29. Cybercrime Newsletter

15.07.2022

1) Nach Besitzerwechsel – Ebay Kleinanzeigen ändert seinen Namen

Eine Umgewöhnung für Stammkunden: Das beliebte Kleinanzeigenportal Ebay Kleinanzeigen ändert seinen Namen. Außerdem kommen zwei wichtige neue Funktionen.

Der digitale Kleinanzeigenmarkt Ebay Kleinanzeigen heißt künftig anders. Das kündigte das Unternehmen nun in einer Pressemitteilung an. Der neue Name wird dabei allerdings kaum überraschen. Künftig lautet er nur noch: Kleinanzeigen. Die Adresse wird dann kleinanzeigen.de sein.

Nutzer werden vorerst aber überhaupt nichts von der Umbenennung merken. Der neue Markenauftritt samt Logo und neuem Namen werde noch bis Juni 2024 entwickelt und erst danach sichtbar. Bislang führe die Adresse kleinanzeigen.de noch ins Leere.

Hintergrund der Namensänderung ist, dass Mutterkonzern Ebay die Sparte bereits im vergangenen Jahr an den Konkurrenten Adevinta verkauft hat. Das Unternehmen ist laut eigener Aussage nun weltweit führender Anbieter von Online-Kleinanzeigen.

"Was ist Ebay Kleinanzeigen ohne Ebay? – Kleinanzeigen"

Der CEO von Ebay Kleinanzeigen, Paul Heinemann, erklärte die Namensänderung so: "Wir haben uns die Frage gestellt, was Ebay Kleinanzeigen ohne Ebay ist – die Antwort ist einfach: Kleinanzeigen. Der neue, alte Name ist zugleich ein Versprechen an unsere Nutzer – wir bleiben, wofür wir heute stehen. Immerhin zählt Kleinanzeigen hierzulande zu den bekanntesten und beliebtesten Marken."

Schon in den kommenden Wochen wird das Portal auch eine große Neuerung einführen: "Direkt kaufen". Damit sollen Kauf und Verkauf auf Wunsch deutlich beschleunigt werden. Verkäufer, die Angebote mit einem Festpreis einstellen, können Käufern damit ermöglichen, ein Produkt direkt zu kaufen, ohne vorher verhandeln oder mit dem Verkäufer in Kontakt treten zu müssen. So können sie sich gute Angebote direkt sichern.

Bezahlt wird dann über die "Sicher bezahlen"-Funktion, die das Geld treuhändisch verwaltet, bis der Erhalt der Ware bestätigt wird. Natürlich sei es aber auch weiterhin möglich, Angebote einzustellen und dann wie bisher über deren Preis zu verhandeln.

Außerdem soll in den kommenden Wochen eine Zwei-Faktor-Authentifizierung eingeführt werden. Dadurch sollen Accounts deutlich besser gegen Missbrauch und Account-Diebstahl geschützt werden.

Der Online-Kleinanzeigenmarkt führt mit rund 40 Mio. Nutzern im Monat regelmäßig das Ranking der unabhängigen *Arbeitsgemeinschaft Onlineforschung* an.

Quelle: https://www.t-online.de/digital/internet-sicherheit/internet/id_100027496/ebay-kleinanzeigen-aendert-seinen-namen.html

2) Das sind die aktuellen Spam-Rufnummern

Im Juni kam es wieder zu unzähligen unerwünschten Anrufen. In unserer aktuellen Liste finden Sie die zehn häufigsten Spam-Nummern, die Sie ignorieren können.

Das Telefon klingelt, man nimmt ab und hört eine unbekannte Stimme, oder es tut sich erst einmal nichts. Plötzlich hört man eine Bandansage oder der Anrufer legt auf, ohne ein Wort gesagt zu haben. In vielen Fällen handelt es sich dabei um unerwünschte Werbe- oder Betrugsanrufe, mit denen unwissende Opfer in die Falle gelockt werden sollen.

Wie jeden Monat kam es auch im Juni wieder zu Zehntausenden solcher Anrufe auf deutsche Festnetz- und Mobilfunkanschlüsse. Beliebt waren vor allem wieder angebliche Lotteriemitgliedschaften, Gewinnspiele ("Sie haben gewonnen") oder vermeintlich günstigere Energietarife ("Sie bezahlen zu viel für Strom").

In unserer Liste für Juni 2022 haben wir die zehn häufigsten Spam-Nummern für Sie zusammengefasst:

Top 10 der Spam-Nummern im Juni 2022

Top 10 Spam-Telefonnummern Juni 2022

Platz	Vorwahl	Nummer	Info / Typ	Calls insgesamt	Blockiert von	Bewertung
1.	+49	040254671238	Kostenfalle	9005	385	1,5
2.	+49	015210151906	Kostenfalle	2423	229	1,4
3.	+49	030439729068	Kostenfalle	2410	579	1,4
4.	+49	03016637169	Gewinnspiel	2271	831	1,4
5.	+49	06920091655	Andere	2247	356	1,3
6.	+49	01773996325	Kostenfalle	2016	232	1,2
7.	+49	04029996426	Kostenfalle	1902	450	1,4
8.	+49	040607739322	Kostenfalle	1425	296	1,3
9.	+49	01768429693	Gewinnspiel	1370	295	1,3
10.	+49	021198709935	Andere	1370	368	1,5

Clever Dialer cleverdialer.de

Das sind die zehn häufigsten Spam-Telefonnummern aus dem Juni 2022. (Quelle: Clever Dialer)

So berichten Angerufene unter anderem davon, dass sie mehrmals am Tag von der Hamburger Nummer 040254671238 angerufen worden sind. Nimmt man den Hörer ab, meldet sich eine Stimme und erzählt etwas von einem kostenpflichtigen Lotteriegewinnspiel, an dem man angeblich teilgenommen hätte und jetzt monatlich etwas bezahlen müsse.

