täglich hin- und zurück. Und vor allem: nie auf Links klicken, die von vermeintlichen Fahrern geschickt werden. Nutzer, die ihre Mitfahrgelegenheit bezahlen möchten, sollten stattdessen immer direkt auf die App oder Plattform gehen oder bei Abfahrt im Auto in bar bezahlen.

Polizei warnt vor "Enkeltrick" per WhatsApp

Update vom 28. März: Die Polizei warnt: Derzeit häufen sich Fälle einer neuen Variante des sogenannten Enkeltricks - und zwar nicht wie bisher vor allem üblich über Telefonate, sondern über WhatsApp. Zielgruppe der Kriminellen ist auch nicht mehr nur Großeltern-Generation. In den vergangenen drei Monaten seien Betrüger in rund mehr als einem Drittel der gemeldeten Fälle erfolgreich gewesen, teilt das Landeskriminalamt(LKA) Schleswig-Holstein mit. Der Schaden insgesamt: mehr als 113.000 Euro. "Wir gehen von einer hohen Dunkelziffer aus, da viele Betrugsversuche vermutlich gar nicht angezeigt werden", sagte eine LKA-Sprecherin.

Die Betrüger geben sich als Angehörige aus und teilen per WhatsApp-Nachricht von einer unbekannten Nummer mit, dass ihr Smartphone defekt oder verloren sei und sie dringend Geld benötigten. Eine Notlage wird vorgetäuscht, dringend müsse eine Rechnung bezahlt werden, heißt es etwa, oder es gebe Probleme beim Online-Banking. Häufig werden mehrere Tausend Euro gefordert, typischerweise "aufgrund der zeitlichen Dringlichkeit" per Echtzeitüberweisung. "Damit ist das Geld verloren und eine spätere Rückholung aussichtslos", sagte die LKA-Sprecherin.

Die Opfer werden meist aufgefordert, die vermeintlich nicht mehr gültige Telefonnummer gleich zu löschen. Damit wollen die Betrüger verhindern, dass die Geschädigten Kontakt zu ihren

Familienangehörigen aufnehmen, um die Behauptungen zu überprüfen. "Das sollte man auf keinen Fall tun", warnte die Sprecherin. Das LKA warnt davor, auf anonym versandte Geldforderungen angeblicher Verwandter per Messenger-Dienst einzugehen. "Die einfachste Methode, die Echtheit des Kontakts zu überprüfen, ist ein Telefonat oder ein persönliches Gespräch mit der genannten Person", sagt sie.

Kreditkartendaten-Klau bei Kleinanzeigen-Deals

Update vom 22. Februar: Verkäufer auf Kleinanzeigenportalen müssen derzeit verstärkt mit Kreditkarten-Betrugsversuchen rechnen. Bei einer aktuellen Masche, vor der das Landeskriminalamt (LKA) Niedersachsen warnt, meldet sich der vermeintliche Käufer eines Artikels und behauptet, dass der Bezahlvorgang fehlgeschlagen sei.

Kurz darauf kommt eine Nachricht, die angeblich vom Kleinanzeigenportal stammt. Darin heißt es, man solle einen Link öffnen und seine Kreditkartendaten samt Kontrollziffer eingeben - angeblich, um das Bezahlproblem zu lösen. Tatsächlich werden die Daten von den Betrügern abgegriffen.

Zur Ablenkung starteten die Kriminellen teils sogar gleichzeitig einen Chat, in dem man dann mitunter auch noch einmal aufgefordert wird, seine Kreditkartendaten anzugeben. Die angeblichen Mitarbeiter des Kleinanzeigenportals sind Betrüger und gehen am Ende mit den gestohlenen Kreditkartendaten in Fremdwährungen einkaufen.

Das LKA rät Betrugsopfern:

- Sofort die eigene Bank kontaktieren und die Zahlungen nach Möglichkeit noch stoppen.
- Auch kann es sinnvoll sein, die Karte zu sperren.
- Falls Sie den Betrügern Zugangsdaten für das Kleinanzeigenportal mitgeteilt haben, sollten Sie diese schnellstens ändern.
- Zusätzlich informiert man den Support des Portals und erstattet am besten auch Anzeige bei der örtlichen Polizei.

Noch eine Masche, die Ebay-Kleinanzeigen-Kunden trifft

Update vom 22. Februar: Von einer weiteren Betrugsmasche berichtet das IT-Fachportal "Heise.de". Demnach gibt ein scheinbarer Käufer vor, auf dem Portal Ebay Kleinanzeigen die Funktion "Sicher bezahlen" nutzen zu wollen. Auch hier entlocken die Betrüger den Verkäufern Kreditkartendaten oder Angaben zum Kontostand. Am Ende buchen sie dann vom Konto des Verkäufers Geld ab, statt den Kaufpreis zu überweisen.

Die Polizei Berlin weist darauf hin, dass Verkäufer auf Plattformen wie Ebay Kleinanzeigen nie zur Eingabe von Kreditkartendaten sowie Bank- oder Kontodetails aufgefordert werden. "Sicher bezahlen" werde ausschließlich auf der Webseite des Kleinanzeigenmarktes abgewickelt.

- **So funktioniert "Sicher bezahlen":** Wählen Käufer die treuhänderische Bezahlfunktion "Sicher bezahlen", müssen sie den Kaufpreis an den mit Ebay-Kleinanzeigen kooperierenden Dienstleister Online Payment Plattform (OPP) überweisen. Der verwahrt das Geld, bis der Käufer die Ware erhalten und dies bestätigt hat. Erst dann erhält der Verkäufer das Geld. Für diesen Service zahlen Käufer eine geringe Gebühr. Kommt die Ware nicht an oder weicht der Artikel von der Beschreibung ab, zahlt OPP dem Käufer den Kaufpreis zurück. Das Entgelt entfällt dann.

Webseiten verbreiten Schadsoftware

Update vom 9. Februar: Die Domain einer Webseite heißt exakt so, wie die Software, die man sucht, und hat eine DE-Endung. Was soll da schiefgehen? Eine ganze Menge. Immer

wieder registrieren Betrüger solche Domains, um arglose Nutzerinnen und Nutzer in die Falle zu locken. Wer Windows-Software von solchen Seiten installiert, holt sich also Schadsoftware auf den Rechner.

Zwei aktuelle Beispiele betreffen den freien Audio-Editor Audacity und den freien Passwortmanager Keepass. Die offiziellen Projektseiten lauten "Audacityteam.org" und "Keepass.info". Wer hingegen "Audacity.de" oder "Keepass.de" aufruft, landet auf Seiten, die den Anschein erwecken, die gesuchte Software anzubieten, aber Schadsoftware verbreiten. Davor warnt der IT-Sicherheitsforscher Mike Kuketz in seinem Blog.

Das können Sie tun, wenn Sie Zweifel bezüglich der Sicherheit von heruntergeladener Software haben:

- Laden Sie sie etwa auf der Seite "Virustotal.com" hoch. Dort können Sie sie von mehr als 70 Antivirenprogrammen gleichzeitig prüfen lassen - natürlich vor einer Installation.

Noch besser ist es aber, von Anfang an die richtige, offizielle Seite eines Softwareprojektes anzusteuern:

Hier empfehlen Experten Wikipedia als Anhaltspunkt: Bei Software werden die offiziellen Seiten von Unternehmen oder Projekten immer ganz unten im Infokasten auf der rechten Seite angezeigt. Auch verlässliche Downloadportale können gute Software-Quellen sein, etwa das Angebot des Heise-Verlags.

E-Mail von einer Polizeibehörde? Vorsicht!

Update vom 14. Januar: Interpol, Europol, Europäisches Polizeiamt oder auch Bundespolizei: Für eine Phishing-Kampagne missbrauchen Cyberkriminelle derzeit die Namen zahlreicher Polizeibehörden. In den E-Mails versuchen sie, den Empfängerinnen und Empfängern glauben zu machen, dass sie eine wichtige, dringende Vorladung erhalten hätten, auf die sie nun reagieren müssten.

Wer so eine Mail erhält, sollte keine Anhänge öffnen, warnt das Landeskriminalamt (LKA) Niedersachsen. Keine Links anklicken und keinesfalls antworten, um geforderte persönliche Informationen oder gar Ausweiskopien zu übermitteln.

- **Wichtig:** Behörden laden meist postalisch zu Anhörungen vor, manchmal auch persönlich, aber niemals per E-Mail. Die in den Mails vorgeworfenen Straftaten sind dem LKA zufolge natürlich frei erfunden - ebenso die Drohung, Freunde oder Familie über die "Tat" zu informieren, wenn man nicht antwortet.

Wer den Kriminellen trotzdem bereits geantwortet hat oder ihnen Daten und Dokumente übermittelt haben sollte, informiert man den Angaben zufolge am besten seine örtliche Polizeidienststelle und erstattet gegebenenfalls Anzeige.

Wer sich von den Mails nicht gleich überrumpeln lässt und sich die Nachrichten nur etwas genauer anschaut, wird aber gleich feststellen, dass da Betrüger am Werk waren: Behördennamen, Logos, Stempel, Unterschriften und Namen werden laut LKA gefühlt wahllos vermischt oder frei erfunden. Zudem sei die Schreibweise alles andere als fehlerfrei.

Regelmäßig wiederkehrende Betrugsmaschen

Falsche Microsoft-Anrufe

Es ist eine Masche, die seit Jahren ein "Dauerbrenner" ist: Anrufe von angeblichen IT-Firmen. Der Betrug ist vielen unter dem Schlagwort "Microsoft-Anrufer" bekannt. Die Anrufer wollen mit erfundenen Geschichten etwa über einen virenverseuchten PC ihres Opfers Geld und Daten ergaunern.

So gehen die Betrüger vor:

- Die Anrufer geben sich als Mitarbeiter von IT-Firmen wie Microsoft aus und melden sich mit Worten wie "Hallo, ihr Rechner ist von Viren befallen".
- Dann fordern sie dazu auf, einen Code einzugeben, ein Programm herunterzuladen oder Daten herauszugeben.

Gegen Zahlung wird Hilfe beim Entfernen der vermeintlichen Schadsoftware angeboten. Mit Software und Fernzugriff lassen sich die Täter auf den Rechner des Opfers schalten. Dort spähen sie Daten wie Online-Banking-Zugänge und Kreditkarteninformationen aus. Oft erfolgen die Anrufe auf Englisch oder in gebrochenem Deutsch.

Tipps der Polizei:

- Legen Sie im Fall eines solchen Anrufs sofort auf und melden Sie die Nummer des Anrufers der Polizei oder Bundesnetzagentur.
- Geben Sie auf keinen Fall private Daten - etwa Bankkonto- oder Kreditkartendaten, oder Zugangsdaten zu Kundenkonten wie PayPal - heraus.
- Erlauben Sie einem unbekannten Anrufer nie Zugriff auf Ihren Rechner.

Ohne Auftrag rufen Computerfirmen nie an, betonen die Verbraucherschützer. Selbst offizielle Hilfe nach Support-Anfragen erfolge fast immer per E-Mail.

Wenn Sie Opfer wurden:

- Trennen Sie Ihren Rechner vom Internet und fahren Sie ihn herunter. Über einen nicht infizierten Rechner sollten Sie unverzüglich Ihre Passwörter ändern.
- Lassen Sie Ihren Rechner überprüfen und das Fernwartungsprogramm auf Ihrem Rechner löschen.
- Über dieses Formular können Sie einen Tech-Support-Scam direkt bei Microsoft melden.
- Nehmen Sie Kontakt zu den Zahlungsdiensten und Unternehmen auf, deren Zugangsdaten in den Besitz der Täter gelangt sind.
- Lassen Sie sich von Ihrem Geldinstitut beraten, ob Sie bereits getätigte Zahlungen zurückholen können.
- Melden Sie sich bei der Polizei, etwa bei der Internetwache des jeweiligen Bundeslandes.

Der falsche Polizeibeamte

Sich auszugeben als jemand, der sie nicht sind, ist die typische Masche bei Betrug: "Wenn es um die momentan häufigsten Betrugsarten geht, wäre der 'falsche Polizeibeamte' zu nennen", heißt es dazu von der Polizeiliche Kriminalprävention auf Anfrage unserer Redaktion. Die Zahl der Delikte habe so zugenommen, dass der "falsche Polizeibeamte" inzwischen gesondert in die Polizeiliche Kriminalstatistik des BKA aufgenommen wurde. Die Schadenssummen seien häufig beträchtlich.

So funktioniert der Trick: Betrüger geben sich als Polizeibeamte aus, um das Vertrauen ihres Gegenübers - meist ältere Menschen - zu gewinnen. Sie manipulieren ihre Opfer so gekonnt, dass diese freiwillig hohe Geldbeträge oder Wertsachen übergeben. Die Täter erreichen das, indem sie von erfundenen Einbrecherbanden erzählen und so Angst und Verunsicherung erzeugen. Schließlich täuschen sie vor, das Hab und Gut ihrer Opfer vor Einbrechern in Sicherheit bringen zu wollen - und nehmen es mit.

Warnung: "Die Polizei fordert Bürgerinnen und Bürger niemals dazu auf, Geld oder Wertsachen an Beamte zu übergeben. Nur Betrüger wollen an Ihre Wertgegenstände", betont Gerhard Klotter, Vorsitzender der Polizeilichen Kriminalprävention der Länder und des Bundes.

Tipps der Polizei:

- Lassen Sie niemals Unbekannte in Ihre Wohnung.
- Lassen Sie sich nicht unter Druck setzen und übergeben Sie niemals Geld an fremde Personen.
- Verlangen Sie von angeblichen Amtspersonen grundsätzlich den Dienstausweis und prüfen Sie ihn sorgfältig auf Druck, Foto und Stempel. Rufen Sie im Zweifel die entsprechende Behörde an. Die entsprechende Telefonnummer sollten Sie selbst heraussuchen, nicht vom Unbekannten verlangen.
- Stellen Sie keine Wertgegenstände zur Abholung vor die Tür.
- Rufen Sie im Zweifelsfall 110 oder bei Ihrer Polizeidienststelle vor Ort an.
- Wurden Sie zum Opfer, wenden Sie sich sofort an die Polizei und erstatten Sie Anzeige.

Varianten des Haustürbetrugs

Neben dem Beamten geben sich Betrüger sehr häufig auch als Hilfsbedürftige, Handwerker oder Mitarbeiter der Stadtwerke aus oder treten als seriös gekleideter Geschäftsmann auf.

So funktioniert der Trick: Mit schauspielerischem Geschick überrumpeln die Täter ihre Opfer und verschaffen sich unter einem Vorwand Zutritt zu deren Wohnung: Sie bitten um ein Glas Wasser, etwas zum Schreiben oder fragen, ob sie die Toilette benutzen dürften. Als Handwerker verkleidet weisen sie auf einen vermeintlichen Wasserrohrbruch hin, der schnell behoben werden müsse.

Tatsächlich gelingt es laut Polizei auf diese Weise leider oft, dass eine zweite Person unbemerkt in die Wohnung eindringt und nach Wertsachen sucht.

Die schriftliche Variante: Die Täter werfen Benachrichtigungen in den Briefkasten, die mit den Namen der Opfer ausgefüllt sind. Darin heißt es, dass "niemand angetroffen" wurde und man sich bitte "zur Vereinbarung eines Gesprächstermins in Ihrer Angelegenheit“ oder "zur Abholung Ihres Pakets" telefonisch melden möge. Beim angegebenen Telefonkontakt handelt es sich dann um eine kostenintensive Telefonnummer.

Tipps der Polizei:

- Öffnen Sie Unbekannten die Tür höchstens bei vorgelegtem Sperrriegel.
- Bestellen Sie Unbekannte für später ein, wenn eine Vertrauensperson anwesend ist.
- Wehren Sie sich energisch gegen zudringliche Besucher, sprechen Sie sie laut an oder rufen Sie um Hilfe.

Geschäfte an der Haustür

Ein "einmaliges Schnäppchen", ein "Gratisangebot": Bei diesen Worten sollte jeder hellhörig werden. Ebenso, wenn es um Handwerksleistungen geht, die an der Haustür angeboten werden, oder der Unbekannte behauptet, für ein soziales Projekt zu arbeiten.

So funktioniert der Trick: Mit unterschiedlichen Maschen - indem sie entweder mit Gewinnen locken oder das Mitgefühl der Opfer wecken - **besorgt sich der Täter die Unterschrift des Opfers.** Letztlich handelt es sich aber um einen Vertrag - für eine Versicherung, ein Abo oder sonstiges - den das Opfer unterschrieben hat.

Bietet der Betrüger eine Handwerksleistung an, beginnt er diese zur Täuschung, beendet sie dann aber nicht. Der Auftraggeber aber wird zur Kasse gebeten.

Tipps der Polizei:

- Kaufen oder unterschreiben Sie niemals etwas an der Haustür. Angebote Produkte - Teppiche, Besteck, Schmuck - oder Handwerkerleistungen sind meist wertlos.

- Lassen Sie nur Handwerker in Ihre Wohnung, die Sie selbst bestellt haben oder die von der Hausverwaltung angekündigt worden sind. Das gleiche gilt für vermeintliche Vertreter der Stadtwerke.
- Nehmen Sie für Nachbarn nichts ohne deren Ankündigung entgegen, etwa Nachnahmesendungen oder Lieferungen gegen Zahlung.
- Geben Sie keine Unterschrift für angebliche Geschenke oder Besuchsbestätigungen.
- Banken, Sparkassen, Polizei oder andere Behörden schicken nie "Geldwechsler" oder "Falschgeld-Prüfer" an die Haustür. Informieren Sie umgehend die Polizei, wenn derartige Unbekannte bei Ihnen auftauchen.
- Wechseln Sie niemals Geld an der Haustür. Es könnte sich um Falschgeld handeln.

Falsche Mails: Beispiele Amazon und Netflix

Zu den häufigsten Betrugsmaschen gehören auch falsche Emails, die angeblich von Behörden, der Bank oder bekannten Unternehmen stammen. Dieses Jahr kursieren beispielsweise falsche Amazon- und Netflix-Mails.

So funktioniert der Trick: Die Kriminellen locken ihre Opfer auf gefälschte Seiten, damit diese dort ihre Daten - inklusive Bankdaten - eingeben. Im Fall von Netflix wird den Usern per Mail vorgegaukelt, ihr Konto werde in 48 Stunden auslaufen - wenn sie nicht online ihre Daten aktualisieren. Ein Link führt zu einer gefälschten Website, wo die Kunden ihre Logindaten und Bezahlinformationen eingeben sollen.

Im Fall Amazon erhielten die User eine angebliche Bestellbestätigung, was zu Verunsicherung führt, denn die angebliche Bestellung wurde nie durchgeführt. Das Ziel der Betrüger: Der irritierte User öffnet den Anhang, gelangt über einen Link auf die Fake-Seite und gibt seine Daten ein.

In beiden Fällen handelt es sich um den Phishing-Trick: Die Kriminellen greifen die Anmeldedaten der Nutzer sowie Zahlungsdaten und Adressen ab.

Tipps der Polizei:

- Niemals Links oder Anhänge in verdächtigen Emails öffnen.
- Wer Opfer geworden ist, sollte unverzüglich die echten Amazon- oder Netflix-Webseiten aufrufen, sich dort einloggen und seine Zugangsdaten ändern.
- Nehmen Sie Kontakt mit dem Support des Unternehmens auf.
- Unbedingt sollten Betroffene sofort die Bank informieren, zu der die Zahlungsdaten gehören, die auf der Phishing-Seite preisgegeben wurden.