Auch unter anderen der genannten Nummern (015210151906 und 01773996325) verstecken sich sogenannte Kostenfallen, die den Betroffenen eine zahlungspflichtige Lotterie- oder Gewinnspielteilnahme anhängen wollen und eine Zahlung einfordern. Ein Nutzer berichtet davon und gibt auch gleich einen Ratschlag, wie damit umzugehen ist: "Lotto-Betrugsmasche – Angeblich 3-monatiges Sonderkündigungsrecht. Gleich auflegen." Das sind die zehn häufigsten Spam-Telefonnummern aus dem Juni 2022. (Quelle: Clever Dialer)

In diesem Monat nutzten Betrüger ebenfalls wieder die steigenden Energiekosten als Vorwand, den Angerufenen neue, angeblich bessere Stromverträge anzubieten. Hierfür würden

persönliche Daten und auch die Zählernummer benötigt. So klagt ein Nutzer über die Nummer 040607739322 (Platz 8):

"Ganz furchtbar unfreundliche und freche Menschen versuchen, einem einen Energievertrag anzudrehen. Auf meine Bitte, mich nicht mehr zu kontaktieren, fing die Dame an, beleidigend zu werden!!!"

Auch hier aufgepasst: Es handelt sich um eine Betrugsmasche. Geben Sie auf keinen Fall persönliche Informationen oder gar Ihre Bankverbindungen preis.

Um sich zuverlässig vor Betrugsversuchen oder potenziellen Kostenfallen zu schützen, lauten die goldenen Regeln: Rufen Sie keine unbekannten Nummern zurück. Kommen Ihnen ein Anrufer oder eine Nummer suspekt vor, sollten Sie diese ignorieren oder blockieren. Wie das funktioniert, erklären wir in unserer Anleitung Schritt für Schritt. In vielen Fällen hilft es auch schon, einen Anruf schlicht abzubrechen und aufzulegen, wenn der Gesprächspartner mit dubiosen Anfragen an Sie herantritt.

Quelle: https://www.t-online.de/digital/handy/id_100026200/spam-anrufe-juni-2022-diese-nummern-koennen-sie-ignorieren-.html

3) Polizei warnt: So kapern Gangster die Konten ihrer Opfer und so schützen Sie sich

Die Polizei warnt vor einer Betrugsmasche, mit der Cybergangster derzeit verstärkt nach Opfern suchen: "Job-Scamming". So läuft die Masche und so schützen Sie sich.

Das Polizeipräsidium Südosthessen warnt vor einer Betrugsmasche, mit der Cybergangster derzeit verstärkt nach Opfern suchen. Dabei handelt es sich um so genanntes "Job-Scamming".

So ködern die Gangster ihre Opfer

Dabei erstellen die Betrüger gefälschte Stellenanzeigen im Internet, vorwiegend auf Job- oder Internetverkaufsportalen. Sie versprechen einen Job mit sehr guter Bezahlung, oftmals mit freier Zeiteinteilung und Aussicht auf Homeoffice. Also ein möglichst attraktives Angebot, das für viele Job-Suchende interessant sein könnte. Besonders raffiniert: In vielen Fällen zahlen die Täter zunächst einen kleinen Geldbetrag, um die Opfer zu ködern - so wird eine große Anzahl potenzieller Opfer angelockt.

Opfer sollen Konten eröffnen

Den Opfern wird in der Regel angeboten, als Tester von Banking-Apps zu arbeiten oder ein Auswahlverfahren durchlaufen zu müssen, was in aller Regel online stattfindet. Das Entscheidende: In beiden Fällen werden die Opfer von den Tätern dazu veranlasst, via Video-Ident-Verfahren persönliche Daten und Bilder preiszugeben, mit denen die Betrüger echte Bank- oder Bitcoin-Konten auf die Namen der Geschädigten eröffnen. Denn darum geht es bei dieser Betrugsmasche: Die Cybergangster wollen über die von den Opfern eröffneten Konten ihre Betrügereien durchführen.

Im weiteren Verlauf werden die Opfer gebeten, die ihnen zugestellten Kontoeröffnungsunterlagen (PIN/TAN usw.) den Tätern zuzuleiten, wie die Polizei erläutert. Die Zuleitung der Unterlagen soll angeblich dazu dienen, die eröffneten Konten von Seiten des "Arbeitgebers" nach erfolgreicher Testung zu schließen. Doch die Täter verändern unmittelbar nach Erhalt der Unterlagen die Onlinezugangsdaten zu den Konten, so dass die Opfer ab diesem Zeitpunkt keinen Zugriff auf das bzw. die eröffneten Konten haben. Zum Teil werden Konten bereits mit dem Namen des Bewerbers, allerdings mit falschen Kontaktdaten von den

Tätern eröffnet. Somit ist der Zugang des Kontos bereits ab Eröffnung des Bewerbers für die Täter offen.

Dafür nutzen die Gangster die Konten der Opfer

Die Cybergangster nutzen die im Namen der Opfer eröffneten Konten für Zahlungen aus weiteren kriminellen Handlungen, etwa beim Warenbetrug. Das geht dann so: Die Täter bieten im Internet hochwertige Ware, wie etwa Smartphones oder Gartengeräte, günstig als Fake-Angebote an. Kauft nun ein Dritter das vermeintlich günstige Angebot und überweist das Geld auf das zuvor eröffnete Konto, ist das Geld weg - es wird nämlich sofort über andere Konten ins Ausland weitergeleitet. Die gesamte Kommunikation zwischen Tätern und Geschädigten findet in den meisten Fällen über Messenger-Dienste statt.

Über den Betrug informiert werden die Opfer meist erst Wochen oder Monate später, wenn etwa ein Warenbetrugs-Opfer Anzeige erstattet oder sich das Amtsgericht mit dem Hinweis meldet, dass das Konto gepfändet wurde. Dann droht den Opfern, in deren Namen die Konten eröffnet wurden, sogar noch Ärger wegen Verdachts der Geldwäsche.

Die Polizei rät:

- Im Rahmen eines Bewerbungsverfahrens sollte eine Kontoeröffnung via Video-Ident-Verfahren auf jeden Fall abgelehnt werden.
- Wenn bereits an einem solchen Verfahren teilgenommen wurde, sollte das Konto sofort gesperrt werden.
- Sichern Sie Chatverläufe und erstatten Sie in jedem Fall Strafanzeige bei der Polizei, wenn Sie einer fremden Person Ihre Daten übermittelt haben.

Quelle: https://www.pcwelt.de/news/Polizei-warnt-So-kapern-Gangster-die-Konten-ihrer-Opfer-und-so-schuetzen-Sie-sich-11262426.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3690280&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Betrugsversuch an Sparkassenkunden: Neue Masche

Betrüger haben sich einen neuen Vorwand ausgedacht, um an die Logindaten von Sparkassenkunden zu gelangen.

Cybergangster versuchen mit einem neuen Trick an die Zugangsdaten von Sparkassenkunden zu kommen. Davor warnt die Verbraucherzentrale Schleswig-Holstein.

Hierzu verschicken die Betrüger eine Mail, die die Empfänger darüber informiert, dass angeblich eine ungelesene Nachricht im Postfach ihres Online-Banking-Postfaches auf sie wartet. Die Betreffzeile der Mail heißt "Wichtige Information zu Ihrem Konto".

Um den Druck auf die Empfänger zu erhöhen, wird in der Mail ein kurzfristiges Datum genannt, bis zu dem die Nachricht gelesen werden sollte. Wie immer bei solchen Phishingmails befindet sich dann ein großer Button unter dem Mailtext, den die Empfänger anklicken sollen. In diesem Fall ist der Button farblich passend in das "Sparkassen-Rot" eingefärbt. Doch der hinter dem roten Button hinterlegte Link führt (wie immer in solchen Fällen) auf eine Phishingseite, auf der die ahnungslosen Sparkassenkunden ihre Logindaten für das Onlinebanking eingeben sollen. Damit diese in die Hände der Betrüger fallen.

So reagieren Sie richtig

Diese Phishingmail verdient nur eine adäquate Behandlung: Löschen Sie die Mail, ohne etwas darin anzuklicken.

Sparkassenkunden im Fokus der Cybergangster

Sparkassenkunden gehören zu den bevorzugten Zielen von Phishingmails. Die Angriffe ähneln sich beim Ablauf immer sehr stark, nur der Vorwand, unter dem die Mails verschickt werden, variiert. Damit Sie sich einen Überblick über die unterschiedlichen Tarnungen verschaffen können, mit denen die Cybergangster ihre Phishingmails zu begründen versuchen, haben wir hier die jüngsten Phishing-Attacken auf Sparkassenkunden zusammengestellt:

Sparkasse warnt vor Diebstahl der Online-Banking-Daten

Sparkasse: Raffinierte Angriffe auf Kunden - neue Masche

Sparkassen-Kunden aufgepasst: Neue Betrugsmasche mit pushTAN 2.0

Diese Mail lockt Sparkassen-Kunden mit drohender Kontosperrung in Falle

Sparkasse, Volksbank & Raiffeisenbank: Angriffe von unterschiedlicher Gefährlichkeit

Sparkasse und Paypal: Neue Angriffswelle

Quelle: https://www.pcwelt.de/news/Betrugsversuch-an-Sparkassenkunden-Neue-Masche-11263808.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3699965&pm_cat%5B0%5D=eMail+Management&pm_cat%5B1%5D=Web+Security&pm_cat%5B2%5D=Security+Software&pm_cat%5B3%5D=Virenschutz&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Bei Kunden der Haspa – Verbraucherzentrale warnt vor täuschend echten Betrugsanrufen

Betrüger haben es auf Kunden der Haspa abgesehen: Mithilfe eines technischen Tricks versuchen die Kriminellen sensible Daten ihrer Opfer zu erfragen.

Die Verbraucherzentrale Hamburg warnt aktuell vor Anrufen falscher Mitarbeiter der Hamburger Sparkasse (Haspa). Ziel der Betrüger sei es, einen speziellen Zugangscode zu erschleichen, um damit Überweisungen vom Konto des Opfers zu tätigen, heißt es in einer Pressemitteilung. Grundsätzlich solle man am Telefon keine sensiblen Daten preisgeben und derartige Anrufe umgehend der Polizei melden.

Die Kunden werden dabei von den Betrügern informiert, dass es eine verdächtige Buchung auf deren Konten gebe. Gleichzeitig bieten die Anrufer an, die Buchung zu stoppen. Dafür sollen die Opfer den Vorgang mit einer Push-TAN am Telefon autorisieren. Mit dieser ist es den Kriminellen dann möglich, Geld vom Konto der Angerufenen zu überweisen.

Betrüger können mit Haspa-Telefonnummer anrufen

"Wichtig! In der Regel ruft die Haspa Sie nicht unaufgefordert hat", warnt die Verbraucherzentrale. Dabei solle man sich auch nicht von einer scheinbar der Haspa zugehörigen Nummer täuschen lassen. "Uns liegt ein Fall vor, in dem eine Verbraucherin während des Gesprächs die Telefonnummer des Anrufers überprüfte. Sie stimmte mit der Nummer der Haspa bis auf die letzte Ziffer überein."

Von der Haspa heißt es dazu auf der eigenen Webseite: "Ihre Sparkasse wird Sie niemals per Telefon oder E-Mail auffordern, Ihre Daten wie IBAN, Anmeldenamen PIN, TAN oder Ihre Kreditkartendaten preiszugeben oder diese auf einer Internetseite einzutragen." Außerdem

sensibilisiere man laufend über die eigenen Social-Media-Kanäle zu dem Thema, sagt Unternehmenssprecherin Stefanie von Carlsburg t-online. Die Masche sei jedoch nicht neu und auch eine besondere Häufung gebe es gegenwärtig nicht.

Quelle: https://www.t-online.de/region/hamburg/id_100025880/haspa-kunden-aufgepasst-warnung-vor-taeuschend-echten-betrugsanrufen.html

6) Betrugsmaschen: Achtung, diese Nachrichten stammen nicht von DHL

- **Betrüger am Telefon, im Internet oder an der Haustür gehen immer geschickter vor.**
- **Mit immer neuen Tricks versuchen sie etwa, per E-Mail Daten abzufangen.**
- **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.

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 verkleiden sich als Polizeibeamte, 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-nachrichten-dhl-34288658

Anwenderinformationen:

1) Unbegrenzte Auswahl – WhatsApp bringt neue Emoji-Reaktionen

Mit Emoji-Reaktionen hat WhatsApp vor einiger Zeit eine neue Funktion in seinen beliebten Messenger integriert. Diese wird jetzt deutlich ausgebaut.

WhatsApp stockt das Repertoire an verfügbaren Emoji-Reaktionen deutlich auf, wie **Mark Zuckerberg** auf **Facebook** bekanntgegeben hat. Dort kündigt der Meta-Chef an, dass bald alle verfügbaren Emojis zur Auswahl stehen. Damit stehen Nutzern hunderte verschiedene Optionen zur Auswahl und der Kreativität sind keine Grenzen mehr gesetzt.