"Romance Scamming" oder "Loverboy"-Masche

Immer häufiger wird auch vor der "Loverboy"-Masche gewarnt, auch bekannt als "Romance Scamming": Kriminelle erschleichen sich in den sozialen Medien oder beim Online-Dating das Vertrauen ihrer Opfer und bringen sie im schlimmsten Fall um sehr viel Geld. Wie Sie die "Loverboy"-Betrüger erkennen, lesen Sie hier. Das rät die Polizei im Verdachtsfall:

Geben Sie den Namen Ihrer Bekanntschaft mit dem Zusatz "Scammer" oder "Loverboy" in eine Suchmaschine ein - oft ließe sich der Verdacht dadurch schon bestätigen.

- Falls ein Bild mitgeschickt wurde, lassen sich anhand der umgekehrten Bildersuche zusätzliche Informationen zu dem Bild erhalten.
- Anfragen ignorieren, Person blockieren.
- Hilfe holen, etwa bei der Polizei.
- Beweise sichern, etwa durch Screenshots.

Trickbetrüger tarnen sich als Rentenversicherung oder Energieanbieter

Diese immer wiederkehrende Masche besteht aus einem täuschend echt wirkenden Brief, einem unangekündigten Besuch zu Hause oder einem unerwarteten Telefonat: Getarnt als angebliche Mitarbeitende der Rentenversicherung versuchen Betrüger, an persönliche Daten oder sogar an die Bankverbindung von Versicherten heranzukommen.

Die typische Masche:

- Rentnerinnen und Rentner werden von Anrufern aufgefordert, Geld auf ein fremdes Konto zu überweisen. Es wird den Angerufenen mit angeblichen Rentenpfändungen, Rentenkürzungen oder anderen Nachteilen gedroht, wenn die Zahlung verweigert wird.
- Auch telefonische Angebote, Medikamente oder medizinische Hilfsmittel zu verkaufen, stammen nicht von der Deutschen Rentenversicherung.

In keinem Fall sollten Betroffene aufgrund telefonischer Aufforderungen Geld ins In- oder Ausland überweisen.

Verbraucherschützer warnen zudem vor einer Masche unseriöser Energieanbieter: Sie rufen Verbraucher an und fragen am Telefon unter einem Vorwand nach dem aktuellen Zählerstand und der Zählernummer.

Geben Verbraucher diese Daten preis, leiten sie unter Umständen den Anbieterwechsel ein, ohne es zu wollen. Denn dem unseriösen Anbieter reichen diese Daten aus, um den Vertrag beim bisherigen Versorger zu kündigen.

- Tipp der Verbraucherzentrale Bremen: Legen Sie auf. Der derzeitige Energieanbieter würde sich schriftlich melden, wenn er den Zählerstand erfragen möchte, erklären die Experten. Grundsätzlich sollten am Telefon keine Daten durchgegeben werden - weder die Zählernummer noch der Name und die Anschrift.

Wer seine Daten einem unbekannten Anrufer genannt hat, sollte den untergeschobenen Vertrag schriftlich mit einem Einwurfeinschreiben innerhalb von 14 Tagen widerrufen.

Unerwünschte Anrufe & Co.: So legen Sie Beschwerde ein

Besteht der Verdacht eines Betrugs, wenden sich Bürgerinnen und Bürger am besten schnellstmöglich an die Polizei. Niemand muss es sich zudem gefallen lassen, unerwünschte automatisierte Anrufe zu erhalten, Fax-Spam oder Werbenachrichten über Messenger-Dienste: Solche Fälle können Verbraucher der Bundesnetzagentur melden. Auch etwa über hochpreisige Kundenhotlines können Sie sich dort beschweren.

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/aktuelle-betrugsmaschen-vorsicht-abholung-kurierdienste-34288658

5) Aufgedeckt: Die 12 fiesesten Online-Fallen

Cyberkriminelle erfinden immer raffiniertere Methoden, um ahnungslosen Internetnutzern das Geld aus der Tasche zu ziehen. Einfache Grundregeln können vor Onlinediebstahl schützen.

Gelegenheit macht Diebe. Im Zeitalter von Onlineshopping bieten sich Dieben zahlreiche Gelegenheiten, durch betrügerische Aktivitäten Kasse zu machen. Vor allem Verkäufe von privat zu privat auf Plattformen wie Ebay-Kleinanzeigen und Ähnlichen sind oftmals Zielscheibe der Gauner.

Das beste Gegenmittel besteht darin, genau zu verstehen, wie die Betrüger vorgehen. Wenn Sie die Fallen kennen, tappen Sie auch nicht hinein. Wenn Sie darüber hinaus noch ein paar Grundregeln beherzigen, dann kann Ihnen eigentlich nicht mehr viel passieren und Sie können beruhigt weiter einkaufen.

1. Dreiecksbetrug auf Ebay

Raffiniert und schwer zu erkennen: Beim Dreiecksbetrug erhält der Gauner einen Artikel, den Sie etwa bei Ebay- Kleinanzeigen anbieten, ohne einen Cent dafür zu bezahlen.

Ebay-Kleinanzeigen hat sich zur größten Plattform für private Verkäufe gemausert. Es gibt fast nichts, was sich dort nicht erwerben lässt. Das haben natürlich auch die Betrüger mitbekommen. Sie versuchen mit immer neuen Tricks, illegal an Geld oder Waren zu gelangen. Die neueste Masche ist der Dreiecksbetrug. Er ist ziemlich raffiniert und nicht leicht zu durchschauen.

So funktioniert der Betrug: Sie schalten eine Anzeige bei Ebay-Kleinanzeigen, zum Beispiel für einen hochpreisigen Elektronikartikel. Dann meldet sich der Betrüger als Interessent. Er will den Artikel aber nicht bar bezahlen, sondern über Paypal. Wenn Sie sich damit einverstanden erklären und die Paypal-Adresse angeben, dann folgt der eigentliche Dreh dieses Betrugs: Der Kriminelle schaltet selbst eine Anzeige mit einem identischen Verkaufswert. Sobald sich ein Käufer auf diese Fake-Anzeige meldet, gibt der Betrüger Ihre Paypal-Adresse an. Sie erhalten also Geld von einer unbekannten Person, der Sie gar nichts verkauft haben. Sie erkennen nichts Ungewöhnliches: Die mit dem Betrüger vereinbarte Summe ist schließlich auf Ihrem Konto gelandet, und Sie versenden den Artikel. Was Sie stutzig machen könnte: Die Versandadresse weicht von der Adresse ab, die Sie mit der Zahlungsbestätigung von Paypal erhalten haben. Vermutlich hat der Dieb Sie in der Zwischenzeit gebeten, die Ware an eine andere, abweichende Adresse oder an eine Packstation zu verschicken.

Auf der anderen Seite wartet die dritte Person, die das Geld für den Artikel, den der Betrüger eingestellt hat, auf Ihr Paypal-Konto überweisen hat, vergeblich auf die gekaufte Ware. Oft dauert es Tage, bis Opfer merken, dass sie auf einen Betrug hereingefallen sind und nicht etwa die Post die Ware verschludert hat. Die Person beschwert sich daraufhin bei Paypal. Die Folge: Der Bezahldienst zieht Ihr Geld ein und sperrt das Konto. Der Betrüger hat somit Ihren Artikel zum Nulltarif bekommen. Die dritte Person hat einigen Ärger am Hals und erhält den gekauften Artikel nicht, hat aber immerhin keinen finanziellen Schaden, da sie den Kaufbetrag über den Paypal-Käuferschutz wiedererhält.

So schützen Sie sich: Der Dreiecksbetrug ist schwer zu erkennen, da scheinbar ja alles mit rechten Dingen zugeht. Mit ein paar Verhaltensregeln bleiben Sie stets auf der sicheren Seite: Achten Sie unbedingt auf die korrekte Adresse in der Zahlungsbestätigung! Nur wenn die Versandadresse und die Adresse in der Paypal-Zahlung übereinstimmen, greift der Verkäuferschutz. Versenden Sie Ihre Ware möglichst per Einschreiben und niemals an Packstationen. Auf diese Weise erhalten Sie einen rechtsgültigen Nachweis. Am sichersten ist natürlich der Austausch Geld gegen Ware direkt an Ihrer Haustür.

Tipp: Online-Shopping: Was tun im Schadensfall?

2. Der Gutschein-Trick

Diese neue Betrugsmasche konzentriert sich ebenfalls weitgehend auf Ebay-Kleinanzeigen. Der Betrüger bietet dabei möglichst teure Güter wie Spielekonsolen oder Smartphones zum Verkauf an oder beantwortet entsprechende Suchanfragen. Wenn es dann zu einem Kontakt kommt mit einem potenziellen Käufer, dann drängt der Betrüger darauf, die weitere Kommunikation auf außerhalb von **Ebay** zu verlagern. Das geschieht aus dem einfachen Grund, dass die Sicherheitsmechanismen der Handelsplattform den Betrug sofort erkennen und Alarm schlagen würden.

Wenn der Kontakt dann extern weiterläuft, erhält der Käufer die Nachricht, doch bitte mit Gutscheinen zu bezahlen, etwa von Amazon oder der Spieleplattform Steam. Wenn der Käufer darauf eingeht und die Gutscheincodes verschickt, sieht er weder die gekaufte Ware noch den vermeintlichen Verkäufer jemals wieder. Der vergnügt sich mit den Gutscheinen und geht nach Herzenslust auf Einkaufstour.

Als Schutz genügt eine einfache Grundregel: Bezahlen Sie niemals mit Gutscheinen. Auch bei Bezahlung mit Paypal lauert noch ein weiterer Fallstrick. Wenn ein Verkäufer Sie drängt, doch bitte mit der Bezahlmöglichkeit „Freunde und Familie“ zu bezahlen, um die Gebühren zu sparen, dann sollten Sie dies ablehnen. Denn andernfalls erlischt Ihr Käuferschutz.

3. Paypal-Betrug

Diese Betrugsmasche betrifft wieder in erster Linie Ebay-Kleinanzeigen, aber auch andere Onlineshops. Sie ist nicht brandneu, aber erfolgreich. Das bestätigen immer wieder entsprechende Meldungen in den Medien und Klagen in Foren.

So funktioniert es: Sie bieten einen Artikel zum Verkauf an, und ein Interessent meldet sich. Dieser gibt an, per Paypal bezahlen zu wollen. Der Betrüger behauptet dann, dass Sie einen Code an ihn weiterleiten müssen, den Sie per SMS erhalten haben. Dadurch solle der Kauf durch den Paypal-Käuferschutz abgesichert sein. Das ist natürlich Humbug, klappt aber manchmal. Mit diesem Code ist es dem Betrüger dann möglich, virtuell zu bezahlen. Der dazugehörige Dienst nennt sich „PayPal Buy with Mobile“. Er ermöglicht es, etwa in sozialen Netzwerken oder Onlinespielen für virtuelle Güter per Smartphone zu bezahlen. Dafür muss man eine Telefonnummer angeben und die Bezahlung dann mit einem Sicherheitscode autorisieren, welcher an die entsprechende Nummer versendet wird. Der Betrüger behauptet also, dieser Code würde per SMS dem Verkäufer mitgeteilt und daraufhin müsse der Verkäufer dem Käufer den Code nennen. Zusammen mit Ihrer mobilen Telefonnummer, die normalerweise auf der Handelsplattform ersichtlich ist, kann der Betrüger dann munter auf Einkaufstour gehen.

4. Geklaute Identitäten

Deutlich einfacher ist eine andere Betrugsmasche: Ein Krimineller übernimmt das Konto eines Verkäufers auf **Ebay** Kleinanzeigen und profitiert auf diese Weise von dessen positiven

Bewertungen. So kann er nun Waren anbieten, die er nicht besitzt, und nach der Bezahlung einfach verschwinden. Die Zugangsdaten für das Kleinanzeigen-Konto verschafft er sich entweder durch Phishing, also über gefälschte E-Mails oder Webseiten, die den Kontobesitzer zur Eingabe seiner Daten auffordern. Oder er stößt in geleakten Passwortlisten auf die E-Mail-Adresse des Besitzers und stellt fest, dass dieser bei mehreren Diensten das immer gleiche Kennwort verwendet. Schließlich gibt es noch den Betrug mit den defekten Elektrogeräten: Der Kriminelle kauft einen Fernseher, bezahlt ihn und schickt dem Verkäufer nach dem Erhalt eine wütende Mail, dass das Gerät defekt sei. Er wolle den Kauf rückabwickeln, wozu er nach deutschem Recht auch berechtigt ist. Er bekommt sein Geld zurück, schickt aber anstatt des gelieferten, in Wahrheit völlig einwandfreien Geräts ein identisches, aber defektes Modell zurück.

5. Phishing von Kreditkartendaten

Bei einem anderen, weit verbreiteten Trick interessiert sich ein Käufer nur vorgeblich für eine Ware und nutzt die Onlineplattform lediglich für das Phishing von Kreditkartendaten. Zunächst vereinbart der angebliche Interessent mit dem Verkäufer die Nutzung der Funktion „Sicher bezahlen“, bei der die Bezahlung über Ebay Kleinanzeigen abgewickelt wird. Doch der Verkäufer wartet vergeblich auf den Eingang der Zahlung. Stattdessen erhält er nach einiger Zeit eine E-Mail von den Kriminellen, dass der Bezahlvorgang gescheitert sei.

Noch etwas später kommt eine weitere Mail, angeblich von Ebay Kleinanzeigen. In ihr wird der Verkäufer aufgefordert, dem Link auf eine Website zu folgen, wo der angeblich abgebrochene Bezahlvorgang in die Wege geleitet werden soll.

Auf dieser Seite, die tatsächlich von den Kriminellen aufgesetzt wurde, soll der Verkäufer seine Kreditkartendaten inklusive der CVC-Nummer auf der Rückseite der Karte eingeben. Teilweise existiert sogar eine Chat-Funktion, über welche die Betrüger dem Verkäufer den Vorgang erklären und etwaige Bedenken zerstreuen. Sobald die Kriminellen im Besitz der Kartendaten sind, verwenden sie sie sofort für umfangreiche Warenbestellungen. Falls die Bank, welche die Karte ausgestellt hat, eine zusätzliche Verifizierung verlangt, wird auch das dem Verkäufer im Chat plausibel gemacht. Anschließend brechen die Betrüger den Kauf sofort ab und sind nicht mehr erreichbar.

Beliebt ist auch der Trick mit den angeblichen Transportkosten. Der Betrüger bestellt eine große, schwere und auch teure Ware wie etwa ein Möbelstück. Für den Nachweis der Bezahlung schickt er dem Verkäufer eine gefälschte E-Mail von einer Bank oder einem Dienstleister wie Paypal. Er behauptet dann, er habe ein Transportunternehmen mit der Abholung beauftragt. Die Transportkosten von mehreren Hundert Euro soll der Verkäufer tragen. Um der Forderung mehr Nachdruck zu verleihen, droht ihm der Kriminelle vorsorglich mit einem Anwalt. Bezahlt der Verkäufer, ist der angebliche Kunde verschwunden. Bei kleinen, hochwertigen Waren wie Uhren oder Schmuck arbeiten die Kriminellen einfach nur mit gefälschten Zahlungsbestätigungen.

6. Anruf von Microsoft

Diese Betrugsmasche startet in der Regel telefonisch und verlagert sich später ins Internet. Hier geht es nicht direkt um Geld, sondern um einen Zugang zu Ihrem Rechner. Dort können dann zum Beispiel Passwörter und Zugangsdaten für Onlinebanking ausgespäht werden.

So geht der Betrüger vor: Sie erhalten einen Anruf von einer Person, die vorgibt, Mitarbeiter im Support von Microsoft oder einem anderen großen Software-Konzern zu sein. Er erzählt Ihnen, interne Messungen hätten ergeben, dass mit der Netzwerkverbindung etwas nicht stimme oder man habe einen kritischen Fehler entdeckt und wolle nun helfen, das Problem zu beseitigen. Das klingt hilfreich, ist es aber nicht. Es folgt eine Anleitung, wie Sie ein Remote-

Desktop-Programm herunterladen und installieren, damit der Mitarbeiter aus der Ferne Ihren PC reparieren kann. Damit geben Sie dem Betrüger aber die volle Kontrolle über den Rechner in die Hand. Er hat fortan Zugriff auf alle Dateien und persönliche Informationen, inklusive Passwörter und Zugangsdaten. Hier hilft die strikte Grundregel: Gewähren Sie niemandem einen Remote-Zugriff auf Ihren Rechner.

7. Gefälschte Trading-Plattformen

Die Süddeutsche Zeitung beschreibt in einem Artikel einen noch recht neuen Trend: Massenhaft ausgesendete E-Mails und Meldungen in den sozialen Medien behaupten, dass Prominente wie Dietrich Mateschitz oder Lena Meyer-Landrut von einem geheimen System neuartiger Geldanlagen im Internet profitieren. Oder: Eine Startup-Firma habe einen neuen Algorithmus für die Geldanlage im Internet entwickelt, der Tausende Euro Gewinn garantiere. Auch Medien wie ZDF, N24, Spiegel oder Bild hätten bereits darüber berichtet, dazu werden die Logos dieser Medien eingeblendet.

In beiden Fällen führt ein Link zu einer Website, auf der die Besucher in das neue System investieren können. Bereits mit einem dreistelligen Betrag sind sie dabei. Die Tabellen auf der Site melden denn auch nach kurzer Zeit bereits stattliche Gewinne. Angebliche Broker melden sich per Telefon und fragen, ob man nicht noch ein wenig mehr investieren wolle, um den Gewinn noch zu erhöhen. Alles läuft gut – bis der Anleger sich die Gewinne auszahlen lassen möchte. Dann ist plötzlich niemand mehr erreichbar. Denn die angeblichen Geldanlagen existieren nicht, die Website mit ihren Auswertungen ist nur ein Bluff.

8. Fake-Shops

Unter **www.watchlist-internet.at** finden Sie Listen von unseriösen Onlineshops, Streaming-Anbietern, Handwerksbetrieben etc. Falls Ihnen eine Firma verdächtig vorkommt, können Sie deren Adresse dort abgleichen. Quelle: www.pcwelt.de

Wenn Sie bei einem Onlineshop bestellen, die Ware nie eintrifft, der Rechnungsbetrag allerdings von Ihrer Kreditkarte abgebucht wird, dann sind Sie vermutlich einem Fake-Shop aufgesessen. Die Betreiber dieser Seiten kopieren häufig seriöse Onlineshops und treten unter einer nur leicht veränderten Adresse auf, die schnell verwechselt werden kann. Sie bieten die Waren allerdings zu einem deutlich günstigeren Preis an. Viele betreiben mittlerweile einen hohen Aufwand, um ihre Seiten seriös wirken zu lassen. Die Texte sind in gutem Deutsch und ohne Rechtschreibfehler, der Datenverkehr ist per https geschützt, es gibt

ein Impressum und sogar mehrere Gütesiegel. Dennoch werden Sie nach einer Überweisung an einen solchen Fake-Shop Ihr Geld bestenfalls per Anwalt wiedersehen.

9. Lukratives Stellenangebot

Diese Anzeige, die nach Produkttestern sucht, ist keineswegs von der Drogeriekette dm, sondern eine gemeine Fälschung, die Malware verbreitet. Quelle: www.pcwelt.de

Der Onlinetrick mit lukrativen „Stellenangeboten“ ist insbesondere auf Social-Networking-Plattformen wie Xing und Linkedin sowie Jobbörsen wie Stepstone verbreitet.