Bereits Anfang Mai haben wir berichtet, dass WhatsApp nach langer Wartezeit endlich Emoji-Reaktionen einführt, die bei anderen Messengern wie Telegram seit Jahren zum Standard gehören. Die Auswahl der verfügbaren Emojis war aber auf sechs voreingestellte Optionen begrenzt. Mit der unbegrenzten Auswahl zieht WhatsApp jetzt an der Konkurrenz vorbei.

Auf Nachrichten können Nutzer reagieren, indem sie diese antippen und gedrückt halten. Anschließend öffnet sich ein Auswahlfenster, das neben Optionen wie "Antworten", "Weiterleiten" und "Löschen" auch eine Reihe mit Emojis bereithält – diese wird in der neuen Version um ein "+" ergänzt, über das sich alle weiteren Emojis auswählen lassen.

Neue Funktionen am laufenden Band

Die WhatsApp-Entwickler sind stetig dabei, der Chat-App neue Funktionen zu spendieren oder vorhandene Funktionen auszubauen und zu verbessern. Neben den Emoji-Reaktionen, die bereits seit ein paar Monaten verfügbar sind, wird auch an neuen Funktionen gearbeitet.

Unter anderem sollen in einer künftigen Version bereits verschickte Nachrichten bearbeitet werden können. Darüber hinaus arbeitet der Meta-Konzern daran, **die Online-Statusanzeige personalisieren zu können**. Dort soll sich dann auswählen lassen, welche Kontakte den Status sehen können und welchen Kontakten er nicht angezeigt werden soll.

Tipp:

- Ratgeber: WhatsApp funktioniert nicht mehr – was tun?
- Schutz vor neugierigem Chef: Neue WhatsApp-Funktion verhindert peinliche Enthüllungen
- Leichter erkennbar: WhatsApp überarbeitet die Statusanzeige

Quelle: https://www.t-online.de/digital/handy/id_100027800/whatsapp-emoji-reaktionen-werden-deutlich-erweitert.html

2) Online-Banking: Neue TAN-Verfahren im Überblick

Derzeit stellen mehrere große Geldinstitute ihre TAN-Verfahren für Online-Überweisungen um, Millionen Bankkunden sind betroffen. Unser Ratgeber stellt die TAN-Alternativen vor, gibt Empfehlungen und erläutert, wie Sie sich vor Kontendiebstahl durch Phishing schützen.

Immer wieder stellen Geldinstitute irgendetwas an der Art und Weise um, mit der Kunden

Online-Überweisungen per TAN ausführen können. So schaltete die Deutsche Bank im März das HBCI-Verfahren mit Chipkarte ab, die Postbank musterte im Mai die Chip-TAN aus, und die Volksbanken und Sparkassen haben angekündigt, den SMS-Versand der TAN noch in diesem Jahr einzustellen. Schon diese drei Großbanken betreffen Millionen Bankkunden, Änderungen bei kleineren Finanzinstituten sind da noch gar nicht berücksichtigt.

Solche Umstellungen haben zum einen zur Folge, dass sich viele Verbraucher mit Fragen konfrontiert sehen: Muss ich aktiv werden, um meine Bankgeschäfte weiter online abwickeln zu können? Welche Alternativen gibt es, und welches TAN-Verfahren ist für mich geeignet? Und schließlich: Was muss ich tun, wie funktioniert die Umstellung tun, und brauche ich eine neue App oder gar neue Hardware?

Zum zweiten rufen bereits die Ankündigungen, dass sich bei den TANs etwas ändert, Betrüger auf den Plan, per Phishing-Mail oder -SMS an Ihre Zugangsdaten fürs Online-Banking zu kommen. Davor warnten im Frühjahr die Verbraucherzentralen nochmals ausdrücklich. Welche Betrugsversuche aktuell verbreitet sind, listet die Verbraucherzentrale NRW in ihrem „ Phishing-Radar “ auf.

Übersicht: Aktuelle Gefahren und Schutz beim Online-Banking

EU-Zahlungsdiensterichtlinie verlangt dynamische TANs

Wie bei anderen Online-Accounts üblich, loggt man sich auch beim Internet-Banking mit seinen persönlichen Zugangsdaten ein. Danach zeigt das Bankportal eine Übersicht der eigenen Konten, Kreditkarten und so weiter inklusive der Saldi. Machen im eigentlichen Wortsinn können Sie nach dem Log-in jedoch noch nichts. Denn für jede Aktion wie eine Überweisung, das Einrichten eines Dauerauftrags oder das Ändern der persönlichen Daten benötigen Sie eine TAN, also eine Transaktionsnummer.

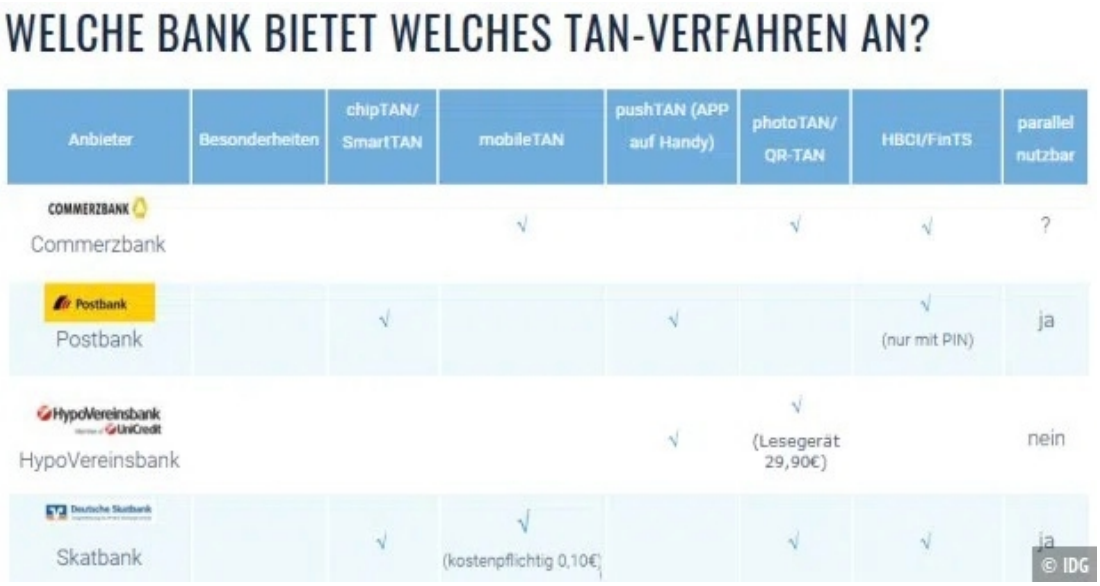
Eine solche Transaktionsnummer stellt ein aus sechs Ziffern bestehendes Einmal-Passwort und damit neben dem Log-in einen zweiten Faktor dar. Salopp ausgedrückt sehen potenzielle Gelddiebe Ihrer Zugangsdaten zwar, wie viel Geld Sie besitzen, ohne gültige TAN kommen sie aber nicht ran. Die Nummern sollen also sicherstellen, dass Banktransaktionen im Internet wirklich von der autorisierten Person durchgeführt werden. Nicht mehr erlaubt sind die früher üblichen gedruckten TAN-Listen. Denn mit Inkrafttreten der zweiten EU-Zahlungsdiensterichtlinie (PSD2) im Jahr 2019 müssen die TANs zusammen mit dem Überweisungsdaten erzeugt werden, zudem sind sie zeitlich nur begrenzt gültig.