Eine recht neue Betrugsvariante geht so: Sie erhalten über eines der genannten Portale eine Mail mit einem Stellenangebot für eine Nebentätigkeit mit einem netten Zuverdienst. Die angebotene Stelle hat in der Regel nichts mit Ihrem tatsächlichen Beruf zu tun. Stattdessen handelt es sich um unspezifische Angebote wie Produkt- oder Apptester. Wenn Sie zusagen, die Stelle antreten und einen Lohn vereinbaren, dann erhalten Sie nach einiger Zeit einen Scheck mit einem Betrag, der höher ist als der vereinbarte. Der vermeintliche Auftraggeber verweist auf einen Fehler in der Buchhaltung und fordert die Rückzahlung des zu viel bezahlten Betrags. Wenn Sie die Differenz begleichen, dann stellen Sie später fest, dass der ursprüngliche Scheck gefälscht oder ungültig war, und Ihr Geld ist futsch. Um sicher zu gehen, warten Sie immer ab, bis das Geld tatsächlich auf Ihrem Konto gelandet ist. Eine alternative Variante lotst Sie zu manipulierten Webseiten, die mit Schadsoftware verseucht sind.

10. Vermeintlicher Lottogewinn

Nicht wirklich neu, aber immer wieder in Wellen auftretend und überraschend erfolgreich ist der Betrug mit einem vorgegaukelten Gewinn in einer Lotterie. Denn wer träumt nicht von einem solchen Gewinn? Wenn dann eine Mail eintrudelt, der zufolge der Glücksfall tatsächlich eingetreten ist, dann setzt der gesunde Menschenverstand mitunter aus. Meistens handelt es sich dabei um eine unbekannte Lotterie im Ausland. Um den Gewinn einzulösen, sollen Sie einen kleinen Geldbetrag überweisen.

Diese Betrugsmasche ist eigentlich leicht zu erkennen. Suchen Sie im Internet nach der vermeintlichen Lotteriegesellschaft und nehmen Sie direkt Kontakt auf.

11. Vorschuss-Betrug

Bestimmt haben Sie auch schon Mails bekommen von einem nigerianischen Geschäftsmann, der sein enormes Vermögen oder ein ausstehendes Erbe ins Ausland schaffen will. Wenn Sie ihm dabei helfen, erhalten Sie einen Prozentsatz des Vermögens. Die Hilfe besteht aus lauter

kleinen Zahlungen etwa für die Bestechung der Zollbeamten, Transaktionsgebühren oder die Gebühren für die Auflösung eines Fonds, um die Überweisung der Gelder zu ermöglichen. Das Ganze nennt sich dann üblicherweise Vorschuss-Betrug.

Auch im Internet gilt die Weisheit, was zu schön ist, um wahr zu sein, ist es nicht.

12. Verdächtige Whatsapp-Nachrichten

Auch Whatsapp wird von Betrügern als Werkzeug benutzt. Sie erhalten eine Nachricht, die Ihnen ein zusätzliches Freivolumen für Ihren Mobilvertrag verspricht, wenn Sie an einer Umfrage teilnehmen. Außerdem sollen Sie die Nachricht an 30 Ihrer Kontakte weiterleiten – das alte Kettenbrief-Prinzip. Der mitgeschickte Link führt Sie jedoch nur zu mehreren kommerziellen Websites. Denn den Absendern geht es allein darum, Klicks zu sammeln und die Einnahmen durch Werbung zu erhöhen.

Weniger harmlos ist dagegen der Enkel-Trick. Großmutter, Großvater oder auch ein Elternteil bekommt eine Nachricht von einer unbekannten Nummer. Der Absender gibt sich als Enkel oder Tochter aus und behauptet, er habe ein neues Smartphone, da das alte verlorengegangen sei – daher die neue Nummer. Häufig gehen nun ein paar Tage belanglose Nachrichten hin und her. Dann kommt der Hilferuf: Das angebliche Familienmitglied schreibt, es sei in Not und könne eine Rechnung nicht bezahlen. Es bittet daher um die schnelle Überweisung eines vierstelligen Betrags. Und auch für das Konto mit dem fremden Besitzer hat es eine Erklärung: Auf dem neuen Smartphone sei das Onlinebanking noch nicht eingerichtet oder die Bank habe den Zugang zum Konto gesperrt. Sobald das Geld überwiesen ist, bricht der Kontakt ab.

Geld zurück: So geht’s

Die Betrüger sind raffiniert, sodass jeder mal in die Falle tappen kann. Zum Glück gibt es Wege, das Geld zurückzuholen.

Das gilt für Überweisungen, Lastschriften und Zahlvorgängen mit Kreditkarte oder Bezahldiensten. Am einfachsten lässt sich eine Sepa-Lastschrift widerrufen. Sie können den entsprechenden Betrag innerhalb von acht Wochen ab dem Zeitpunkt der Abbuchung von der Bank zurückbuchen lassen. Eine Überweisung können Sie nicht mehr rückgängig gemacht machen, sobald Ihre Bank den Auftrag durchgeführt hat. Hier kommt es also darauf an, schnell zu reagieren. Manche Banken bieten im Onlinebanking eine Stornierungsfunktion, die für ein paar Minuten nach dem Abschicken aktiv ist. Andernfalls hilft ein schneller Anruf bei der Bank. Auch Kreditkartenzahlungen können Sie im sogenannten Charge- Back-Verfahren rückgängig machen. Normalerweise ist dafür aber eine Bearbeitungsgebühr fällig. Bei Internet-Bezahldiensten wie Paypal springt der Käuferschutz ein. Der ist aber an bestimmte Nutzungsbedingungen geknüpft. Bei Bargeldtransferdiensten wie Western Union ist ein Rückruf möglich, bis das Geld vom Empfänger abgeholt worden ist.

Die 10 wichtigsten Vorsichtsmaßnahmen gegen Abzocke

Viele betrügerische Websites sind für Laien kaum zu erkennen beziehungsweise schwer zu durchschauen – umso wichtiger ist es, sich mit einer Reihe von Maßnahmen zu schützen. Hier finden Sie die zehn wichtigsten Regeln zusammengefasst:

- Bezahlen Sie niemals per Vorauskasse. Greifen Sie auf die Dienste von Zahlungsdienstleistern wie Paypal zurück. Am besten ist der Kauf auf Rechnung nach Erhalt der Ware.
- Vereinbaren Sie bei Ebay Kleinanzeigen eine persönliche Übergabe und Barzahlung.
- Reagieren Sie nicht auf E-Mails, die Ihnen hohe Gewinne bei der Investition in neue

Geldanlage-Systeme oder angeblich revolutionäre neue Produkte versprechen.

- Werden Sie misstrauisch, wenn teure Markenartikel zu einem erheblich günstigeren Preis angeboten werden.
- Notieren Sie sich bei Rückrufen des Verkäufers die Telefonnummer.
- Überprüfen Sie bei unbekannten Shop-Sites, ob sie ihre AGB (Allgemeinen Geschäftsbedingungen) veröffentlichen und ein Impressum aufweisen. Falls eine Telefonnummer angegeben ist, rufen Sie dort an.
- Überprüfen Sie, ob die Domain-Adresse mit dem Namen des Shops übereinstimmt.
- Geben Sie die Handelsregisternummer bei www.handelsregister.de und die Umsatzsteuer-ID bei www.ust-id-pruefen.de ein.
- Überprüfen Sie eventuell vorhandene Gütesiegel, indem Sie auf den Seiten der Anbieter nachsehen, ob der Shop in deren Listen erscheint: EHI-Geprüfter Online Shop , Trusted Shops , safer-shopping , Internet Privacy Standards
- Falls Sie auf einen Betrug hereingefallen sind, kontaktieren Sie sofort Ihre Bank oder das Finanzinstitut, das Ihre Kreditkarte ausgestellt hat. Eventuell können Sie die Überweisung noch stornieren oder im Rahmen des Käuferschutzes eine Rückerstattung bekommen.

Hilfe von den Verbraucherzentralen

Bei Onlinebetrug stehen Ihnen die Verbraucherzentralen mit Rat und Tat zur Seite. In Deutschland sind die Verbraucherzentralen auf Landesebene organisierte gemeinnützige Vereine. Sie kümmern sich um den Verbraucherschutz und stehen in rund 200 Beratungsstellen zum persönlichen Gespräch bereit. Eine Karte mit den Beratungsstellen finden Sie auf der Webseite www.verbraucherzentrale.de/beratung .

Die größte Einzelorganisation ist die Verbraucherzentrale Nordrhein-Westfalen mit Sitz in Düsseldorf. Sie finden sie auf der Webseite www.vz-nrw.de . Weitere große Landeszentralen sind Bayern und Baden-Württemberg . Die Verbraucherzentralen stellen auch Musterbriefe zur Verfügung, um sich gegen Abzocker und Betrüger im Internet zur Wehr setzen.

Wenn das Kind schon in den Brunnen gefallen ist, dann helfen Ihnen die Verbraucherzentralen, das verlorene Geld zurückzuholen. Grundsätzlich ist die Verbraucherzentrale in Ihrem Bundesland oder die nächstgelegene Beratungsstelle der erste Ansprechpartner, da alle ähnliche Leistungen anbieten. Zwischen den einzelnen Verbraucherzentralen gibt es einen regen Austausch, so dass es einheitliche Beratungsstandpunkte gibt.

Zu den Aufgaben der Verbraucherzentralen gehört es, außergerichtlich wie auch gerichtlich gegen unzulässige Allgemeine Geschäftsbedingungen, verbraucherschutzwidrige Geschäftspraktiken und unlautere Werbemaßnahmen eines Anbieters vorzugehen. Die Verbraucherzentralen helfen gegen Entgelt bei individuellen Rechtsproblemen und vertreten Interessen der Verbraucher auch in Verbands- oder Sammelklagen. Auf der Webseite www.verbraucherschutz.com , die nichts mit den Verbraucherzentralen zu tun hat, erhalten Sie einen Ticker mit aktuellen Warnhinweisen.

Quelle: https://www.pcwelt.de/ratgeber/Aufgedeckt-Die-12-fiesesten-Online-Fallen-8028039.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3035350&pm_cat%5B0%5D=eMail+Management&pm_cat%5B1%5D=Web+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) Achtung: Volksbank-Kunden im Visier von Betrügern

Derzeit kursieren wieder vermehrt Phishing-Mails, die Volksbank-Kunden um ihre Daten bringen sollen. Wie Sie die Mails erkennen und was Sie damit tun sollten.

Die Verbraucherzentrale warnt vor aktuell kusierenden Phishing-Mails, die Volksbank-Kunden um ihre Daten bringen soll. Das Vorgehen ist dabei altbekannt. In der Mail wird der Empfänger aufgefordert, den "VR-Secure-GO"-Dienst bis zu einem zeitnahen Ablaufdatum zu aktivieren. Und zwar über den in der Mail angefügten Link, der natürlich nicht zu einem Volksbank-Service führt, sondern zu einer optisch der Volksbank nachempfunden Phishing-Seite. Wenn Sie dort Ihre Daten eintragen, landen diese direkt bei den Betrügern und gibt ihnen damit die Möglichkeit, Unfug mit Ihrem Ersparten zu betreiben. Ein Screenshot zeigt den möglichen Aufbau der Phishing-Mail.

Quelle: Volksbank-Kunden sollten vermehrt auf Phishing-Mails achten. © Verbracherzentrale

So erkennen Sie Phishing-Mails

Phishing-Mails sind oftmals einfach zu erkennen, können je nach Aufbau aber auch ein gutes Auge erfordern. Achten Sie immer auf die Mail-Adresse des Senders. Oft enthält diese den Namen der vermeintlichen Bank, um einen seriösen Eindruck zu erwecken. Wenn Sie sich unsicher sind, googeln Sie die Mail-Adresse. Nach einem Blick auf die Suchergebnisse wissen Sie Bescheid.

Auch der Aufbau der eigentlichen Mail kann ein Indiz sein. Phishing-Mails fallen häufig mit wirrer Struktur und Rechtschreibfehlern auf. Um Druck auszuüben, wird häufig ein Datum genannt, bis zu dem auf einen Link in der Mail geklickt werden muss.

Wenn Sie eine Phishing-Mail in Ihrem Posteingang entdeckt haben, klicken Sie auf keinen Link in der Mail und löschen Sie diese sofort. Sie können erhaltene Phishing-Mails auch der Verbracherzentrale melden, damit diese gegebenenfalls eine Warnung veröffentlichen kann. Dafür leiten Sie die Mail einfach an phishing@verbraucherzentrale.nrw weiter.

Quelle: https://www.pcwelt.de/news/Achtung-Volksbank-Kunden-im-Visier-von-Beruegern-11287034.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700651&pm_cat%5B0%5D=eMail+Management&pm_cat%5B1%5D=Datenbank&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Gehackte Geschäftskonten – Echte Paypal-Mails mit falscher Rechnung

Aktuell sorgen E-Mails, die von den Paypal-Servern stammen, für Unruhe. Cyberkriminelle verschicken angebliche Rechnungen. Ein Einspruch kann zu Datenverlust führen.

Der Sicherheitsforscher Brian Krebs berichtet von einer neuen Betrugsmasche im Zusammenhang mit dem Online-Bezahldienst Paypal. Cyberkriminelle haben vermutlich Geschäftskonten gekapert oder solche gefälscht und können über die Paypal-Server E-Mails mit fingierten Informationen verschicken. In beobachteten Fällen wurden falsche Rechnungen für vorgebliche Transaktionen verschickt. Klickt ein potenzielles Opfer auf die Transaktion, werden Beträge über mehrere Hundert US-Doller genannt, die in Kürze abgebucht werden.

Möchte man diese Transaktion dann rückgängig machen, wird eine Telefonnummer angezeigt, unter der sich das Opfer melden soll. Ab diesem Zeitpunkt gibt es vermehrt Gründe, skeptisch zu werden. Nach einem Anruf kommt eine Aufforderung, eine Software auf seinem Rechner zu installieren. Diese bietet den Cyberkriminellen einen Fernzugriff. Eine typische Vorgehensweise von beispielsweise falschen Support-Mitarbeitern, die statt einer vermeintlichen Fehlerlösung auf Datenjagd am eigenen Rechner gehen.

Bis zu diesem Zeitpunkt werden Menschen auf sehr arglistige Weise durch die E-Mails getäuscht. Sowohl Absender als auch Inhalte der Mail stammen von Paypal bzw. der zugehörigen Server und lassen kaum Rückschlüsse darauf zu, dass es sich um typische Phishing- oder Spam-Mails handelt. Paypal wurde informiert und ist sich der Masche bewusst, wie Brian Krebs berichtet. Zusätzliche Kontrollen sollen ähnlich geartete Angriffe unterbinden.

Aktuelle Phishing-Versuche: " Beleg für Ihre Zahlung an Netflix.com "

Vor rund einer Woche hat die Verbraucherzentrale übrigens eine weitere Warnung im Zusammenhang mit Paypal ausgesprochen. Dabei sollen angebliche Paypal-Mails Netflix-Nutzende dazu verleiten, auf einer gefälschten Webseite ihre Daten einzugeben. Hier hilft es, klassischerweise die Links zu Webseiten zu prüfen, auf die der Absender Sie schicken möchte.

Wie können Sie sich schützen?

Auch wenn die E-Mail korrekte Links zu Paypal liefert, sollten Sie sie nicht anklicken. Generell gilt, entsprechende Online-Portale händisch aufzurufen, sich mit Zwei-Faktor-Authentifizierung anzumelden und im Profil nach entsprechenden Transaktionen Ausschau zu halten. Gibt es hier Unterschiede zu Angaben in einer vermeintlich echten Rechnung, können Sie davon ausgehen, dass die E-Mail einen unseriösen Ursprung hat - bestärkt wird der Verdacht, wenn es Ihnen erschwert wird, Details einzusehen. Im Zweifel können Sie den Paypal-Support kontaktieren. Lassen Sie sich dazu von niemand Fremden zur Installation von Programmen verleiten, die Ihnen bei einem Problem helfen sollen.

Quelle: https://www.pc-magazin.de/news/paypal-echte-email-falsche-rechnung-transaktion-widerspruch-telefon-3203782.html?utm_source=nachrichten-NL&utm_medium=newsletter

Anwenderinformationen:

1) Kompletter Soundausfall – Windows-Update kann zu Audioproblemen führen

Ein Update für Windows 10 kann zu Audioproblemen führen. Bei manchen Rechnern sorgt das für einen kompletten Ausfall des Sounds. Das können Sie tun.

Auf seiner offiziellen Support-Seite hat **Microsoft** bekanntgegeben, dass ein aktuelles Windows-10-Update zu Audioproblemen führen kann. Die Windows-Version vom 26. Juli mit der Nummer "KB5015878" sorgt dafür, dass betroffene Rechner keinen Ton mehr abspielen, obwohl alle Audiogeräte richtig angeschlossen und die aktuellen Treiber installiert sind.

Ein Softwareupdate mit einer passenden Problemlösung steht derzeit nicht bereit, aber der Konzern hat eine Reihe von temporären Lösungsansätzen veröffentlicht, mit denen Nutzer ihren Sound wieder zum Laufen bringen können.

Lösungsansätze: Das können Sie tun

Als Hauptursache für das Problem hat Microsoft die Option "Audioverbesserungen" ausgemacht. Diese könnten dazu führen, dass durch das Update entweder der komplette Sound ausfällt oder zumindest in manchen Anwendungen und Programmen keine Töne mehr abgespielt werden. Je nach Situation hat der Konzern unterschiedliche Szenarien und Herangehensweisen vorgestellt:

Falls Sie das Update "KB5015878" noch nicht installiert haben

Die Audiogerätetreiber zu aktualisieren, könnte vor dem Update das Auftreten der Soundprobleme verhindern. Deshalb empfiehlt Microsoft, erst die entsprechenden Treiber auf den aktuellen Stand zu bringen, bevor ein Windows-Update angestoßen wird.

Falls Sie das Update "KB5015878" bereits installiert haben

Die integrierte "Problembehandlung" im Bereich "Sound" der Systemeinstellungen könnte laut Microsoft das Problem bereits lösen. Falls nicht, sollen betroffene Nutzer Audioverbesserungen ausschalten. Wie das funktioniert, wird auf dieser Hilfeseite erklärt.

Quelle: https://www.t-online.de/digital/computer/software/windows/id_100042848/windows-10-update-kann-audio-probleme-verursachen.html

2) Alle Mediatheken auf dem Handy zugänglich haben

Die Mediatheken der Fernsehanstalten sind ideal, um versäumte Sendungen nachzuholen. Und auch spontane Fernsehabende lassen sich damit schnell realisieren. Die Wiedergabe muss dabei nicht notgedrungen auf dem großen Fernseher erfolgen.

Denn auch unterwegs, auf dem Smartphone oder Tablet, lassen sich der Tatort vom letzten Sonntag, die Lieblings-Soap oder die Sportschau nachträglich ansehen. Einzige Voraussetzung ist, dass Ihr Wiedergabegerät eine Verbindung ins Internet hat, vorzugsweise per WLAN.

Mit der kostenlosen App Mediatheksuche stehen Ihnen die Mediatheken aller großen Fernsehsender zur Verfügung. Die App bietet, wie der Name schon andeutet, eine Suchfunktion und spielt die Inhalte, soweit diese frei verfügbar sind, gleich ab. Nach der Installation geben Sie einfach den gewünschten Suchbegriff in die Suchleiste oben ein und

tippen im Anschluss daran auf das Lupensymbol. Die Ergebnisliste zeigt alle Sendungen an, die den Suchbegriff enthalten. Hier müssen Sie also auf der Suche nach einem bestimmten Inhalt entweder ein wenig blättern oder den Suchbegriff erweitern. Alternativ dazu können Sie die Ergebnisliste über den Reiter „Mediathek“ nach Sender aufschlüsseln.

Tippen Sie auf einen Eintrag, öffnet sich eine kurze Inhaltsbeschreibung, und Sie dürfen wählen, ob Sie das Video in der dazugehörigen Mediathek (per Browser oder App, falls installiert) oder über den integrierten Player der Mediatheksuche ansehen möchten. Wenn Sie sich für Letzteres entscheiden, stehen Ihnen drei Qualitätsstufen für die Wiedergabe zur Auswahl. Über das Kontextmenü jeder Qualitätsstufe, das Sie über die drei Punkte rechts daneben aufrufen, können Sie die Inhalte auch per Chromecast auf dem Fernseher ausgeben, herunterladen oder teilen.

Tipp: ARD und ZDF Mediathek: Filme sofort herunterladen - so geht’s

Quelle: https://www.pcwelt.de/tipps/Alle-Mediatheken-auf-dem-Handy-zugaenglich-haben-11275064.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3700646&pm_cat%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) PDFs lassen sich jetzt direkt im Browser unterschreiben: Nie mehr drucken und wieder abfotografieren

Zum Unterschreiben werden PDF-Formulare oft noch ausgedruckt, dann mit Stift signiert und zum Versenden wieder abfotografiert. In Firefox können Sie PDFs direkt unterschreiben.

PDF-Formulare mögen nicht Hightech sein, aber wenn man sie am Rechner ausfüllt und weiterschickt, spart man Papier und Zeit. Doch häufig ist auch eine Unterschrift fällig und dann wird erst ausgedruckt, dann per Stift unterschrieben, nur um das Dokument dann wieder abzufotografieren und einzuscannen. So kann man es dann wenigstens digital übermitteln und spart sich das Briefporto, trotzdem ist das Prozedere umständlich.

Das geht aber auch wesentlich einfacher: Im neuen Firefox 104 steckt ein Update für den PDF-Viewer. Mit dem können Sie per virtuellem Stift Dokumente unterschreiben.

PDF-Dokumente direkt in Firefox unterschreiben

Wenn Sie jetzt ein PDF mit Firefox öffnen, kriegen Sie eine erweiterte Toolbar angezeigt. Ganz rechts sehen Sie ein kleines Stiftsymbol, über das Sie dann eine Unterschrift einfügen können. Halten Sie die rechte Maustaste gedrückt und unterschreiben sich per Maus oder Touchpad. Haben Sie ein Notebook mit Touchscreen, können Sie auch direkt auf dem Bildschirm unterschreiben.

Viel gibt es nicht einzustellen: Sie können die Farbe anpassen, Standard ist schwarz und die Liniendicke per Schieberegler justieren. Mit der Maus unterschreiben geht meist nicht so flott von der Hand wie mit Stift. Sollten Sie mit dem Ergebnis nicht zufrieden sein, klicken Sie außerhalb von Firefox, dann wird die Unterschrift rot umrandet. Sie können den Baustein dann einfach entfernen und nochmal neu unterschreiben.
Leider gibt es noch keine Möglichkeit, die Unterschrift zu speichern. Das wäre praktisch, dann könnte man sie als Baustein einfach in jedes PDF einsetzen. Was aber möglich ist: Sie können die Größe der Unterschrift anpassen. Dazu einfach mit der Maus in die rechte untere Ecke der Umrandung gleiten und den Rahmen größer oder kleiner ziehen.

Neuen PDF-Viewer in Firefox aktivieren

Nicht überall zeigt sich der neue PDF-Editor in Firefox 104 sofort. Er steckt aber auf jeden Fall unter der Haube. Um ihn zu aktivieren, tippen Sie "about:config" in die Adresszeile ein, klicken auf "Risiko akzeptieren und fortfahren" und suchen nach der Einstellung **pdfjs.annotationEditorMode**. Die muss den Wert **0** haben, erst dann können Sie PDFs direkt in Firefox unterschreiben.

Anmerkung der Redaktion: Funktioniert, wenn Firefox 104 aktuell ist und der Wert auf 0 gestellt worden ist.

Quelle: https://www.chip.de/news/PDFs-lassen-sich-jetzt-direkt-im-Browser-unterschreiben-Nie-mehr-drucken-und-wieder-abfotografieren_184397999.html

4) Android 13: Malware umgeht bereits neue Sicherheitsfunktionen

Hacker haben bereits die neueste Android-Version von Google im Visier genommen und neue Sicherheitsfunktionen umgangen.

Hacker haben mithilfe einer neuen Malware schon Wege gefunden, die neuen Sicherheitsmechanismen von Android zu umgehen, die eigentlich genau diese Art von Schadsoftware stoppen sollte. Die Malware, der dieses Kunststück geglückt ist, mimt dabei einen App-Store, um an den Einschränkungen vorbeizukommen.

Sicherheitsforscher des Betrugserkennungsunternehmens ThreatFabric haben in einem Blogbeitrag die neue Sicherheitslücke aufgedeckt. Dem Beitrag zufolge kann sich eine bösartige App als App-Store ausgeben und so die neuen Sicherheitsmaßnahmen von Android 13 aushebeln.

Wie Android Police berichtet, baut dieser neue Exploit auf einer älteren Malware auf, die die Zugangsdienste von Android nutzt, um den Zugriff auf private Daten, Passwörter und mehr zu erleichtern.

Im Gegensatz zu früheren Versionen des mobilen Google-Betriebssystems erlaubt Android 13 nicht mehr, dass von außen geladene Anwendungen Zugriff auf die Eingabehilfsdienste des Smartphones anfordern. Diese muss der Nutzer erst über den App-Infobildschirm aktivieren. Das könnte Google jedoch noch vor der allgemeinen Veröffentlichung von Android 13 entfernen.

Der Grund dafür, dass Google beschlossen hat, den Zugriff auf Zugangsdienste für von außen heruntergeladene Apps zu erschweren, ist die Tatsache, dass bösartige Apps und andere Malware während der Installation in der Regel nach zusätzlichen Berechtigungen fragen. Wenn Sie nun eine App außerhalb eines offiziellen App-Stores herunterladen, ist es für diese App schwieriger, auf Ihre Kontakte zuzugreifen, um Spam zu verbreiten oder sich in anderen Apps zu erscheinen.

Sicherheitsfunktion Segen und Fluch zugleich

Die Sache hat allerdings einen Haken, denn viele Menschen sind auf Zugangsdienste angewiesen, um ihre Geräte besser nutzen zu können. Alle Apps, die aus dem Play Store oder App-Stores von Drittanbietern wie F-Droid oder dem Amazon App Store heruntergeladen werden, sind von dieser Einschränkung ausgenommen. Das ist sinnvoll, aber auch die Krux zugleich.

Die Malware-Entwickler der Hadoken-Gruppe nutzen diese Schwachstelle jetzt zu ihrem Vorteil aus, und zwar in Form des neuen Exploits, der den Namen BugDrop trägt. Der Exploit selbst besteht aus zwei Teilen, wobei der erste Teil eine "Dropper"-App installiert, die wie ein App-Store auf dem Gerät des Opfers funktioniert. Von hier aus wird eine sitzungsbasierte Paketinstallations-API verwendet, um eine weitere Anwendung zu installieren, die Malware enthält.

Wie die ThreatFabric berichtet, befindet sich diese Malware glücklicherweise noch im Anfangsstadium und ist im Moment noch sehr fehleranfällig. Dennoch könnte sie bereits genutzt werden, um Smartphones mit Malware zu infizieren, sobald mehr Telefonhersteller ihre Android-13-Updates ausrollen.

So schützen Sie sich vor bösartiger Software auf dem Smartphone

Zunächst einmal sollten Sie auf Ihrem Android-Smartphone keine Apps per Sideload laden, sondern sie aus den offiziellen App-Stores herunterladen. Aber auch hier gilt, die Bewertungen lesen – schwarze Schafe gibt es nämlich auch in offiziellen Stores.

Die Aktivierung von Google Play Protect auf Ihren Geräten ist eine weitere Möglichkeit, sich zu schützen, da die Google-eigene Android-Antivirus-App alle von Ihnen installierten Apps auf Malware und andere Bedrohungen überprüft.

Wenn es um Berechtigungen geht, sollten Sie sich vor jeder App in Acht nehmen, die um Berechtigungen bittet, die sie eigentlich nicht benötigt, wie die Möglichkeit, über andere Apps zu zeichnen. Apps, die Zugriff auf die Zugangseinstellungen von Android verlangen, sind ebenfalls mit besonderer Vorsicht zu genießen. Apps, die Sie schon lange nicht mehr nutzen, sollten Sie ebenfalls löschen.

Passend dazu: Diese Android-Apps sollten Sie sofort löschen – Malware im Play Store

Quelle: https://www.pcwelt.de/news/Android-13-Malware-umgeht-bereits-neue-Sicherheitsfunktionen-11286139.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700621&pm_cat%5B0%5D=Apple&pm_cat%5B1%5D=Mobile+Client&pm_cat%5B2%5D=Mobile+Plattformen&pm_cat%5B3%5D=Android&pm_cat%5B4%5D=Mobilfunk&pm_cat%5B5%5D=Google&pm_cat%5B6%5D=Kreativ+Software&pm_cat%5B7%5D=Virenschutz&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Brandgefahr: Asus ruft 600-Euro-Mainboard zurück

Asus muss tausende Mainboards zurückrufen. Ein Konstruktionsfehler kann zu Ausfällen und im schlimmsten Fall sogar zum Brand führen. Erste Fälle sind bereits bekannt.

Wenn Sie im letzten Jahr ein Premium-Mainboard von Asus gekauft haben, könnte diese Rückrufaktion für Sie relevant sein. Asus ruft schätzungsweise 10.000 Hauptplatinen vom Modell ROG Maximus Z690 Hero zurück. Aktueller Preis: Rund 640 Euro. Der Grund: Brandgefahr.

Ob Ihr Mainboard von der Rückrufaktion betroffen ist, können Sie mithilfe dieser Website überprüfen. Dafür wird die Seriennummer ihres Modells mit der Datenbank abgeglichen. Besonders betroffen sind die Chargen, deren Seriennummer mit MA, MB oder MC beginnt. Wo Sie die Seriennummer auf ihrem Mainboard finden, zeigen Ihnen Abbildungen auf der Website.

Fehlerhaft verbaut: Kondensator kann sich erhitzen

Der Grund für die Rückrufaktion ist ein Kondensator, der in einigen Fällen falsch herum verbaut wurde. Das führt offenbar nicht zu einer sofortigen Fehlfunktion der Hauptplatine, sondern das kann nach längerem Gebrauch zu Fehlercodes, Ausfällen oder (zumindest

potenziell) zu einem direkten Durchbrennen der Hauptplatine und anderer Komponenten führen.

Laut der US-amerikanischen Verbraucherschutzkommission (Consumer Product Safety Commission, CPSC) hat Asus zehn Berichte über Überhitzung und Schmelzen der Mainboards erhalten. Verletzungen wurden nicht gemeldet. Asus macht keinen Angaben darüber, in welchen Ländern die betroffenen Chargen verkauft wurden. Bisher beschränken sich die Meldungen auf die Vereinigten Staaten.

Sollte Ihr Mainboard wirklich betroffen sein, bietet Asus einen kostenlosen Austausch und übernimmt auch die Liefergebühren für Versand und Rückversand.

Quelle: https://www.pcwelt.de/news/Brandgefahr-Asus-ruft-600-Euro-Mainboard-zurueck-11285695.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700608&pm_cat%5B0%5D=Hardware+allgemein&pm_cat%5B1%5D=Notebook+Ultrabook&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) Millionenfach heruntergeladen: Schadsoftware in zahlreichen Android-Apps entdeckt

Bei zahlreichen Android-Apps haben Sicherheitsexperten Schadsoftware entdeckt. Die Anwendungen wurden insgesamt rund zwei Millionen mal aus dem Play Store heruntergeladen. Nutzern wird die sofortige Deinstallation empfohlen.

Obwohl der Google Play Store über Sicherheitsvorkehrungen verfügt, um gefährliche Apps auszusortieren, schaffen es einige, unbemerkt durchzukommen. Bitdefender entdeckte nun 35 bösartige Anwendungen im Google Play Store.

Diese Anwendungen geben sich als Einstellungs-Apps aus und haben über 2 Millionen Installationen. Sobald sie installiert sind, zeigen diese Anwendungen Werbung auf den Telefonen der Nutzer an. Nach der Installation ändert die Software ihren Namen und ihr Symbol, um auf dem Smartphone verborgen zu bleiben.

Schadsoftware bei Android entdeckt: Diese Apps sind betroffen

Laut BitDefender können Nutzer die Programme zum Glück deinstallieren, was auch unbedingt getan werden sollte. Hier ist eine Liste der Anwendungen, die als schädlich eingestuft wurden:

- Walls light – Wallpapers Pack
- Big Emoji – Keyboard
- Grad Wallpapers – 3D Backdrops
- Engine Wallpapers – Live & 3D
- Stock Wallpapers – 4K & HD
- EffectMania – Photo Editor
- Art Filter – Deep Photoeffect
- Fast Emoji Keyboard
- Create Sticker for Whatsapp
- Math Solver – Camera Helper
- Photopix Effects – Art Filter
- Led Theme – Colorful Keyboard
- Keyboard – Fun Emoji, Sticker
- Smart Wifi
- My GPS Location
- Image Warp Camera

- Art Girls Wallpaper HD
- Cat Simulator
- Smart QR Creator
- Colorize Old Photo
- GPS Location Finder
- Girls Art Wallpaper
- Smart QR Scanner
- GPS Location Maps
- Volume Control
- Secret Horoscope
- Smart GPS Location
- Animated Sticker Master
- Personality Charging Show
- Sleep Sounds
- QR Creator
- Media Volume Slider
- Secret Astrology
- Colorize Photos
- Phi 4K Wallpaper – Anime HD

Um solche Fehler in Zukunft zu vermeiden, sollten Sie immer die Berechtigungen im Google Play Store ansehen, bevor Sie eine App herunterladen und installieren.

Quelle: https://www.chip.de/news/Mehrere-Android-Apps-mit-Schadsoftware-verseucht-Millionen-Downloads_184396310.html

7) Whatsapp: So sehen Sie, wer Sie blockiert

Ob ein Kontakt Sie auf Whatsapp blockiert, können Sie recht schnell herausfinden. Wir zeigen Ihnen, wie das geht.

Aus Gründen der Privatsphäre teilt Whatsapp Ihnen nicht mit, wenn jemand Sie blockiert. Und doch gibt es Möglichkeiten, es herauszufinden. Es gibt nämlich einige Hinweise, die Ihnen Aufschluss darüber bringen, wer Sie bei Whatsapp blockt.

Nachricht wird nicht zugestellt – nur ein Haken

Schicken Sie eine Nachricht an einen Whatsapp-Kontakt und es erscheint nur ein Häkchen unter der Nachricht, dann ist dies ein erster Hinweis. Denn kommt eine Nachricht ganz regulär beim Empfänger an, erscheinen normalerweise zwei Häkchen: Das erste Häkchen bedeutet, dass die Nachricht auf den Servern bei Whatsapp gelandet ist. Das zweite Häkchen erscheint, wenn die Nachricht erfolgreich beim Empfänger angekommen ist.

Fehlt der zweite Haken, kann dies bereits ein Indiz sein, dass der Empfänger keine Nachrichten mehr von Ihnen bekommen möchte. Das Indiz kann aber erst durch die nächsten Punkte bekräftigt werden. Denn es kann auch daran liegen, dass es aktuell ein technisches Problem seitens Whatsapp gibt oder, noch wahrscheinlicher, der Empfänger das Handy derzeit ausgeschaltet, es in den Flugmodus gestellt oder einfach keinen Internetempfang hat.

Das Profilbild fehlt plötzlich

Befindet sich auf einmal an der Stelle des Profilbildes nur noch ein grauer Platzhalter und Sie können den Whatsapp-Status der Person nicht mehr sehen, dann wurden Sie wahrscheinlich

blockiert. Fehlt nur das Profilbild, kann es auch daran liegen, dass Ihr Kontakt sein Bild entfernt hat.

Sehr sicheres Indiz: Neue Whatsapp-Gruppe erstellen

Erstellen Sie eine neue Whatsapp-Gruppe und fügen Sie unter anderem den Kontakt hinzu, von dem Sie vermuten, blockiert zu werden. Schauen Sie sich anschließend die Teilnehmer der Gruppe genau an. Taucht hier der Kontakt nicht auf, hat dieser Sie blockiert. Daher ist diese Methode sehr sicher, um festzustellen, ob Sie geblockt werden.

Interessant ist aber: Sind Sie bereits mit dem Blockierer in einer bestehenden Gruppe, dann können Sie diesen in der Gruppe noch immer markieren und anschreiben. Allerdings sehen diese Nachricht natürlich auch die anderen Gruppenmitglieder.

Whatsapp-Anrufe nicht mehr erfolgreich

Bei Whatsapp können Sie Video- und Sprachanrufe über eine Internetverbindung führen. Wenn Sie blockiert sind, dann sind Anrufe nicht mehr erfolgreich, heißt: Der Empfänger sieht diese nicht und kann sie entsprechend nicht annehmen. Sie hören allerdings die Anruftöne, der Anruf bricht nicht sofort ab. Ein sicherer Hinweis ist der misslungene Anruf also nicht.

"Zuletzt Online" prüfen

Hat ein Kontakt Sie blockiert, dann können Sie nicht mehr sehen, wann dieser zuletzt online war. Hier ist allerdings Vorsicht geboten: Denn auch, wenn ein Kontakt die entsprechende Einstellung unter "Datenschutz" deaktiviert hat, können sie diese Info nicht einsehen.

Hinweis: Die meisten Punkte treffen auch dann zu, wenn eine Person ihren Whatsapp-Account gelöscht hat.

So können Sie selbst einen Kontakt blockieren

Um selbst jemanden zu blockieren, tippen Sie auf den Chat mit der Person und dann auf deren Namen. Scrollen Sie nach ganz unten und tippen Sie dort auf "Blockieren" und bestätigen Sie dies anschließend. Um zu sehen, wen Sie alles blockieren, navigieren Sie in die Whatsapp-Einstellungen und tippen Sie dort auf "Account – Datenschutz". Hier finden Sie den Punkt "Blockierte Kontakte". Tippen Sie den Kontakt an, können Sie ihn wieder "freigeben".

Alle Nachrichten, die der Kontakt während der Blockierung an Sie geschickt hat, können Sie nicht sehen. Und andersherum sieht der Blockierer nicht, was Sie ihm während der blockierten Zeit geschrieben haben.

Weitere spannende Whatsapp-Themen

- So nutzen Sie WhatsApp auf PC, iPad und Android-Tablet
- Whatsapp-Status heimlich ansehen
- Gelöschte Whatsapp-Nachrichten trotzdem lesen
- Whatsapp mit Festnetzummer nutzen
- Whatsapp für Notizen verwenden
- Whatsapp-Profilbilder von anderen Kontakten abspeichern

Quelle: https://www.macwelt.de/ratgeber/Whatsapp-blockiert-wer-hat-mich-geblockt-11007222.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=0&pm_cat%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

8) Warum Schnellladen beim iPhone 14 noch immer langsam ist

Das iPhone 14 soll schneller aufladen als zuvor. Nur ist das noch immer viel zu langsam – hier erfahren Sie alle Details.

Wie kürzlich bekannt wurde, soll das iPhone 14 mit bis zu 30 Watt „superschnell“ aufladen . Gegenüber den Vorgänger-Modellen mag das tatsächlich ein Fortschritt sein – wenn auch ein kleiner. Im Vergleich zu so manchem Android-Handy kann das neue iPhone aber einpacken. Ein iPhone 13 braucht fast 90 Minuten, um vollgeladen zu sein. Ein aktuelles OnePlus 10T ist in unter 20 Minuten bei 100 Prozent Akkuladung .