Zum Generieren der TANs stehen technisch ganz unterschiedliche Wege zur Verfügung, die Methoden unterscheiden sich hinsichtlich Komfort und Sicherheitslevel. Sicherheitsgründe sind es auch, dass der TAN-Versand per SMS mehr und mehr eingestellt wird. In der Vergangenheit war es Betrügern immer wieder gelungen, über die Mobilfunkprovider an Ersatz-SIM-Karten zu kommen und damit auch an die von den Banken per SMS verschickten Transaktionsnummern. Ein weiteres Risiko stellen Trojaner auf dem Smartphone dar.

Welche TAN-Verfahren die Banken jeweils anbieten, liegt in deren eigenem Ermessen. Als Kunde haben Sie darauf keinen Einfluss und zudem nur dann eine Wahl, wenn Ihr Kreditinstitut überhaupt mehrere Verfahren offeriert. Ob und welche das gegebenenfalls sind, ist nicht immer einfach herauszufinden. Denn häufig drängen Banken ihre Kunden aus Kosten- oder administrativen Gründen in ein Verfahren oder geben ihnen Fantasiebezeichnungen: Was sich hinter BestSign, easyTAN, SecurePlus oder TAN2go verbirgt, erschließt sich nicht jedem Nutzer sofort. Hier helfen Übersichten im Internet weiter, wie sie beispielsweise Kostenloses Konto 24 unter und Kontovergleich24 bieten.

Tipp: Schafft die eigene Bank Ihre bislang bevorzugte TAN-Methode ab, wechseln Sie deshalb nicht gleich das Institut – das neue könnte ein paar Monate später nachziehen. Meist gewöhnt

man sich schnell an das geänderte Verfahren. SMS-, Chip-, Push-TAN & Co.: Die Möglichkeiten im Überblick



Übersichten im Internet wie diese helfen bei der Orientierung, welche Kreditinstitute welche TAN-Verfahren anbieten. Allerdings ändern sich Auswahl und Angebot ständig. (Quelle: www.pcwelt.de)

Dass es nicht die eine beste Methode zum Erzeugen der Transaktionsnummern gibt, zeigen schon die Vorgänge bei Deutscher Bank, Postbank, Sparkassen und Volksbanken: Während die Postbank die Chip-TAN abgeschafft hat, wird das Verfahren von den Sparkassen aktiv beworben. Der folgende Überblick nennt alle gängigen Arten inklusive ihrer Vor- und Nachteile, einige erfordern ein zusätzliches Gerät.

SMS-TAN (auch **mobileTAN** oder **mTAN** genannt): Die Bank verschickt die generierten TANs per Kurznachricht. Weil Smartphones eben- so wie PCs mit Schadcode infiziert sein können oder die TAN-SMS über eine zusätzliche SIM-Karte abgefangen werden kann, ist das Verfahren tendenziell unsicher und wird zunehmend abgeschafft.

Chip-TAN (auch **eTAN** oder **Smart-TAN** genannt): Bei der Chip-TAN kommt ein handlicher TAN-Generator zum Einsatz, in den man seine Girocard („EC-Karte“) einsteckt. Das Ausführen einer Überweisung am PC erzeugt am Bildschirm einen optischen Code, den der TAN-Generator einliest und daraus die zugehörige TAN erzeugt. Diese tippt man im Browser oder Banking-Programm ein und führt dadurch online die Geldtransaktion aus. Weil dabei zwei voneinander unabhängige Geräte zum Einsatz kommen, ist Chip-TAN sehr sicher. Nachteil: Man benötigt einen TAN-Generator, den man von der Bank bekommt oder im Handel kaufen muss (ab etwa 15 Euro).

Photo-TAN und **QR-TAN** sind Unterarten der Chip-TAN, hier werden statt der Flicker-Codes farbige Mosaikgrafiken beziehungsweise ein QR-Codes erzeugt. Für beides benötigt man spezielle TAN-Generatoren, die es ab ca. 25 Euro zu kaufen gibt, oder eine kostenlose Smartphone-App.

AppTAN oder **PushTAN** erzeugt TANs in einer App auf dem Smartphone oder Tablet. Die App ist per Passwort, Gesichtserkennung oder Fingerabdruck geschützt und arbeitet separat von Banking-App beziehungsweise vom Browser. Deshalb gilt das Verfahren als sicher, obwohl alles auf einem Gerät läuft. So lassen sich Geldgeschäfte auch unterwegs erledigen, und man benötigt keinerlei Zusatzmodul.

BestSign kommt ganz ohne TAN aus und arbeitet stattdessen mit einer digitalen Signatur. Wie

bei der App- oder PushTAN ist eine App erforderlich, in der jede Banktransaktion manuell bestätigt werden muss. Alternativ zur App lässt sich BestSign auch mit speziellen Zusatzgeräten von Seal One (ab 30 Euro) nutzen.