Während also vor allem die chinesischen Marken wie Xiaomi, Oppo (und damit auch OnePlus) hier ordentlich auf den Putz hauen und mit Wattzahlen protzen, ist Apples Umgang mit der Ladetechnik bzw. einer hohen Ladegeschwindigkeit eher konservativ. Will Apple nicht hervorstechen? Oder kann Apple es etwa gar nicht?

Alle Hersteller von aktuellen Android-Handys setzen auf einen USB-C-Anschluss und verschiedene Schnellladeprotokolle. Oppos eigener VOOC-Standard etwa ermöglicht, wie oben erwähnt, derzeit 150 Watt zum Beispiel beim OnePlus 10T (beide Marken gehören zu einem Konzern). Außerdem stellt Oppo sogar 240 Watt mit VOOC in Aussicht, ein Handy mit einem 4500-mAh-Akku wäre dann in 9 Minuten vollgeladen. Das OnePlus 10T lädt derzeit von 1 auf 100 Prozent in 19 Minuten. Tatsächlich aber ist es ein Problem, wenn Sie ein Smartphone laden, das den entsprechenden Lade-Standard nicht unterstützt, dann lädt es sogar deutlich langsamer auf, als es mit dem Netzteil möglich wäre. Es gibt aber Standards wie Power Delivery oder Quick Charge, die sehr verbreitet sind und von vielen Hersteller unterstützt werden.

Ist Lightning das Problem?

Insgesamt ermöglicht USB-C mit seinen Schnellladeprotokollen höher Ladegeschwindigkeiten als Lightning bei gleicher Spannung. USB-C unterstützt höhere Stromstärken. Interessant ist auch, dass ein Standard-Lightning-Kabel keine Schnellladung unterstützt. Deswegen gibt es für neuere iPhones auch die USB-C-auf-Lightning-Kabel, die höhere Ladegeschwindigkeiten erlauben.

Das iPhone 14 (warum sich Warten lohnt) wird wie gewohnt ebenfalls mit einem Lightning-Anschluss kommen, jetzt aber immerhin 30 Watt unterstützen. Nun ist es aber so, dass die EU sich darauf geeinigt hat , USB-C als Standard für kabelgebundenes Laden festzulegen. Bis Herbst 2024 sollen demnach unzählige Geräte mit dem universellen USB-C-Anschluss ausgestattet werden.

Zwar behauptet Apple, dass ein solcher Schritt Innovation bremsen würde. Doch wirft man einen Blick auf die Unterschiede zwischen Lightning und USB-C (oder, genau genommen, die dazugehörigen Verbindungsstandards), dann wird deutlich, dass USB-C die proprietäre Technologie von Apple unlängst überholt hat. Wirklich abgeneigt ist man bei Apple gegenüber USB-C jedoch sowieso nicht, denn das Unternehmen verbaut den Anschluss schon lange in seinen Macbooks und legt aktuellen Geräten wie dem iPad ein USB-C-Ladegerät bei – aber eben in Kombination mit einem Lightning-auf-USB-C-Kabel.

Mit dem iPhone 15 könnte Apple also schon auf USB-C setzen. Das Handy könnte dadurch auch deutlich schneller laden – wenn Apple dies auch erlaubt. Tatsächlich aber könnte Apple auch einen eigenen, radikalen Weg einschlagen und den Anschluss komplett abschaffen, denn die Voraussetzungen dafür sind alle vorhanden.

Gerade beim kabellosen Laden gibt es auch außerhalb des Apple-Kosmos große Fortschritte. So können sie etwa das Honor Magic 4 Pro (bei Amazon ansehen) auch kabellos mit satten 100 Watt laden – deutlich schneller als Apple es derzeit kabelgebunden am iPhone kann.

Ist Schnellladen schädlich für den Akku?

Dem einen oder anderen Nutzer wird sich jetzt die Frage stellen, wie das sein kann. Bei so einem Unterschied muss es doch einen Haken geben – ist Schnellladen gar schädlich für den Akku? Dieser Frage gehen wir in unserem ausführlichen Ratgeber dazu auf den Grund . Kurz gesagt: Bisher weist alles darauf hin, dass Schnellladen den normalen Verschleiß eines Akkus *nicht* beschleunigt. Fakt ist aber auch, dass Schnellladen durch die höheren Wattzahlen mehr Wärme erzeugt, vor der das Telefon geschützt werden muss. Dazu bedienen sich die Hersteller verschiedener Maßnahmen – sei es durch optimierte Netzteile, paralleles Laden von zwei Akkuzellen (statt nur einer) oder smarte Hardware und Sensoren zur Regulierung von Temperaturschwankungen.

Obwohl Apple bei seinen iPhones kein „echtes“ Schnellladen bietet, wie Sie es von der Konkurrenz kennen, verspricht das Unternehmen nur 500 Ladezyklen , nach denen das iPhone noch eine Akkukapazität von 80 Prozent aufweist. OnePlus mit seinen 150 Watt gibt an, dass der Akku des OnePlus 10T nach 1600 Ladezyklen noch 80 Prozent seiner Anfangskapazität besitzt. Das entspricht einer täglichen Ladung über einen Zeitraum von 4 Jahren.

Quelle:https://www.macwelt.de/ratgeber/Warum-Schnellladen-beim-iPhone-14-langsam-ist-11287182.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700638&pm_cat%5B0%5D=Hardware+allgemein&pm_cat%5B1%5D=Apple&pm_cat%5B2%5D=iOS&pm_cat%5B3%5D=Mobile+Client&pm_cat%5B4%5D=Mobile+Plattformen&pm_cat%5B5%5D=Mobilfunk&pm_cat%5B6%5D=Mobile+Security&pm_cat%5B7%5D=BYOD&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

9) Warum Sie ein Antivirus-Programm für den Mac brauchen

Noch immer gilt eine Antivirensoftware für Macs als überflüssig, das ist aber etwas zu kurz gedacht. Wir räumen mit einer Legende auf.

Beim Thema Antivirensoftware für den Mac treffen Sie vermutlich auf zwei Meinungen: Viele erfahrene Apple-Anwender haben zu Antivirensoftware eine sehr negative Einstellung und behaupten Ihnen gegenüber, das sei komplett überflüssig – „Snake Oil“. Fast jeder Systemadministrator eines Unternehmens schlägt dagegen die Hände über den Kopf zusammen und findet Macs ohne Virenscanner äußerst fahrlässig.

Und beide haben eigentlich recht. Die Ablehnung von Antivirensoftware hat zwei Hauptgründe: Für einen Heimanwender kann eine Antivirensoftware zum Ärgernis werden, schließlich greifen die Apps tief ins System ein. Apple verspricht außerdem auf seiner Webseite, macOS sei ein besonders sicheres System und die vorinstallierten Sicherheitssysteme völlig ausreichend. Anders sieht dies ein Systemadministrator eines Unternehmens, der für die IT-Sicherheit seines Unternehmens verantwortlich ist. Angriffe durch Malware sind häufiger als vermutet und die Verantwortlichen haben wenig Verständnis für Mac-Anwender, die sich aus Komfortgründen gegen Antivirensoftware wehren. In den letzten Jahren hat es immer wieder ernst zu nehmende Angriffe auf Macs gegeben. Für Unternehmen ist deshalb Sicherheitssoftware unerlässlich und viele Anwender bekommen abgewehrte Sicherheitsangriffe oft gar nicht erst mit, werden diese doch oft schon auf Ebene des Firmennetzes oder der E-Mail-Konten abgewehrt. Auch viele Universitäten wie die TU München empfiehlt Mac-Anwendern die Nutzung von Antivirensoftware.

Antivirus für den Mac: Zehn Programme im Vergleich

Selbst Craig Federighi musste während der Gerichtsverhandlung mit Epic zugeben „Today, we have a level of malware on the Mac that we don't find acceptable and is much worse than iOS". (Heute gibt es auf dem Mac ein Ausmaß an Malware, das wir nicht für akzeptabel halten und das viel schlimmer ist als bei iOS)

Welche Fachleute soll man fragen?

Sucht man Expertise zu diesem Thema, gibt es außerdem ein Problem: Fachleute sind selten völlig unabhängig. Fragt man etwa einen Sicherheitsexperten von Apple, bestätigt dieser mit Sicherheit die Firmenpolitik, dass Antivirenprogramme unnötig seien. Ein bei einer Antivirensoftware-Firma angestellter Experte ist dagegen gleichermaßen von der Relevanz von Antiviren-Software überzeugt. Auch die Meinung der Macwelt ist hier vielleicht nicht fachlich befriedigend. Eine unabhängige und auch fachlich anerkannte Position nimmt aber die Behörde BSI an, die wir für diesen Artikel um ihre Stellungnahme gebeten haben. Laut einem Sprecher lautet sie:

„Für MacOS gibt es deutlich weniger Malware als beispielsweise für Windows. Die Notwendigkeit für zusätzlichen Virenschutz hängt daher sehr von der Nutzung ab. Werden IT-Systeme für berufliche oder kommerzielle Zwecke genutzt oder bestehen besondere Anforderungen bzgl. IT-Sicherheit (z. B. nach DSGVO), empfiehlt das BSI einen zusätzlichen Virenschutz. Insbesondere wenn MacOS-Systeme in einem Netz mit Windows-Systemen betrieben werden, ist ein zusätzlicher Virenschutz notwendig. Bei ausschließlich privater Nutzung reicht in der Regel der eingebaute Virenschutz von Apple. Wer bei privater Nutzung bewusst ein höheres Risiko eingeht (z. B. Filesharing) oder häufig E-Mails von unbekannten Personen erhält, sollte ebenfalls einen zusätzlichen Virenschutz in Erwägung ziehen."

Nach unserer Meinung eine ausgewogene Empfehlung.

Welche Anwendungen sind zu empfehlen?

Wir veröffentlichen mehrmals im Jahr einen Vergleichstest der wichtigsten Antivirenprogramme für den Mac . Aktuell empfehlen wir etwa die kostenlose Lösung Avast und für anspruchsvollere Anwender die kostenpflichtige Lösung Bitdefender.

Ist macOS sicherer als Windows?

Noch immer hat Apple den Ruf, das sicherere System zu sein. Wie viele Experten bestätigen, hat Windows aber längst aufgeholt und viele Schwachstellen beseitigt. Auf der Windows-Plattform ist Antivirensoftware selbstverständlich, sogar Microsoft hat mittlerweile (zum Leidwesen viele Antivirensoftware-Hersteller) eine gute Schutzsoftware vorinstalliert. Auch das Bug-Bounty-Programm von Microsoft ist sehr erfolgreich – wer eine Sicherheitslücke oder andere kritische Fehler entdeckt und sie an den Hersteller meldet, bekommt eine finanzielle Belohnung. Allerdings ist Windows noch immer das Hauptangriffsziel aller Malware-Autoren. Überspitzt formuliert: Im Prinzip mag Windows vielleicht sogar sicherer als macOS sein, steht aber deutlich mehr unter Beschuss. AV-Test etwa meldet für 2022 bereits 37,66 Millionen neue Malware-Varianten für Windows, aber nur 4280 Mac-Schädlinge. Auch bei den sogenannten Lästlingen (meist Adware) steht es mit 1,03 Millionen vs. 7935 kaum besser. (Stichtag 10. Juli 2022). Auch auf der iOS-Plattform geht es bedeutend ruhiger zu, als auf der Android-Plattform.

Neigen Mac-Anwender zur Selbstüberschätzung?

Dass Apple verspricht, macOS sei sicher, hat aber auch einen psychologischen Effekt, der nicht ganz ungefährlich ist. Nicht falsch ist sicher die Befürchtung des Sicherheitsprofis Patrick Wardle, dass Mac-Anwender sich dank Apples Sicherheits-Versprechen oft in falscher Sicherheit wiegen . Die Einstellung, Macs wären sicher, kann deshalb zu riskanteren Aktionen führen – etwas dem Download dubioser Tools oder Filme oder dass man einfach doch auf

einen verdächtigen Link klickt "man hat ja einen Mac".

Ist in macOS eine Antivirensoftware vorinstalliert?

Was viele nicht wissen und was Apple oft etwas vage erklärt: Eigentlich ist ja laut Apple unter macOS bereits eine Antivirensoftware installiert : „state-of-the-art antivirus software built in to block and remove malware“. Das ist richtig. Gemeint ist damit XProtect, eine auf regelmäßig aktualisierten Signaturen basierende Systemfunktion. In den letzten Jahren hat Apple dieses System deutlich weiter entwickelt. Im Prinzip funktioniert Xprotect ebenso wie ein Virenscanner und überprüft mit Safari heruntergeladenen Dateien vor dem Öffnen und vor der Installation. XProtect arbeitet dabei mit Gatekeeper zusammen und ist für das Aufspüren und Entfernen von Malware auf dem Mac zuständig . Wie die letzten Jahre gezeigt haben, ist aber Apple bei der Bereitstellung neuer Signaturen weit langsamer als Drittthersteller und oft wurden Mac-Schädlingen von XProtect deutlich schlechter erkannt. Nicht zuletzt ist das Überlisten von XProtect das wichtigste Ziel jedes Malware-Autoren. Ein gutes Antivirenprogrammen eines Drittherstellers kann XProtect nach unserer Einschätzung nicht voll ersetzen.

Es gibt nicht nur Viren

Nicht vergessen sollte man, dass viele Betrugsversuche gar nicht auf Malware basieren, sondern auf Social Engineering und Phishing. Angefangen vom angeblichen Kollegen, der eine Datei zuschickt, bis zur täuschend echt wirkenden E-Mail von der Hausbank. Anrufe von angeblichen Microsoft-Mitarbeitern sollte man ebenfalls nicht vergessen, die angeblich einen Virus auf ihrem Rechner entdeckt haben… Auch hier helfen Apples Sicherheits-Funktionen wenig, wenn manche sogar auf Anfrage einfach ihre Konto- oder Anmeldedaten mitteilen.

Sind die meisten Angriffe lästige Adware?

Geht es um die Zahl der Angriffe auf Macs, handelt es sich größtenteils um Adware. Ziel der Schadsoftware ist nicht wie bei Malware die Erpressung oder das Stehlen von Daten, sondern Anzeige von Werbung. Dazu installieren Sie Hintergrund-Tools, die gezielt Werbung in Safari aufrufen. Wie die Daten von AV-Test zeigen, ändert sich dies aber das Verhältnis der beiden Angriffsarten immer wieder, die Entwicklung ist eher wellenförmig als kontinuierlich. So gab es 2016 besonders viele Angriffe durch Adware, 2020 durch Malware.

Auch 2022 scheint Adware zu dominieren. 2022 wurden bisher 4280 Malware-Versionen entdeckt, 7935 Schädlingen aus dem Bereich Adware und PUA. Das sind recht niedrige Zahlen, 2020 gab es mit 673 743 Malware-Versionen und 48191 Adware-Versionen weit mehr „echte“ Malware.

Ohne Antivirensoftware gäbe es weniger bekannte Angriffe

Was auch Kritiker der Antivirensoftware bestätigen müssten: Ohne diese Firmen blieben viele Angriffe unentdeckt. Neue Mac-Malware wird meist von Firmen wie Bitdefender, Sophos, Kaspersky nicht nur entdeckt, sondern auch öffentlich bekannt gemacht. Apple ist da weit sparsamer mit Informationen.

Genügt ein aktuelles System?

Malware nutzt oft Schwachstellen des Systems, um auf einen Mac zu gelangen. Das schnelle Aufspielen von Sicherheitsupdates ist wichtig, um den Mac zu schützen. Allerdings wird man dadurch nicht vor Sicherheitslücken geschützt, die bisher noch nicht von Apple korrigiert wurden.

Darum ist Antivirensoftware unter iOS überflüssig

Eine Antivirensoftware ist unter iOS wenig sinnvoll, Apple hat das System nach außen stark

abgesichert. Hier setzt Apple auf die komplette Abschottung des Systems und die Kontrolle von Installationen durch den App Store. Ein per App Store installierter Scanner könnte die Installation von Malware-Apps ohnehin nicht verhindern, nicht einmal nach vorhandenen Malware-Apps suchen. Als iOS-Anwender kann man sich außerdem darauf verlassen, dass Apple den App Store frei von Malware hält – oder zumindest ebenso schnell reagiert wie ein Hersteller von Antiviren-Software. Trotzdem hätten sich Antiviren-Apps im App Store vermutlich erfolgreich verkauft: Es gibt einfach zu viele Windows-Anwender, die durch Viren-Attacken schon mal richtigen Ärger hatten. Vermutlich um auch diese Anwender zu überzeugen, verbannte Apple die Antivirensoftware aus dem App Store: Allein ihre Existenz widersprach schließlich dem Versprechen, iOS sei ein sicheres Betriebssystem. Dass dies so nicht stimmt, haben allerdings Angreifer wie die NSO Group mit ihrer Spyware Pegasus bewiesen . Aber auch gegen diese Spyware würde ein iOS-Scanner wohl nicht schützen, zu raffiniert sind diese Tools.

Alternative Tools statt Antivirenprogrammen

Patrick Wardle ist ein renommierter Sicherheitsexperte für Mac-Sicherheit, statt einer Antivirensoftware empfiehlt er mehrere von ihm entwickelte Sicherheitstools . Das ist im Prinzip eine gute Lösung, da sich mit diesen Tools Schadsoftware gut aufspüren lässt. Auch der Autor nutzt regelmäßig einige dieser Tools wie Rei Key und vor allem das Analysetolol Knock Knock. Rei Key etwa prüft das System auf Keylogger, mit Knock Knock kann man das System auf verdächtige Hintergrundprogramme prüfen und so Malware aufspüren. Das Problem: Es handelt sich um Tools, die weit mehr Vorwissen erfordern als eine übliche Antivirensoftware. Ein Tool wie Knock Knock ist erklärungsbedürftig und wohl eher für erfahrene Anwender geeignet. Dass Wardle mittlerweile dreizehn unterschiedliche Spezialtools bereitstellt, macht es für Einsteiger ebenfalls nicht einfacher. Eine Antivirensoftware kann ein Anwender dagegen installieren und muss sich nicht weiter kümmern – und wird über Probleme automatisch informiert.

Quelle: https://www.macwelt.de/ratgeber/Warum-Sie-ein-Antivirus-Programm-fuer-den-Mac-brauchen-11287041.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=0&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

10) Google Maps: Neue Routen-Funktion hilft euch, Sprit und somit Geld zu sparen

Wer gerne und viel mit dem Auto fährt, wird mit hohen Preisen für Benzin und Diesel konfrontiert. Google reagiert auf die Entwicklung und integriert in Google Maps eine Funktion, mit der ihr Geld sparen könnt, indem ihr eine Route fahrt, die weniger Sprit verbraucht. Das kann auch für E-Autos eine gute Option sein.

Google Maps führt Navigation zum Sparen von Sprit ein

Manchmal muss man nur eine leicht veränderte Strecke fahren, um spürbar Sprit zu sparen. Mithilfe von künstlicher Intelligenz und Miteinberechnung von vielen Faktoren startet Google jetzt auch in Deutschland eine neue Routen-Navigation, die euch in **Google Maps eine Spritspar-Route vorschlägt**. Ihr könnt über die erweiterte Anzeige direkt auf Basis eurer Route sehen, wie viel Sprit und somit Geld ihr sparen würdet, wenn ihr eine andere Route fahrt und wie viel mehr Zeit das in Anspruch nehmen würde. Wie das funktioniert, zeigt Google in diesem Video:

Anmerkung der Redaktion: Das Video kann unter dem u.g. Link abgerufen werden

Ihr bekommt zukünftig also weiterhin die grauen Routen als alternative Wege angezeigt, **zusätzlich jetzt aber auch ein kleines grünes Blatt eingeblendet**, das zeigt, dass diese Route besonders sparsam gefahren werden kann. Gleichzeitig könnt ihr euch dann auch ansehen, wie viel Sprit im Vergleich zur anderen Route gespart werden kann und ob euch das die Zeit, die ihr dafür vielleicht mehr braucht, wert wäre.