Android: Das sind die 10 häufigsten Banking-Trojaner

Wenn Sie das TAN-Verfahren wechseln müssen: So geht's

Angesichts der ständigen Gefahren durch Phishing, Trojaner und Schadcode am PC sowie am Smartphone sollten bei Ihnen alle Alarmglocken klingeln, wenn E-Mails Änderungen beim TAN-Verfahren, beim „Sicherheitssystem" oder Ähnlichem ankündigen: Die überwiegende Mehrzahl solcher Nachrichten sind Phishing-Versuche. Klicken Sie deshalb in solchen Mails niemals auf irgendwelche Links, und loggen Sie sich dort nicht mit Ihren Bankdaten ein!

Weil manche Geldinstitute ihre Kunden aus Kostengründen jedoch tatsächlich per Mail statt per Brief über neue TAN-Verfahren benachrichtigen, lassen Sie solche Ankündigungen andererseits nicht ganz unbeachtet, sondern überprüfen die vermeintliche Änderung per Google-Suche oder über Ihre Bank (Webseite, Anruf oder Filiale). Haben Sie sichergestellt, dass Ihre Bank tatsächlich das von Ihnen bislang verwendete TAN-Verfahren abschafft oder ändert, müssen Sie aktiv werden.

Informieren Sie sich im ersten Schritt über die zur Verfügung stehenden TAN-Alternativen, meist zeigt die Webseite dazu eine Übersicht und Informationen zu den einzelnen Methoden sowie zum Umstieg. Tendenziell ist der Einsatz eines echten Zusatzgeräts sicherer als die App-gestützten Methoden, die Kosten für die Hardware sind vergleichsweise gering und für das Plus an Sicherheit gut investiert. Im zweiten Schritt folgen Sie der Anleitung zum Umstieg, unter Umständen muss das neue Verfahren vor der ersten Benutzung erst aktiviert oder freigeschaltet werden. Anfangs ist das neue Verfahren zwar ungewohnt, in aller Regel aber wird man auch damit schnell vertraut – nur Mut also.

Ein Tipp zum Schluss: Statt im Browser können Sie Ihre Bankgeschäfte auch per Software am PC erledigen. Die Software greift über eine standardisierte Schnittstelle auf die IT-Infrastruktur Ihrer Bank zu, ist sicher und bietet mehr Funktionen als das Online-Banking im Browser.

Weitere Sicherheitstipps zum Online-Banking bieten das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Stiftung Warentest .

Quelle: https://www.pcwelt.de/a/banken-schaffen-itan-ab-welches-tan-verfahren-ist-sicher,3426357?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3426357&pm_cat%5B0%5D=Web+Security&pm_cat%5B1%5D=PC&pm_cat%5B2%5D=Apps&pm_cat%5B3%5D=Security+Software&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Whatsapp-Benachrichtigungen personalisieren – so geht's

Verpassen Sie Ihren Whatsapp-Chats und Gruppen individuelle Töne, Vibrationen oder Farben, um direkt zu erkennen, wer Ihnen schreibt. So funktioniert's.

Vorbei sind die Zeiten, in der Sie bei jeder Whatsapp-Benachrichtigung zum Handy greifen müssen, um zu sehen, wer schreibt. Denn was viele Nutzer nicht wissen: In der App kann man bevorzugte Chatkontakte und Gruppen personalisieren und ihnen beispielsweise bestimmte Töne oder LED-Lichter zuordnen. Wie das geht, erklären wir Ihnen in diesem Beitrag.

Whatsapp-Benachrichtigungen unter Android personalisieren

Android-Nutzer profitieren von deutlich mehr Feature als iPhone-Besitzer, denn in hier

ermöglicht Whatsapp sowohl **individuelle Töne als auch Vibrationsmuster und Farben.** Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie Whatsapp und dort einen beliebigen Einzel- oder Gruppenchat, den Sie personalisieren möchten.
2. Tippen Sie oben auf den Namen des Kontakts/der Gruppe.
3. Tippen Sie auf „Eigene Benachrichtigungen“ und setzen Sie einen Haken ins obere Kontrollkästchen.
4. Legen Sie die gewünschten Einstellungen für Chats und Anrufe fest.

Whatsapp-Benachrichtigungen unter iOS personalisieren

Auf dem iPhone oder iPad haben Sie hingegen nur die Möglichkeit, Ihren Chatkontakten **spezifische Mitteilungstöne** zuzuordnen. So geht’s:

1. Öffnen Sie Whatsapp und dort einen beliebigen Einzel- oder Gruppenchat, den Sie personalisieren möchten.
2. Tippen Sie oben auf den Namen des Kontakts/der Gruppe.
3. Tippen Sie auf „Hintergrund und Töne“ und wählen Sie „Mitteilungston“ aus.
4. Legen Sie nun den gewünschten Ton fest.

Noch mehr Whatsapp-Tipps finden Sie hier:

- Whatsapp-Status vor bestimmten Kontakten verbergen
- Whatsapp: "Weitergeleitet"-Hinweis entfernen
- Diese 9 Whatsapp-Regeln darf kein Nutzer brechen
- Whatsapp als Direktlink in die E-Mail-Signatur packen
- Whatsapp auf neues Handy übertragen – so laden Sie ein Backup
- Whatsapp-Sprachnachrichten als Klingelton einstellen unter Android & iOS

Quelle: https://www.pcwelt.de/tipps/Whatsapp-Benachrichtigungen-personalisieren-so-geht-s-11259155.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3690275&pm_cat%5B0%5D=Apple&pm_cat%5B1%5D=iOS&pm_cat%5B2%5D=Mobile+Client&pm_cat%5B3%5D=Mobile+Plattformen&pm_cat%5B4%5D=Mobilfunk&pm_cat%5B5%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Paypal-Konto löschen – so geht’s

Genug von Paypal? Unsere Anleitung erklärt Ihnen, wie Sie Ihr Paypal-Konto schließen und was Sie im Vorfeld unbedingt beachten sollten.

Paypal ist einer der meistgenutzten und beliebtesten Online-Bezahldienste auf der Welt. Ein virtuelles Paypal-Konto vereinfacht nationale wie internationale Geldgeschäfte und ermöglicht einen sicheren und schnellen Zahlungsverkehr. Nichtsdestotrotz können Sie Ihr Paypal-Konto jederzeit kündigen, wenn Sie es nicht mehr brauchen. Alle Infos zu den Voraussetzungen und zum Vorgehen selbst erfahren Sie hier:

Paypal-Konto löschen: Voraussetzungen

Bevor Sie den finalen Schritt wagen und Ihr Paypal-Nutzerprofil löschen, sollten Sie prüfen, ob Sie auch alle Voraussetzungen erfüllen. Für die Löschung eines Paypal-Kontos gelten folgende Bestimmungen:

- Es dürfen keine offenen Zahlungen, Konflikte oder Rückbuchungen bestehen.
- Es dürfen keine offenen Anträge auf Käuferschutz vorliegen.
- Es darf sich kein Guthaben mehr auf Ihrem Paypal-Konto befinden.