Da Google Maps in Echtzeit den ganzen Verkehr beobachtet und analysiert, könnt ihr zu unterschiedlichen Zeiten auch andere Routen angezeigt bekommen, selbst wenn ihr eigentlich immer das gleiche Ziel habt. Haltet ihr euch an die Route, könnt ihr **über das Jahr gerechnet durchaus viel Geld sparen**. Google will damit natürlich auch die Umwelt schonen und den CO_2-Ausstoß reduzieren.

Neue Funktion ab sofort in Deutschland verfügbar

In den USA ist die neue Funktion schon vor einiger Zeit an den Start gegangen und wurde in Google Maps freigeschaltet. Ab sofort ist die Funktion auch in Deutschland verfügbar. Sie wird in den kommenden Wochen in Google Maps bei allen Nutzerinnen und Nutzern auftauchen, wenn ihr eine Route plant. Damit dürften zukünftig nicht nur Verbrenner Geld sparen, sondern auch E-Autos Energie, wenn die effizienteste Route gefahren wird. In den Einstellungen könnt ihr nämlich **zwischen den Antriebsarten eures Autos wählen.**

Quelle: https://www.giga.de/news/google-maps-neue-routen-funktion-hilft-euch-sprit-und-somit-geld-zu-sparen/

11) Der Federtrick – Mit einem Handgriff den Kabelbruch verhindern

Nie wieder Kabelbruch: Mit einem einfachen Trick verlängern Sie die Haltbarkeit Ihrer Ladegeräte enorm. Dafür benötigen Sie nur eine Kugelschreiberfeder.

Abgeknickte Stellen und ständiges enges Aufrollen – es gibt zahlreiche Praktiken, die die Haltbarkeit von Ladekabeln verringern. Um einen Kabelbruch zu verhindern, gibt es eine simple Methode: den sogenannten Federtrick.

Wie der Trick geht, sehen Sie oben im Video.

Dabei wird die kritische Stelle am Kabel mit einer Feder aus einem Kugelschreiber verstärkt. Meist ist das die Stelle, an der das Kabel endet – entweder am Ladegerät oder am Stecker, der mit dem Handy, Notebook oder Fernseher verbunden wird.

So geht's:

- Schrauben Sie den Kugelschreiber auf und entnehmen Sie die Feder, die sich meist am unteren Teil der Mine befindet.
- Wickeln Sie die Feder um das Kabel, das Sie verstärken wollen. Dafür sollten Sie die Feder an einem Ende etwas aufbiegen, dadurch geht es leichter.
- Prüfen Sie danach, ob die Feder straff sitzt. Sollte Sie sich einfach hin und her schieben lassen, ist die Feder zu groß und könnte verrutschen. In dem Fall sollten Sie eine kleinere Feder nehmen.

Anmerkung der Redaktion: Das Video kann unter dem u.g. Link abgerufen werden

Quelle: https://www.t-online.de/digital/computer/hardware/id_100043802/der-feder-trick-so-gehen-ihre-ladekabel-nicht-mehr-kaputt.html

12) Ist schnell aktiviert: Praktische FritzBox-Funktion spart bares Geld

Internet-Router wie die FritzBox von AVM sind meist Tag und Nacht aktiv und verbrauchen dadurch pausenlos Strom. In vielen FritzBoxen versteckt sich allerdings eine Funktion, mit der Sie den Stromverbrauch des Routers bequem reduzieren können. Was Sie dafür tun müssen, erklären wir Ihnen hier. Diese und weitere clevere Funktionen der FritzBox sehen Sie im Video.

Um zu Hause Strom zu sparen, gibt es viele verschiedene Ansätze. Vor allem Geräte, die Sie nur selten oder zu bestimmten Zeiten verwenden, die aber trotzdem rund um die Uhr laufen, bieten sich an. Allerdings lässt sich nicht jedes davon einfach ausschalten; so muss zum Beispiel der Kühlschrank natürlich auch nachts mit derselben konstanten Temperatur laufen wie am Tag, damit die Lebensmittel frisch bleiben.

Anders sieht es aber zum Beispiel mit Internet-Routern aus. Viele Menschen nutzen das Internet nur tagsüber und abends, nicht aber nachts. Während dem Schlafen läuft der Router meist, ohne dass das WLAN überhaupt benutzt wird.
Ganz abschalten kann sich Ihre FritzBox zwar nicht; um Energie und damit bares Geld zu sparen, können Sie bei vielen FritzBoxen und auch anderen modernen Routern aber eine Zeitschaltung aktivieren, in der das WLAN-Signal zu bestimmten Zeiten abgeschaltet wird, und somit bequem Strom sparen.
Lesetipp: Praktisch für FritzBox-Nutzer: So einfach verbessern Sie Qualität & Reichweite Ihres WLANs

Mit der FritzBox Strom sparen - so klappt's

Gehen Sie dafür einfach in die **Einstellungen** Ihrer FritzBox und wählen Sie die Reiter **WLAN > Zeitschaltungaktivieren**.

Hier können Sie nun Ihrem persönlichen Tagesablauf entsprechend einzelne Wochentage und Zeitspannen einstellen, in denen das WLAN abgeschaltet ist. Allem voran bietet es sich natürlich an, das WLAN über Nacht in einem Zeitfenster zu deaktivieren, in dem Sie und alle anderen Nutzer des WLAN-Zugangs schlafen.
Was Sie jedoch beachten sollten: Geräte, die sonst mit dem WLAN verbunden sind, sind das dann über Nacht natürlich nicht mehr. Das kann für etwaige Updates zum Beispiel hinderlich sein. Haben Sie diese Geräte also im Blick, stoßen die die Updates manuell an oder stellen Sie ein, dass die Geräte nur im WLAN updaten sollen.
Die FritzBoxen von AVM sind sehr populär; viele Nutzer beschränken den Einsatz jedoch auf die Basisfunktion einer stabilen Internetverbindung. Dabei bieten die AVM-Router eine ganze Reihe praktischer Funktionen für das eigene Heimnetz an: Die besten Features stellen wir Ihnen in unserem großen FritzBox Feature-Artikel vor.

Quelle:https://www.chip.de/news/Ist-schnell-aktiviert-Praktische-FritzBox-Funktion-spart-bares-Geld_183798476.html

13) Tipps für den Messenger – WhatsApp-Kniffe, die kaum jemand kennt

Kostenlos mit Freunden chatten und Gruppenchats für die Familie einrichten – klar, das alles geht mit WhatsApp. Der Messenger kann aber noch viel mehr.

WhatsApp veröffentlicht immer wieder neue Funktionen. Diese Funktionen, die Anfänger und Gelegenheitsnutzer leicht übersehen, sind eher unbekannt:

Sieben nützliche WhatsApp-Kniffe

1. WhatsApp auf Computer nutzen

Wenn man sowieso gerade am Computer sitzt, lassen sich WhatsApp-Nachrichten viel schneller über die PC-Tastatur eintippen. Dafür gibt es zwei Möglichkeiten: Entweder lädt man sich die Desktop-App für Mac oder Windows hier herunter. Oder man geht auf web.whatsapp.com, um direkt im Web-Browser zu chatten. Im Browser von t-online.de gibt es seit Version 7.47 sogar oben rechts einen eigenen Button dafür.

In dem Fenster erscheint zunächst ein QR-Code, den man mit der Kamera des Smartphones scannen muss, um den Computer mit der Handy-App zu synchronisieren. Android-Nutzer tippen dazu auf das App-Menü (die drei Punkte oben rechts) und dann auf "WhatsApp Web" und richten Sie die Kamera auf das Symbol. Das Handy muss mit dem Internet verbunden sein. Kurz darauf öffnet sich das Chatfenster mit all Ihren gewohnten Kontakten und den bisherigen Chatverläufen. Wenn Sie fertig sind, vergessen Sie nicht, sich wieder abzumelden.

Auf iPhones finden Sie den Scanner für den QR-Code, indem Sie unten rechts auf "Einstellungen" und dann auf "Verknüpfte Geräte" tippen. Hier tippen Sie dann auf "Gerät hinzufügen".

2. Direkt auf Dateien auf dem Computer zugreifen

Es müssen nicht immer Fotos sein: Über WhatsApp lassen sich auf iOS und Android beliebige Dateien mit einer Größe von bis zu 100 Megabyte verschicken. Das kann der Lieblingssong sein, ein Word-Dokument, die Präsentation fürs nächste Meeting oder ein Kontakt aus dem Telefonbuch.

Unter Android einfach auf das kleine Büroklammer-Symbol im Chat-Fenster drücken und es öffnen sich alle Optionen. Beim iPhone tippt man auf das "+"-Zeichen wählt dann "Dokument" Durch die Web-Browser-Anwendung kann man so auch Dateien vom eigenen Computer hochladen und anderen Leuten direkt aufs Handy schicken.

3. Enge Freunde auf den Startbildschirm hinzufügen

Für Chatpartner, mit denen man besonders häufig schreibt, bietet sich unter Android ein Shortcut für den Startbildschirm des Smartphones an. Öffnen Sie dazu den Chat der Person, gehen Sie auf die Einstellungen und dann auf "**Mehr**" und "**Verknüpfung hinzufügen**", um eine Verknüpfung anzulegen. Das kleine Symbol wird zunächst automatisch an der nächsten freien Stelle auf dem Startbildschirm abgelegt und lässt sich per "drag and drop" (Symbol kurz gedrückt halten) platzieren. Auf iPhones besteht diese Möglichkeit nicht.

4. Nachrichten merken

Wenn man sich Nachrichten für später merken und leicht wieder finden will, empfiehlt es sich, sie mit einem Sternchen zu markieren. So geht es: Etwas länger auf die Nachricht drücken, bis sich ein Menü öffnet. Man kann auch mehrere Nachrichten hintereinander markieren und gesammelt mit einem Sternchen versehen.

5. Erfahren, wie viel Zeit zwischen Zustellung und Lesen einer Nachricht vergangen ist

Zwei graue Häkchen hinter eine Nachricht signalisieren, dass sie dem Empfänger zugestellt wurde. Sobald er sie auch gelesen hat, färben sie sich blau. Doch wie viel Zeit ist vergangen, bis der Empfänger sie geöffnet hat? Das findet man heraus, indem die Nachricht gedrückt hält, dann auf die drei kleinen Punkte rechts oben drückt und hier auf "**Info**". Dort steht dann der jeweilige Zeitpunkt, wann die Nachricht empfangen und wann sie gelesen wurde. Auf iPhones muss man die Nachricht dafür nach links wischen.

6. Im Gruppenchat zitieren

Je mehr Menschen in einer Gruppe miteinander kommunizieren, desto schwieriger wird es, der Unterhaltung zu folgen. Übersichtlicher wird es mithilfe der "Zitieren"-Funktion. Dazu Nachrichten gedrückt halten und im Kontextmenü den Pfeil nach links (Antworten/Reply). Die ursprüngliche Nachricht wird dann Ihrer Nachricht hinzugefügt. So weiß jeder, worauf sich die Antwort bezieht und es kommt ein wenig Ordnung in das Chaos eines Gruppenchats.

7. Broadcast statt Gruppenchat

In einem Gruppenchat reden alle durcheinander und jeder kann sehen, was besprochen wird. Mit der Broadcast-Funktion hingegen lassen sich Massenbotschaften an das gesamte Telefonbuch oder ausgewählte Kontakte verschicken, die Antworten aber bleiben privat. Für den Empfänger sieht es wie eine ganz normale persönliche Nachricht aus. Dass die Botschaft zeitgleich auch an viele andere Empfänger ging, weiß nur der Absender. Das ist zum Beispiel dann praktisch, wenn man viele Leute zu einer Party einladen will, die sich untereinander nicht kennen.

Die Broadcast-Funktion findet sich auf Android-Geräten im Menü oben rechts. Hier einfach auch die drei Punkte tippen, dann auf "Neuer Broadcast". Auf iPhones findet man diese Option ganz oben im Chat-Menü, neben dem Punkt "Neue Gruppe".

8. Text formatieren

Nicht nur Emojis können helfen, Geschriebenes zu betonen. WhatsApp erlaubt es auch, den Text zu formatieren. Um Worte fett zu schreiben, müssen sie zum Beispiel in Sternchen (*) gesetzt werden. Ein Unterstrich vor und hinter dem Wort lassen es kursiv erscheinen. Ein Wort durchstreichen geht mit dem Ungefähr-Zeichen (~). Aus *fett* macht WhatsApp also **fett**, aus _kursiv_ wird *kursiv.* Die Zeichen lassen sich auch kombinieren zum Beispiel so: *_fett und kursiv_* wird zu ***fett und kursiv***. Probieren Sie es aus!

Diese Funktion zu kennen ist auch praktisch, um Scherzmeldungen oder Spam zu erkennen. Es kursieren zum Beispiel WhatsApp-Kettenbriefe, die dem Nutzer vorgaukeln wollen, es handle sich um Fehlermeldungen. Profinutzer wissen natürlich: Jeder kann solche Textnachrichten selbst erstellen.

9. Kreative Status-Updates für den engen Freundeskreis

Das hat sich WhatsApp von Snapchat abgeguckt: Macht man ein Bild in der App, kann man es anschließend mit verschiedenen Filtern bearbeiten, mit Emojis oder Zeichnungen verzieren und vieles mehr. Ähnlich wie in einem sozialen Netzwerk lassen sich diese Werke anschließend in Form von Statusmeldungen zur Schau stellen. Diese verschwinden nach 24 Stunden automatisch wieder.

Quelle: https://www.t-online.de/digital/handy/id_83059668/whatsapp-9-tipps-die-kaum-jemand-kennt.html

14) Wie Sie Ihr iPhone richtig laden

Schaden Sie dem Akku Ihres iPhones, wenn Sie es zu häufig oder zu lange laden? Wir fassen die besten Tipps zusammen, wie Sie den Akku Ihres iPhones nicht zu schnell abnutzen.

Der Akku eines Smartphones wird mit der Zeit immer schlechter. Hält Ihr iPhone anfangs noch locker einen Tag durch, wird es schon nach zwei Jahren deutlich schwieriger, ohne Zwischenladen durch den Tag zu kommen.

Teilweise liegt das daran, wie Sie Ihr Smartphone verwenden. Je mehr Apps Sie installieren, je

mehr Datenmüll sich ansammelt, je mehr Benachrichtigungen eingehen, desto stärker wird die Batterie Ihres iPhones belastet. Solange wir keine bessere Technologie als Lithium-Ionen-Akkus haben, müssen wir lernen, sie möglichst schonend zu verwenden.

Wie alle Batterien verschleißen Smartphone-Akkus mit der Zeit und können immer weniger Ladung aufnehmen. Üblicherweise haben sie eine Lebenszeit von drei bis fünf Jahren – oder 500 bis 1.000 Ladezyklen –, doch bereits ein drei Jahre alter Akku hat eine merklich kürzere Laufzeit als ein neuer.

Drei Faktoren haben die größte Auswirkung auf die Gesundheit von Lithium-Ionen-Akkus:

- Anzahl der Ladezyklen
- Wärme
- Alter

Wenn Sie unsere Tipps zur Pflege Ihres Akkus befolgen, sollte Ihr Akku allerdings deutlich länger halten.

Wann sollten Sie Ihr iPhone laden?

Die Faustregel ist, den Akkustand zwischen 30 und 90 Prozent zu halten. Laden Sie Ihr iPhone auf, wenn es unter 50 Prozent fällt, ziehen Sie es aber wieder ab, bevor es 100 Prozent erreicht. Aus diesem Grund ist es nicht unbedingt die beste Idee, Ihr Smartphone über Nacht zu laden.

Der letzte Abschnitt von 80 bis 100 Prozent belastet den Akku immens und lässt ihn daher schneller altern. Vielleicht ist es also besser, Ihr iPhone beim Frühstück oder bei der Arbeit zu laden. Es ist nicht katastrophal, wenn Sie Ihr iPhone voll aufladen, aber Sie sollten es vermeiden, da jedes Mal der Akku ein kleines bisschen altert.

Gleichermaßen sollten Sie vermeiden, dass die Batterie unter 20 Prozent fällt. Lithium-Ionen-Akkus mögen Füllstände unterhalb der 20-Prozent-Marke genauso wenig wie den Bereich zwischen 80 und 100 Prozent. Sie sollten den unteren Bereich daher als Notreserve für lange Tage betrachten und Ihr Handy aufladen, sobald die Benachrichtigung über geringen Akkustand auftaucht.

Kurz gesagt: Lithium-Ionen-Akkus geht es im mittleren Bereich am besten. Vermeiden Sie am besten zu hohe oder zu geringe Akkustände. Laden Sie Ihr iPhone lieber mehrmals täglich etwas auf, statt einmal am Tag komplett.

Wenn Sie nicht selbst darauf achten können oder wollen, können Sie auf Ihrem iPhone in der App „Kurzbefehle“ eine Benachrichtigung einrichten, die Sie auf hohen oder niedrigen Batteriestatus hinweist. Das können Sie im Tab „Automation“ mithilfe einer persönlichen Automation tun. Der Eintrag für den Batteriestatus befindet sich in der Auswahl weiter unten.

Mit iOS 13 hat Apple außerdem „Optimiertes Laden“ eingeführt. Diese Funktion soll mithilfe einer KI helfen, die Lebensdauer Ihrer iPhone-Batterie zu erhöhen, indem sie den Ladevorgang auf 80 Prozent begrenzt und basierend auf Uhrzeit-, Positions- und Nutzungsdaten lernt, wann der Akku auf 100 Prozent aufgefüllt werden muss. Im Normalfall müssen Sie sich keine Sorgen darum machen, da die Funktion standardmäßig aktiviert ist. Um den Status zu überprüfen, öffnen Sie „Einstellungen > Batterie > Batteriezustand“. Ist der Schalter grün, ist alles in Ordnung. Ist er grau, sollten Sie ihn lieber wieder umlegen.

iPhone schnell aufladen – schadet es dem Akku?

Wie die meisten modernen Smartphones unterstützen auch alle iPhones ab dem iPhone 8 schnelles Aufladen – auch Fast Charging genannt. Benötigt wird dafür mindestens ein 18-Watt-Netzteil, ab dem iPhone 12 müssen es sogar mindestens 20 Watt Leistung sein, schreibt Apple auf der offiziellen Support-Seite .

Die gute Nachricht ist, dass schnelles Aufladen selbst dem Akku nicht schadet. Problematisch ist die Wärme, denn hier verhält es sich wie beim Akkustand: zu wenig ist schlecht, zu viel auch. Am wohlsten fühlt sich ein Lithium-Ionen-Akku zwischen 20 und 30 Grad Celsius. Je höher die Ladeleistung, desto höher die Wärmeentwicklung. Kurze Ausreißer in höhere Temperaturbereiche sind in Ordnung, allerdings sollten Sie aufpassen, dass Ihr iPhone nicht über längere Zeit heiß läuft.

Insbesondere im Sommer ist Ihre Elektronik ohnehin schon höheren Temperaturen ausgesetzt. Sollten Sie Ihr iPhone beispielsweise doch über Nacht laden, legen Sie es lieber nicht unters Kissen, wo überschüssige Wärme nur langsam entweichen kann. Im Sommer kann es sich unter Umständen lohnen, in „cooles“ Zubehör fürs iPhone zu investieren.

Induktives Laden – schädlich oder nicht?

Um induktives Laden – auch Wireless Charging oder kabelloses Laden genannt – ranken sich genauso viele Mythen wie ums Schnellladen. Häufig heißt es, induktives Laden sei schädlicher als konventionelles, kabelgebundenes Laden, schließlich entstehe dabei mehr Wärme. Im Kern ist diese Annahme nicht falsch: Die Spule im Inneren Ihres iPhones wird tatsächlich spürbar warm. Da sie sich meistens in unmittelbarer Nähe des Akkus befindet, überträgt sie die Wärme natürlich auch auf ihn.

Der Knackpunkt ist allerdings, dass die Qi-Charging-Spezifikation voraussetzt, dass Qi-zertifizierte Geräte die Ladeleistung senken müssen, wenn sie zu warm werden. Insofern überschreiten Qi-Ladegeräte beim Ladevorgang nie kritische Temperaturwerte. Sofern Sie also das richtige Ladegerät verwenden, ist induktives Laden nicht schädlicher als konventionelles Laden. Von sich aus wird der Akku beim induktiven Laden übrigens auch nicht warm – das kommt von der Spule.

Das richtige Ladegerät

Auf der sicheren Seite bewegen Sie sich, wenn Sie Ihr iPhone mit einem Apple-zertifizierten Ladegerät und Lightning-Kabel laden. Auf der wirklich sicheren Seite bewegen Sie sich, wenn Sie nur mit einem offiziellen Apple-Ladegerät laden. Tunlichst vermeiden sollten Sie hingegen billige No-Name-Ladegeräte und Kabel von eBay und Amazon, da sie häufig nicht die Qualitätsanforderungen von Apple erfüllen. Unter Umständen kann es zu Schäden kommen, die nicht von der Garantie abgedeckt werden. Wenn Sie auf kabelloses bzw. induktives Laden setzen, sollten Sie auf Geräte mit Magsafe oder Qi-Zertifizierung setzen. Wie oben erwähnt, funktioniert die Schnellladefunktion allerdings erst ab einer bestimmten Leistung. Eine Auswahl kompatibler Ladegeräte und Powerbanks hat Thomas Bergbold erst kürzlich getestet .

Quelle: https://www.macwelt.de/ratgeber/Wie-Sie-Ihr-iPhone-richtig-laden-11280955.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3700477&pm_cat%5B0%5D=Hardware+allgemein&pm_cat%5B1%5D=Mobile+OS&pm_cat%5B2%5D=Apple&pm_cat%5B3%5D=iOS&pm_cat%5B4%5D=Mobile+Client&pm_cat%5B5%5D=Mobile+Plattformen&pm_cat%5B6%5D=Mobilfunk&pm_cat%5B7%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

Allgemeines:

1) Mietrückstand – Miete nicht gezahlt – wann darf der Vermieter kündigen?

Wenn die Miete nicht oder nicht pünktlich gezahlt wird, darf der Vermieter seinem Mieter kündigen – und zwar fristlos. Betroffene Mieter können die sofortige Kündigung in der Regel noch abwenden, wenn sie einiges beachten.

Das Wichtigste im Überblick

- Bei welchem Mietrückstand darf der Vermieter kündigen?
- Was mache ich, wenn ich die Miete nicht bezahlen kann?
- Kann mein Vermieter mich einfach rausschmeißen?

Der Termin rückt immer näher, aber Ihr Konto wird immer leerer: Wenn Sie Ihre Miete mal nicht bezahlen können, ist das noch kein Grund für eine Kündigung. Allerdings gilt: Lange zögern sollten Sie nicht, sondern suchen Sie das Gespräch mit Ihrem Vermieter.

Doch ab wann kann er mich wirklich rausschmeißen? Und welche Rechte habe ich als Mieter in einem solchen Fall? t-online beantwortet die wichtigsten Fragen zu einem Mietrückstand.

Bei welchem Mietrückstand darf der Vermieter kündigen?

Die gesetzlichen Regelungen zum Schutz der Vermieter sind relativ eindeutig formuliert. So gibt es drei Regeln, die zu einer "außerordentlichen fristlosen Kündigung" führen können.

- Zahlt ein **Mieter seine Miete zweimal hintereinander** auch nur einen Tag zu spät, darf der Vermieter das Mietverhältnis fristlos kündigen.
- Eine fristlose Kündigung ist auch möglich, wenn der Mieter **zwei Monate hintereinander nur unvollständig Miete** zahlt und sich der Fehlbetrag auf **mehr als eine Monatsmiete** summiert.
- Wenn der Rückstand über einen längeren Zeitraum **ganze zwei Monatsmieten** beträgt, droht ebenfalls die fristlose Kündigung.

Einen Mietrückstand kann der Mieter beispielsweise auch durch offene **Nebenkostennachzahlungen** anhäufen (diese Fristen sollten Sie daher kennen). Summieren sich offene Nebenkostennachzahlungen oder ungerechtfertigte Mietminderungen auf insgesamt zwei Monatsmieten, kann der Vermieter dem Mieter fristlos kündigen. Dabei kommt es nicht auf den Zeitraum an, in dem sich die offenen Rückstände angesammelt haben.

- **Alles korrekt?** Wie Sie Ihre Nebenkostenabrechnung prüfen
- **Mietrecht:** Wann Mieterhöhungen nicht zulässig sind

Wie muss eine fristlose Kündigung gestaltet sein?

Damit die fristlose Kündigung gültig ist, muss Ihr Vermieter **den Grund für die fristlose Kündigung** anführen – also den **Mietrückstand**. Womöglich wird er auch deutlich machen, wie viel Miete Sie ihm genau schulden.

Außerdem muss die fristlose Kündigung von Ihrem Vermieter **unterschrieben** sein. Ihr Vermieter wird auch schreiben, dass Sie die Wohnung zu räumen haben und ihm die Wohnungsschlüssel übergeben müssen. Dazu wird er Ihnen wahrscheinlich einen Termin

vorschlagen.

Beachten Sie: Ziehen Sie nach einer fristlosen Kündigung nicht aus, kann Ihr Vermieter eine **Räumungsklage** anstreben (siehe unten).

Gut zu wissen: Der Vermieter darf bei einem Mietrückstand nicht auf die Mietkaution zurückgreifen. Das ist erst bei einer Räumungsklage möglich.

- **Mietkaution:** Die wichtigsten Punkte schnell erklärt

Was mache ich, wenn ich die Miete nicht bezahlen kann?

Im Prinzip können Mieter die Kündigung noch verhindern. Sind die Zahlungsrückstände bereits entstanden, sollten Sie das Gespräch mit Ihrem Vermieter suchen.

So könnten Sie versprechen, die Miete nachzuzahlen und gegebenenfalls versuchen, einen Zahlungsaufschub oder eine Ratenzahlung zu vereinbaren. Was Sie noch tun können:

- **Mieterverein:** Wenn es einen Mieterverein gibt, sollten Sie sich zunächst an diesen wenden. Dieser kann Sie bei Problemen mit Ihrem Vermieter unterstützen.
- **Sozialbehörden:** Als Empfänger von Arbeitslosengeld können Sie auch das Jobcenter einschalten, das Ihre Mietschulden gegebenenfalls übernimmt – oder Ihnen ein Darlehen gewährt.
- **Wohngeld:** Wenn Sie nicht arbeitslos sind und kein Hartz IV erhalten, aber nur über ein geringes Einkommen verfügen, haben Sie womöglich Anspruch auf Wohngeld. Lassen Sie sich von der Wohngeldbehörde bei Ihrer Stadt- oder Kreisverwaltung beraten. Wie Sie Wohngeld beantragen, lesen Sie hier.

Gut zu wissen: Grundsätzlich haben Mieter das Recht, die Miete zu mindern, wenn es einen nachvollziehbaren Mangel gibt. Doch wer die Miete zu stark mindert, setzt seinen Mietvertrag aufs Spiel. Messlatte für den kündigungsrelevanten Rückstand ist die vereinbarte Miete, nicht die geminderte, entschied der Bundesgerichtshof (AZ.: VIII ZR 193/16).

- **Miete teilen:** Worauf Sie bei einer Untervermietung achten sollten
- **Mietkautionsversicherung:** Das sind die Vor- und Nachteile für Mieter

Ausreden wie "Ich dachte, die Miete wäre zur Monatsmitte fällig" lässt der Gesetzgeber hingegen nicht gelten. In jedem Mietvertrag ist klar geregelt, zu welchem Zeitpunkt die Miete fällig wird.

Bereits unpünktliche Zahlungen gelten als **"gravierende Pflichtverletzungen"** seitens des Mieters. Sie sind dazu verpflichtet, sich ohne ständige Abmahnungen des Vermieters zu informieren, wann die Miete fällig ist – und auf welches Konto diese überwiesen werden muss.

Flattert eine **Mahnung mit der Zahlungsaufforderung** der rückständigen Miete ins Haus, sollten Sie allerspätestens das Gespräch mit Ihrem Vermieter suchen (siehe oben).

Achtung: Selbst wenn säumige Mieter ihrer Zahlungspflicht nachkommen und den offenen Rückstand zahlen, sind sie nicht vor einer ordentlichen Kündigung des Mietverhältnisses gefeit. Das heißt, sie müssen sich dann zwar nicht sofort, aber innerhalb der gesetzlichen Frist eine neue Bleibe suchen.

Können Mietschulden verjähren?

Ja. Mietschulden unterliegen der gesetzlichen Verjährungsfrist von drei Jahren nach § 195 BGB. Innerhalb dieser Frist hat der Vermieter Zeit, seinen Anspruch auf die rückständige Miete samt Verzugszinsen gerichtlich geltend zu machen.

- **Indexmiete:** Warum das Wohnen so immer teurer wird

Die Verjährungsfrist beginnt mit Ende des Jahres, in dem der Anspruch entstand oder dieser vom Mietrückstand erfahren hat oder hätte erfahren müssen.

Kann mein Vermieter mich einfach rausschmeißen?

Nein. Einfach so geht das nicht. Es muss ein wichtiger Grund vorliegen, etwa dass Sie die Miete nicht bezahlt haben (siehe oben). Doch in der Regel schickt Ihr Vermieter Ihnen eine **Mahnung** – juristisch verpflichtet dazu ist er allerdings nicht.

Sollten Sie darauf nicht reagieren, kann Ihr Mieter Ihnen kündigen. Kommt der Mieter der Aufforderung zum Auszug nicht nach, folgt die **Räumungsklage**.

- Ohne Makler: Wohnung mieten von privat – diese Fehler sollten Sie vermeiden
- Umlagefähige Nebenkosten: Was Sie als Mieter nicht zahlen müssen
- Kleinreparaturen oder Tierhaltung: Diese Klauseln in Mietverträgen sind unzulässig

Bei einer fristlosen Kündigung kann der Mieter seine Schulden zudem noch bis zu zwei Monate nach Zustellung der Räumungsklage bezahlen. Dann folgt keine fristlose Kündigung – mit einer Einschränkung: Wenn in den vergangenen zwei Jahren schon einmal entsprechende Mietrückstande angefallen sind, ist das nicht mehr möglich.

Quelle: https://www.t-online.de/finanzen/immobilien-wohnen/mietrecht-wohnen/id_48751322/mietrueckstand-miete-nicht-gezahlt-darf-vermieter-kuendigen-.html

2) Einweg E-Zigaretten: Dümmster Trend seit langem – so schädlich sind Wegwerf-Vapes

Wegwerf-E-Zigaretten sind im Trend. Bei genauerer Betrachtung zeigt sich aber: Sie sollten verboten werden. Der Grund.

Vor allem bei jungen Menschen sind aktuell Einweg E-Zigaretten im Trend. Nicht zuletzt auch, weil prominente Streamer auf Twitch dafür die Werbetrommel rühren. In aller Munde ist etwa die "Elf Bar", die mit coolen Farben und originellen Geschmacksrichtungen vor allem eine jüngere Zielgruppe anspricht. Es gibt aber auch viele andere Hersteller, die in diesen boomenden Markt drängen.
Bei genauerer Betrachtung entpuppen sich solche Wegwerf-E-Zigaretten aber als extrem umweltschädliche Produkte. Der einfache Grund: In den für rund 10 Euro erhältlichen E-Zigaretten stecken meistens Lithium-Ionen-Akkus, die dann schließlich gemeinsam mit der E-Zigarette im normalen Hausmüll landen, wo sie eigentlich nicht hingehören.

Darauf machen die Hersteller solcher Einweg-E-Zigaretten zwar aufmerksam, aber nicht alle Verbraucher dürften sich dran halten. Laut einer aktuellen Studie aus Großbritannien, wo der Einweg-E-Zigaretten-Trend schon früher begann, landen über 50 Prozent der Wegwerf-E-Zigaretten im normalen Müll. Allein die in einem Jahr in Großbritannien weggeworfenen Einweg-E-Zigaretten würden ausreiche, um 1.200 Batterien für Elektrofahrzeuge herzustellen.

Massive Verschwendung von Akkus durch Wegwerf-E-Zigaretten

In der "Elf Bar 600" steckt beispielsweise laut Hersteller ein 550-mAh-Akku. Nach etwa 600 Zügen landet damit jedes Mal ein eigentlich wiederverwertbarer Akku im Müll. Zum Vergleich: Im Galaxy S22 steckt ein 3.700-mAh-Akku. Mit dem Wegwerfen von 7 Elf Bars wird damit eine Akkukapazität einfach in den Müll weggeschmissen, die für den jahrelangen Einsatz eines Galaxy S22 ausreichen würde.

Ganz zu schweigen von der Verschwendung der wertvollen Seltenen Erden, die für die Herstellung der Akkus benötigt werden. Allein in Deutschland werden jeden Monat eine hohe sechstellige Anzahl solcher Wegwerf-E-Zigaretten verkauft und damit nach dem Verbrauch wieder weggeschmissen.

Youtuberin weist auf Problematik hin und fordert Verbot von Wegwerf-Vapes

Die reichweitenstarke Youtuberin Alicia Jones hat am Donnerstag ein sehenswertes Video mit dem Titel "Warum Einweg Vapes SOFORT verboten werden müssen" veröffentlicht , in dem sich Jones der Problematik annimmt. In dem Clip weist Jones auch darauf hin, dass es Hinweise darauf gibt, dass in den Liquids der in China hergestellten Einweg-E-Zigaretten auch eher schädliche Stoffe enthalten sein könnten. Jedenfalls gäbe es Berichte von Nutzern, die über einen seltsamen Geschmack und Husten klagen.

Alicia Jones kommt in ihrem Video zu einem Schluss: Bei Mehrweg-E-Vapes sollten die Steuern gesenkt werden und dafür die Wegwerf-E-Zigaretten komplett in Europa verboten werden.

Quelle: https://www.pcwelt.de/news/Einweg-E-Zigaretten-Der-duemmste-Trend-seit-langem-so-schaedlich-sind-Wegwerf-Vapes-11287549.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=0&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) E-Bike und Pedelec: Kaufberatung und Tipps

Immer mehr Menschen kaufen Fahrräder mit Elektroantrieb und geben dafür im Schnitt fast 3.000 Euro aus. Wie unterscheiden sich die Modelle? Wichtige Kriterien sind der Antrieb und die Akku-Kapazität.

Fahrräder mit Elektromotor gehörten schon vor der Corona-Pandemie zum Alltag auf den Radwegen. Doch die Angst vor Ansteckungen in öffentlichen Verkehrsmitteln sowie weniger Möglichkeiten im Freizeitbereich haben Fahrrädern zu einem weiteren Boom verholfen.

Breite Preisspanne bei Pedelecs

Besonders die sogenannten Pedelecs haben sich zum Verkaufsschlager entwickelt. Fast jeder Hersteller hat diese Modelle mit einer Höchstgeschwindigkeit von 25 km/h im Programm. Längst sind nicht mehr nur Senioren damit unterwegs. Für Pedelecs gelten die gleichen Vorschriften wie für Räder ohne Motor: Es gibt keine Helmpflicht, Radwege und öffentliche Verkehrsmittel dürfen genutzt werden. E-Bikes mit einer Höchstgeschwindigkeit über 25 km/h dürfen dagegen nur auf der Straße fahren. Die technischen Details von Pedelecs unterscheiden sich ebenso wie die Preise. Einfache Modelle sind bereits für unter 1.000 Euro zu bekommen, Räder mit aufwendiger Technik und hochwertigeren Komponenten kosten schnell 3.500 Euro und mehr. Auch Preise von rund 6000 Euro sind keine Seltenheit.

Knackpunkt bei E-Bikes: Begrenzte Reichweite

Wie bei allen Elektro-Fahrzeugen gehört die begrenzte Reichweite zu den größten Einschränkungen der Pedelecs. Sie hängt in erster Linie von der Akku-Kapazität und der Motorleistung ab. In der Praxis spielen zudem die gefahrene Geschwindigkeit, die Beschaffenheit von Gelände und Bodenbelag, die gewählte Unterstützung beim Treten sowie das Gewicht des Fahrers entscheidende Rollen. Die im Prospekt angegebene Reichweite von vielfach mehr als 100 Kilometern wird meist nur unter optimalen Bedingungen erzielt. Ein einheitliches Verfahren der Hersteller zur Berechnung der Reichweitenangabe gibt es derzeit

noch nicht. In einer NDR-Stichprobe wurde die angegebene Mindestreichweite von allen Rädern erreicht.

Akku-Anzeige im Auge behalten

Auch schwach aufgepumpte Reifen verringern die Reichweite durch einen erhöhten Rollwiderstand. Wer also eine ausgedehnte Tagestour unternehmen möchte, muss die Akku-Anzeige im Auge behalten und mit dem Strom sparsam umgehen. Ist der Speicher leer, kann der Radler zwar ohne Unterstützung weiterfahren, das Gewicht des Elektroantriebs bremst aber spürbar.

Beim Kauf auf Akku-Kapazität achten

Eine digitale Anzeige am Lenker informiert über Geschwindigkeit, Akkustand und Motorleistung. Bei preisgünstigen Modellen muss man hier häufig Abstriche machen und kann nur die Stufen der Motorsteuerung einstellen. Die meisten Stromspeicher arbeiten mit Lithium-Ionen-Technik. Nach einigen Hundert Ladevorgängen sinkt die Kapazität deutlich. Müssen die Akkus ersetzt werden, kostet das mehrere Hundert Euro. Das sollte besonders beachten, wer überlegt, sich ein gebrauchtes Pedelec zu kaufen. Am längsten halten Akkus, wenn sie stets im Bereich zwischen 20 und 80 Prozent geladen sind. Man sollte sie also nicht ganz leerfahren und auch nicht nach kurzer Nutzung bereits wieder voll laden. Auch extremer Hitze oder Kälte sollte der Akku nicht ausgesetzt werden. Viele Hersteller bieten Akkus mit unterschiedlicher Speicherleistung (gemessen in Wattstunden, kurz Wh) an. Räder im mittleren Preisbereich liegen meist bei 350 bis 500 Wh. Ein größerer Akku erhöht die Reichweite, aber auch den Preis des Rades.

Akku an der Steckdose laden

Zum Laden des Akkus genügt eine gewöhnliche Steckdose. Ein kompletter Ladevorgang dauert jedoch mehrere Stunden. Bei einigen Modellen kann der Akku nicht abgenommen und zum Laden mit in die Wohnung genommen werden. Dann muss es einen Stromanschluss zum Beispiel in der Garage geben. Wer sein Elektrorad längere Zeit nicht nutzt, sollte den Akku ausbauen und ihn etwa halb geladen bei einer Temperatur zwischen 10 – 15 Grad lagern. Niedrige Temperaturen im Winter bekommen den Akkus nicht.