Schließen Sie also zuerst alle Transaktionen und Angelegenheiten ab und buchen Sie Ihr Paypal-Guthaben auf ein hinterlegtes Bankkonto. Entfernen Sie auch E-Mail-Adressen oder Konten, deren Bestätigung noch aussteht. Sind diese Punkte geklärt, können Sie mit der folgenden Schritt-für-Schritt-Anleitung fortfahren.

Achtung: Ist Ihr Paypal-Konto erst gelöscht, kann es nicht mehr geöffnet oder reaktiviert werden. Durch die Kontoschließung verlieren Sie alle nicht eingelösten Gutscheine. Außerdem werden alle Geldanforderungen von Ihnen an andere Paypal-User automatisch storniert.

Paypal-Konto löschen per Web & App

Sie können Ihr Paypal-Nutzerprofil sowohl im Webbrowser als auch in der Paypal-App löschen. Beide Wege erklären wir Ihnen nachfolgend.

Paypal-Konto im Browser löschen

1. Loggen Sie sich mit Ihren Zugangsdaten auf der Paypal-Website ein.
2. Klicken Sie im oberen Menü auf das Zahnrad-Symbol neben „Ausloggen“.
3. Klicken Sie unter „Kontoeinstellungen“ auf „Konto schließen“.
4. Bestätigen Sie Ihre Entscheidung mit einem weiteren Klick auf „Konto schließen“.

Paypal-Konto in der App löschen

1. Öffnen Sie Ihre Paypal-App und tippen Sie links oben auf das Profil-Icon.
2. Scrollen Sie nach unten und tippen Sie auf „Konto schließen“.
3. Tippen Sie erneut auf den Button „Konto schließen“.

Was passiert nach der Kontoschließung?

Nachdem Sie Ihr Paypal-Konto gelöscht haben, erhalten Sie eine Bestätigungsmail an die mit Ihrem Profil verknüpfte Adresse. Weitere Schritte Ihrerseits sind ab diesem Punkt nicht mehr nötig.

Weitere Paypal-Themen, die Sie interessieren könnten:

- Diese Gebühren werden bei der Paypal-Nutzung fällig
- Paypal: Geld an Freunde senden – schnell und kostenlos

Quelle: https://www.pcwelt.de/ratgeber/Paypal-Konto-loeschen-so-geht-s-11256356.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=0&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Schadprogramme – Joker-Malware im Play Store: Vier Android-Apps betroffen

Im Google Play Store reibt erneut die Malware "Joker" ihr Unwesen. Vier Apps sollen aktuell von der Schadsoftware betroffen und bereits mehr als Hunderttausend Mal heruntergeladen worden sein.

Vier Android-Anwendungen, die im offiziellen Google Play Store zu finden sind, sollen mit der sogenannten "Joker"-Malware infiziert sein. Wie die Sicherheitsforscher des Unternehmens "Pradeo" in einem Blogbeitrag berichten, beläuft sich die Zahl der Downloads der verseuchten Apps auf eine sechsstellige Zahl und soll bereits aktiv Schaden angerichtet haben.

Bei Joker handelt es sich um Fleeceware, mit der grundsätzlich zahlungspflichtige Abonnements abgeschlossen oder teure SMS und Anrufe getätigt werden, die sich wiederum in der Handyrechnung bemerkbar machen. Mit einer unauffälligen Codestruktur bleibt die Malware von Nutzern in der Regel unbemerkt.

Diese Apps sind betroffen

Die Malware selbst ist bereits seit mehr als drei Jahren aktiv und taucht regelmäßig in neuen Android-Apps auf. Im konkreten Fall handelt es sich um die Anwendungen "Smart SMS Messages" (Version 1.3.2), "Blood Pressure Monitor" (Version 1.3.238), "Voice Languages Translator" (Version 2.0) und "Quick Text SMS" (Version 2.0), welche mindestens seit Juni 2022 mit dem Virus infiziert sind. Nutzer, die eine der Apps installiert haben, sollten die genannten Apps schnellstmöglich vom System entfernen, um sich vor Betrug zu schützen.

Zusätzlich zum finanziellen Schaden können Joker-Apps als Einfallstor - auch als "Dropper" bekannt - für weitere schädliche Apps dienen, die so potenziell noch gefährlichere Malware ins Smartphone einschleusen können. Generell seien solche Apps laut Pradeo nach einem bestimmten Muster gestrickt, das es für Nutzer einfacher machen kann, diese zu identifizieren: So habe das Entwicklerkonto, das die App im Play Store hochlädt, in der Regel nur diese Anwendung im Portfolio und lasse sich nie zu einem echten Firmennamen zurückverfolgen. Zudem seien die notwendigen Datenschutzvereinbarungen nie vollständig auf der Download-Seite zu finden und verlinken stattdessen auf ein herkömmliches Google Doc.

Quelle: https://www.connect.de/news/joker-malware-android-apps-play-store-sicherheit-3202661.html?utm_source=connect-NL&utm_medium=newsletter

6) Nur 2 Klicks: Amazon Prime kündigen wird deutlich einfacher – das sagt Amazon

Nur noch zwei Klicks: Amazon vereinfacht die Kündigung von Prime. Aber erst auf Druck durch die EU-Kommission. Update: Das sagt Amazon.

Die Europäische Kommission hat mitgeteilt, dass Amazon sein vielfach kritisiertes Kündigungsverfahren für Amazon-Prime "mit den EU-Verbraucherschutzvorschriften in Einklang bringen" wolle. Mit anderen Worten: Es soll für Prime-Kunden deutlich einfacher werden, ihr Prime-Abonnement zu kündigen. Das teilte die EU-Kommission mit.