Richtigen Motor wählen: Antrieb per Vorder- oder Hinterrad

Technisch lassen sich drei Antriebsmöglichkeiten unterscheiden:

- Nabenmotor im Vorderrad
- Mittelmotor am Tretlager
- Nabenmotor im Hinterrad

Einfache Modelle setzen auf den Vorderrad-Motor, der allerdings weniger Fahrkomfort bietet als ein Mittelmotor, dessen Kraft über die Kette auf das Hinterrad wirkt. Ein angetriebenes Vorderrad kann auf rutschigem oder weichem Untergrund durchdrehen und das gesamte Fahrrad destabilisieren.

Mittelmotor am beliebtesten

Als günstige Gewichtsverteilung hat sich erwiesen, Motor und Akku in der Mitte des Rades zu platzieren. Daher ist der Mittelmotor derzeit die am häufigsten verkaufte Variante. Das Fahrverhalten entspricht weitgehend dem eines herkömmlichen Rades. In sportlichen Pedelecs kommen vielfach Hinterrad-Motoren zum Einsatz. Sie sind preiswerter und lassen sich mit einer Kettenschaltung mit vielen Gängen kombinieren. Beim Mittelmotor ist das nicht

möglich, er wird meist mit Nabenschaltungen verbunden.

Motorleistung und Drehmoment beachten

Bei allen Antriebs-Varianten darf die Motorleistung eines Pedelecs laut Gesetz 250 Watt nicht übersteigen. Dieser Wert sagt allerdings wenig über die tatsächliche Kraft des Motors aus. Wichtiger ist das Drehmoment, gemessen in Newtonmetern (Nm). Es liegt zwischen etwa 25 und mehr als 60 Nm. Je höher die Zahl, desto kräftiger schiebt der Motor das Rad an. Wer auch am Berg noch gut unterstützt werden möchte, sollte auf mindestens 40 Nm achten.

Scheibenbremsen bieten mehr Sicherheit

Die relativ schweren und schnellen Pedelecs benötigen sichere Bremen. Immer mehr Anbieter setzen statt auf die herkömmlichen Felgenbremsen auf Scheibenbremsen, die besonders bei Nässe kräftiger zupacken. Günstige Varianten funktionieren mit klassischem Bowdenzug, aufwendigere Modelle mit einer Hydraulik, die die Bremsleistung feiner dosiert.

Probefahrt oder Tagestour mit Leihrad

Verbraucherschützer raten dazu, vor dem Kauf eine Probefahrt zu unternehmen. Beim Kauf im Internet ist das schwierig. Und außerdem müssen Kundinnen und Kunden das Rad erst zusammenbauen, bevor sie fahren können. Bei einer Probefahrt sollten sich Radler zunächst vorsichtig mit den Fahreigenschaften eines Elektrorades vertraut machen. In vielen Urlaubsregionen können Interessenten mit einem gemieteten Pedelec (ab etwa 20 Euro) bei einer Tagestour ausgiebig ausprobieren, ob sie künftig stets mit Kraftreserven aus dem Akku unterwegs sein möchten.

S-Pedelecs: Helmpflicht und Versicherungskennzeichen

Wer sich für ein schnelles S-Pedelec entscheidet, dessen Tretunterstützung erst bei einer Geschwindigkeit von 45 km/h abschaltet, muss einen Helm tragen und mindestens einen Führerschein der Klasse AM besitzen. Für diese Fahrzeuge ist ein sogenanntes Versicherungskennzeichen einer Haftpflichtversicherung erforderlich. Sie kostet pro Jahr etwa 50 Euro und ist jeweils bis Ende Februar des Folgejahres gültig. Zudem ist es möglich, für die Fahrzeuge eine Kaskoversicherung abzuschließen, die je nach Tarif für Diebstahl und eigene Schäden aufkommt.

Haftpflicht- und Diebstahlversicherung prüfen

Auch die Nutzer der langsameren E-Bikes bis 25 km/h sollten prüfen, ob ihre Privathaftpflicht-Versicherung bei einem Unfall für verursachte Schäden aufkommt. Im Fall eines Diebstahls springt eventuell die Hausratversicherung ein, ein Blick in die Police klärt die Einzelheiten. Eine Alternative sind spezielle Fahrrad-Versicherungen.

Quelle: https://www.ndr.de/ratgeber/verbraucher/Tipps-zu-E-Bike-Pedelec-und-Elektrofahrrad,ebike123.html

3) Abofallen am Telefon: Welche Rechte haben Verbraucher?

Trickreich versuchen einige unseriöse Firmen, Verbrauchern am Telefon ein Abonnement etwa für Glücksspiele oder Nahrungsergänzungsmittel zu verkaufen. So erkennen Sie den Betrug.

Bei Anruf Abzocke: In den betrügerischen Telefonaten wird oft nicht eindeutig mitgeteilt, dass ein kostenpflichtiges Abo abgeschlossen wird. Behalten Betroffenen anschließend ihre Kontobewegungen nicht im Blick, können große finanzielle Schäden eintreten.
Dabei sind Werbeanrufe ohne vorab geleistete Einwilligung der Angerufenen in Deutschland

unzulässig. Doch immer wieder kommt es vor, dass sich Firmen ohne Einverständnis telefonisch an Verbraucherinnen und Verbraucher wenden.

So funktioniert die Masche der unseriöser Abofallen-Firmen

Die Anrufer verschleiern oft den wahren Hintergrund ihres Anrufs, melden sich zum Beispiel als Meinungsforschungsinstitut. Oder es wird der Eindruck erweckt, dass der oder die Angerufene etwas gewonnen hätte - beispielsweise Probepäckchen für ein Produkt. Manchmal wird ihnen mitgeteilt, dass sie an einem kostenlosen Gewinnspiel-Abo teilgenommen hätten, das jetzt kostenpflichtig sei.

Um an die in Aussicht gestellten Gewinne zu kommen oder Abo-Laufzeiten zu verkürzen, werden die Angerufenen dazu gebracht, in dem Telefonat ihre Bankdaten anzugeben. Die Anrufer nehmen Teile des Telefonats auf. Die Mitschnitte können dann im Anschluss manipuliert werden, sodass sie wie eine mündliche Zustimmung zu einem Vertrag erscheinen.

Wann ist ein am Telefon geschlossener Vertrag rechtsgültig?

Auch ein am Telefon geschlossener Vertrag kann grundsätzlich rechtsgültig sein. Doch dafür müssen eine Reihe von Bedingungen erfüllt sein. Die Anrufer müssen zum Beispiel Kündigungsfristen und Preise nennen und auf das Widerrufsrecht hinweisen. Bei Glücksspielen sieht es allerdings anders aus: Dort kommen Verträge nur durch eine schriftliche Einwilligung des Kunden zustande.

Neuregelungen für Energieversorger und Mobilfunkanbieter

Der Gesetzgeber hat im Juli 2021 für Energie-Versorger eine ganz entscheidende Änderung eingeführt, die telefonische Vertrags-Abschlüsse erschweren. Strom- und Gasanbieter können sich jetzt nur noch in Textform einen Vertrag mit dem Verbraucher bestätigen lassen. Das kann per Post, per Mail oder auch als SMS geschehen.

Ähnliches gilt auch für Mobilfunk-Verträge. Kommt es zu einem Vertrags-Abschluss am Telefon, muss der Anbieter danach unverzüglich in Textform Informationen zur Verfügung stellen und sich den Vertrag in Textform genehmigen lassen. Solange ist der Vertrag in der Schwebe und damit unwirksam. Diese Neuregelung gilt seit Dezember 2021.

Wie kommen Abofallen-Betrüger an Kontaktdaten?

Die Kontaktdaten der Angerufenen beziehen die Firmen häufig von Adresshändlern. Diese wiederum erhalten die Adressen, wenn Verbraucherinnen und Verbraucher an Gewinnspielen teilnehmen und dabei ihr Einverständnis geben, von Werbetreibenden kontaktiert zu werden. Doch nicht immer liegt den Anrufern eine solche Einwilligung vor.

Richtiges Verhalten bei Werbeanrufen

Generell ist ein guter Schutz vor Werbeanrufen, mit der Herausgabe seiner Telefonnummer und anderen persönlichen Daten so sparsam wie möglich zu sein und die Teilnahme an Gewinnspielen zu überdenken.

Bei Werbeanrufen gilt:

- Das Telefonat so schnell wie möglich beenden. Die Aussage: "Kein Interesse" und das Auflegen des Hörers sind ein guter Schutz.
- Möglichst nicht das Wort "Ja" sagen, statt dessen in ganzen Sätzen antworten.
- Keine persönliche Daten herausgeben.
- Die Telefonnummer des Anrufers und den Zeitpunkt des Anrufs notieren. Anschließend

die Bundesnetzagentur informieren.

- Wird die Telefonnummer des Anrufers nicht angezeigt, danach fragen.
- Häufen sich die Anrufe, kann ein Wechsel der Telefonnummer sinnvoll sein.

Hilfe bei unverlangt zugesandter Ware

Wenn Waren zugeschickt werden, ohne dass diese bestellt wurden, können diese Schritte helfen:

- Rechnung nicht bezahlen, Mahnungen und Inkassoschreiben widersprechen.
- Angeblich abgeschlossenen Kauf- oder Abonnementverträgen schriftlich widersprechen.
- Klar darauf hinweisen, dass kein Kaufvertrag zustande gekommen ist. Den angeblichen Vertrag dennoch kündigen.
- Es besteht keine Pflicht, unverlangt zugesandte Ware zurückzuschicken.

Hilfe bei Rechnungen und Lastschrift

Kommen Rechnungen für ein angeblich abgeschlossenes Abonnement oder wird hierfür das Bankkonto belastet:

- Schriftlich Widerspruch einlegen
- Bank kontaktieren, SEPA-Mandat stoppen. Ohne Vorlage einer schriftlichen Einwilligung muss die Bank die Beträge der letzten 13 Monate zurückbuchen
- Regelmäßig Kontobewegungen kontrollieren

Abofallen am Telefon: Hier gibt's Hilfe

Hilfe erhalten Verbraucherinnen und Verbraucher unter anderem bei diesen Anlaufstellen:

- Verbraucherdienst e.V
- Verbraucherschutz.de
- Verbraucherzentrale
- Bundesnetzagentur

Quelle: https://www.ndr.de/nachrichten/netzwelt/Abofallen-am-Telefon-Welche-Rechte-haben-Verbraucher,abofalle128.html

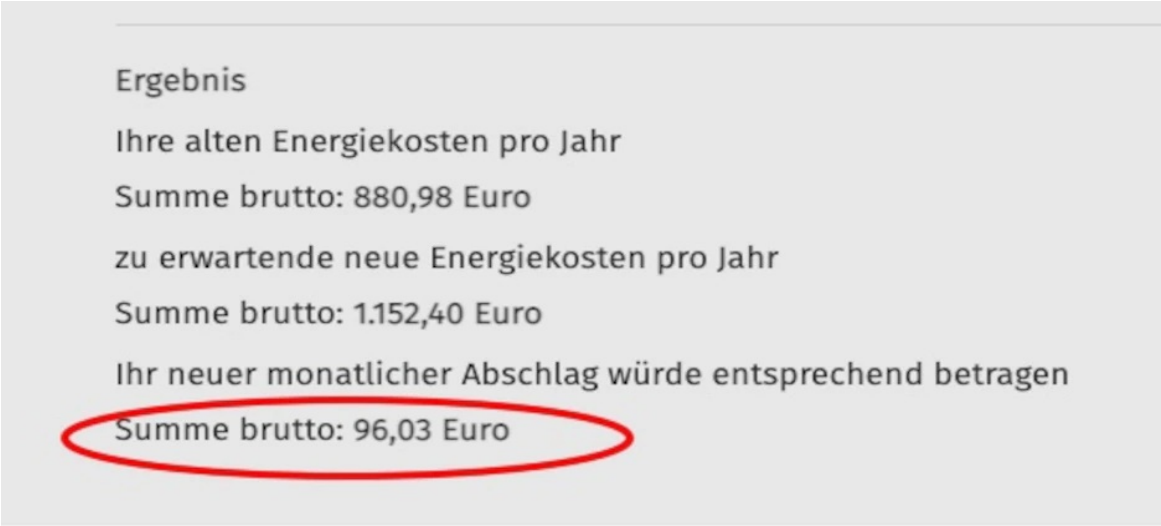
4) Bevor der Kosten-Hammer kommt: Neue Abschlagszahlung für Strom und Gas berechnen

Wer weiter seine üblichen Vorauszahlungen für Strom und Gas tätigt, könnte bald eine saftige Nachzahlung erhalten. So berechnen Sie die optimale Abschlagszahlung selbst.

Viele Menschen in Deutschland sind wegen der stark steigenden Energiepreise verunsichert. Zahlreiche Anbieter kündigen derzeit höhere Preise an und wollen auch gleich höhere Abschlagszahlungen haben. Bei anderen steigen die Preise auch, die Abschläge bleiben jedoch gleich, hier droht dann ein Preishammer bei der Jahresabrechnung.
Was Sie tun sollten? Ermitteln Sie die für Sie passenden Abschläge, sodass Sie nicht zu viel, aber auch nicht zu wenig bezahlen. Dazu brauchen Sie nur Ihre letzte Strom- oder Gasrechnung und die neuen Preise. Damit füttern Sie den Abschlagsrechner der Verbraucherzentrale.

Zur Web-App: Abschlagsrechner Strom und Gas

Passende Abschlagszahlungen für Strom und Gas ermitteln



Lassen Sie den passenden Abschlag ausrechnen. Bild: Screenshot/CHIP

Rufen Sie den Abschlagsrechner der Verbraucherzentrale auf und tragen Sie folgende Daten ein:

- Jahresverbrauch, am besten von der letzten Stromrechnung
- Bisheriger Brutto-Arbeitspreis, steht auf der letzten Stromrechnung
- Neuer Brutto-Arbeitspreis, wurde vom Anbieter angekündigt bzw. lässt sich dort erfragen
- Grundpreis aus der letzten Stromrechnung bzw. der Ankündigung vom Anbieter
- Messentgelt, falls das für Ihren Zähler anfällt

Zumindest die ersten drei Werte sind Pflicht, damit spuckt der Rechner den passenden monatlichen Abschlag aus. Sollte der so überhaupt nicht zum vereinbarten Abschlag passen, wenden Sie sich an Ihren Versorger und bitten Sie um Anpassung.

Quelle: https://www.chip.de/news/Bevor-der-Kosten-Hammer-kommt-Neue-Abschlagszahlung-fuer-Strom-und-Gas-berechnen_184383211.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=22-08-2022%2B17%253A00%253A15&utm_content=nl_chipmob&utm_term=

5) Es besteht Stromschlag-Gefahr: Großer Föhn-Rückruf gestartet

Einen Föhn-Rückruf müssen aktuell deutsche Verbraucher beachten. Bei zwei Modellen, die bei TK Maxx verkauft wurden, besteht Brand- und Stromschlaggefahr. Hier lesen Sie, wie Besitzer jetzt reagieren sollten.

Die Einzelhandelskette TK Maxx informiert aktuell über einen Rückruf von Haartrocknern, wie "produktwarnung.eu" berichtet. Bei zwei Modellen der Marken "Something Cosmetics" und "Elgetec Beauty" entsprechen Kabel und Stecker nicht den erforderlichen Sicherheitsstandards.
Bei den Produkten besteht daher die Gefahr eines Stromschlages oder Brandes. Verkauft wurden die Geräte zwischen Januar 2022 und Juli 2022.

Großer Föhn-Rückruf: Diese Modelle sind betroffen

Quelle: Diese Haartrockner sind von dem Rückruf betroffen. produktwarnung.eu

Konkret geht es um diese Produkte:

Artikel: Ultrapower Ionic Haartrockner
Marke: Something Cosmetics
Kaufdatum: Januar und Juli 2022

Artikel: Ultrapower Ionic Haartrockner
Marke: Elgetec Beauty
Farben: Blau & Beige
Kaufdatum: Januar und Juli 2022
Die Geräte können in jeder TK-Maxx-Filiale zurückgegeben werden. Käufer erhalten dabei auch ohne Vorlage des Kassenbons ihr Geld zurück.

Anmerkung der Redaktion: Den Lesern wird empfohlen ab und zu die Homepage: www.prduktwarnung.eu über aktuelle Informationen/Hinweise aufzurufen.

Quelle: https://www.chip.de/news/Stromschlag-Gefahr-Grosser-Foehn-Rueckruf_184403318.html

6) Achtung, Unfallgefahr – Hersteller ruft Fahrräder zurück

Der Fahrradhersteller Trek ruft einige seiner Modelle zurück. Aufgrund eines technischen Defekts könnte der Lenker während der Fahrt brechen.

Der Fahrradhersteller Trek ruft einige seiner Modelle zurück. Aufgrund eines technischen Defekts könnte der Lenker während der Fahrt brechen.

Aus einer Kundeninformation des Herstellers geht hervor, dass der Carbon-Basislenker und die Lenker/Vorbau-Einheit der betroffenen Produkte bei Überlastung brechen könnte. Bei einem Lenkerbruch während der Fahrt besteht durch den Kontrollverlust akute Unfallgefahr.

Rückruf: Diese Modelle sind betroffen

Abb. 1.
Speed Concept SLR MY 2022

Abb. 2.
Émonda SLR MY 2021 – 2022

Abb. 3. Bontrager Aeolus
RSL VR-C Lenker/Vorbau-Einheit MY 2020 – 2022

Rückruf: Verschiedene Modelle des Herstellers Trek werden aufgrund eines technischen Fehlers zurückgerufen. (Quelle: Trek Bicycle Corporation)

- alle **Speed Concept SLR** Modelljahr 2022, einschließlich Project One-Modelle und Standardmodelle in allen Farben
- alle **Émonda SLR** Modelljahr 2021-2022, einschließlich Project One-Modelle und Standardmodelle in allen Farben
- alle **Aftermarket Bontrager Aeolus** RSL VR-C Lenker/Vorbau-Einheiten

Der Hersteller rät dringend davon ab, betroffene Modelle ohne eine technische Überprüfung weiterhin zu nutzen.

Was können Kunden jetzt tun?

Betroffene Fahrradbesitzer sollten einen Trek-Fachhändler aufsuchen. Bei Speed Concept SLR Modellen stellt Trek einen Ersatz-Basislenker, ein neues Lenkerband und die Montage bereit. Bei Émonda SLR Modellen und Aftermarket Bontrager Aeolus RSL VC-R Lenker/Vorbau-Einheiten wird Trek einen temporären Lenker und Vorbau sowie ein neues Lenkerband bereitstellen, bis eine neue, überarbeitete Lenker/Vorbau-Einheit erhältlich ist. Sobald diese verfügbar ist, werden Kunden vom Hersteller informiert.

- Unbedingt beachten: Fahrrad online kaufen: Diese Tipps sind wichtig
- Unbedingt aufpassen: Achtung beim E-Bike: Dieser Mangel ist gefährlich
- Großer Überblick: Für wen sich das E-Bike eignet – und für wen nicht

Zusätzlich erhalten Besitzer von betroffenen Modellen einen Gutschein im Wert von 100 Euro für Trek- oder Bontrager-Produkte, der bis zum 31. Dezember 2022 eingelöst werden kann.

Quelle: https://www.t-online.de/auto/technik/id_100045558/rueckruf-technischer-defekt-hersteller-trek-ruft-fahrraeder-zurueck.html