Mit nur 2 Klicks Amazon Prime kündigen

Konkret soll das laut der EU-Kommission bedeuten: "Für Verbraucherinnen und Verbraucher aus der EU und dem EWR wird es möglich sein, sich auf der Plattform mit nur zwei Klicks über eine markante und eindeutige 'Cancel'-Schaltfläche von Amazon Prime abzumelden.“

Amazon stand für seinen komplizierten Prime-Kündigungsprozess schon länger in der Kritik: Prime – Amazon soll Kündigungen bewusst erschweren. Die EU-Kommission schreibt dazu: "Nach einer Beschwerde des Europäischen Verbraucherverbands (BEUC), des norwegischen Verbraucherrats und des Transatlantischen Verbraucherdialogs wurde die Kommission im April 2021 in Zusammenarbeit mit nationalen Verbraucherschutzbehörden tätig. Das gemeldete Verfahren war so gestaltet, dass bei der Abmeldung zahlreiche Hindernisse überwunden werden mussten, darunter komplizierte Navigationsmenüs, unklare Formulierungen, verwirrende Wahlmöglichkeiten und wiederholte Verleitungstechniken ('Nudging'). Amazon hat sich nun verpflichtet, sein Abmeldeverfahren zu verbessern, und wird die **Änderungen ab heute umsetzen** ."

EU-Justizkommissar Didier Reynders bringt es auf den Punkt: "Online-Abonnements können eine praktische Sache sein, die Anmeldung ist meist unkompliziert. Die Abmeldung sollte aber genauso einfach sein. Die Verbraucherinnen und Verbraucher dürfen bei der Wahrnehmung ihrer Rechte keinem Druck durch die Plattformen ausgesetzt sein. Eine Sache ist jedenfalls klar: Manipulatives Design und 'Dark Patterns' gehören verboten. Ich begrüße die Zusage von Amazon, seine Verfahren zu vereinfachen, damit sich die Verbraucherinnen und Verbraucher frei entscheiden und auf einfachem Wege abmelden können."

In den letzten Monaten hat Amazon laut der EU-Kommission bereits Änderungen an seiner Prime-Website vorgenommen, die Schaltfläche für die Abmeldung klarer gekennzeichnet und den erläuternden Text verkürzt. Nun soll dieser Text noch weiter reduziert werden, sodass die Nutzer nicht durch Warnhinweise abgelenkt und von der Abmeldung abgehalten werden. Amazon soll schließlich die Möglichkeit bieten, sich in zwei einfachen Schritten über eine einfache, gut sichtbare Schaltfläche abzumelden. Amazon habe sich verpflichtet, diese Änderungen auf all seinen EU-Websites und für alle Geräte (Desktop, Mobilgeräte und Tablets) umzusetzen.

Die Kommission und die nationalen Behörden wollen genau beobachten, ob Amazon seine Zusagen zur Angleichung an das EU-Verbraucherrecht erfüllt.

Update 5.7.: Stellungnahme von Amazon

Amazon ist um Imagepflege bemüht und hat uns unaufgefordert die folgende Stellungnahme zugeschickt. Wir geben diese im vollen Wortlaut und ohne Kommentar wieder (es handelt sich um die Übersetzung des englischsprachigen Originaltexts): "Transparenz und Vertrauen der Kunden haben für uns höchste Priorität. Wir haben es so konzipiert, dass es für die Kunden klar und einfach ist, sich für eine Prime-Mitgliedschaft anzumelden oder diese zu kündigen. Wir hören uns ständig das Feedback an und suchen nach Möglichkeiten, das Kundenerlebnis zu verbessern, wie wir es hier nach einem konstruktiven Dialog mit der Europäischen Kommission tun."

Neue Nutzungsbedingungen: Wird Amazon Prime teurer?

Amazon: Zweiter Prime Day im Herbst 2022?

Amazon Prime Day im Juli: Termin steht fest

Quelle: https://www.pcwelt.de/news/Nur-2-Klicks-Amazon-Prime-kuendigen-wird-deutlich-einfacher-das-sagt-Amazon-11257425.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3690131&pm_cat%5B0%5D=Web+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Tankrabatt vs. Tanken im Ausland: App verrät, wo Benzin und Diesel günstiger sind

Tanken mit Tankrabatt in Deutschland oder aus grenznahen Orten schnell ins Ausland - was ist eigentlich günstiger? Eine App zeigt, ob sich das Tanken im Ausland für Sie lohnt. Auch der ADAC hat sich des Themas angenommen, denn die gleiche Frage stellt sich auch für viele Urlauber: Wie günstig kann ich im Ausland tanken?

Die hohen Benzin- und Dieselpreise haben Autofahrer lange genug kräftig zur Kasse gebeten. Jetzt ist der Tankrabatt da und wird auch an die Kunden weitergegeben. Von Anfang Juni bis Ende August gibt es in Deutschland die Entlastung bei den Spritpreisen. Für viele Urlauber stellt sich die Frage, ob es sich derzeit lohnt, in Deutschland zu tanken oder ob es im Ausland günstigeren Sprit gibt.

Grundsätzlich gilt, holen Sie sich unbedingt eine Benzinpreis-App, um günstige Tankstellen zu finden. Spritspartipps sind natürlich auch immer eine gute Sache, aber irgendwann kommt der Moment der Wahrheit an der Tanke.
Was oft ein guter Tipp ist, sind **ausländische Tankstellen**. Bei Ausflügen ins Ausland oder bei Urlauben mit dem Auto kann man den Tank einfach nochmal bei den Nachbarn vollmachen. Wer im Grenzgebiet wohnt, kommt dauerhaft günstiger an Sprit. Ob sich das überhaupt lohnt, zeigt die kostenlose App Benzinpreis-Blitz. Sie bietet offizielle Benzin- und Dieselpreis aus sieben Ländern.

- Achtung beim Tank-Tourismus: Diese Regeln müssen Sparfüchse einhalten!
- Benzin auf Vorrat kaufen: So viel Sprit dürfen Sie bunkern

Der ADAC hat Daten darüber zusammengestellt, was Benzin und Diesel im Vergleich zu Deutschland im europäischen Ausland kosten. Was man erkennen kann: In Deutschland liegen die Preise dank Tankrabatt für Verbraucher gar nicht so schlecht. Beim Abstecher nach Belgien, Dänemark, in die Niederlande oder nach Österreich zahlt man als Autofahrer an der Tanke mehr.

Doch wo ist es am günstigsten in Europa? Ungarn liegt bei Super und Diesel klar vorn. Doch Vorsicht, auch die Ungarn arbeiten mit einem Tankrabatt, doch der gilt nur für Fahrzeuge mit ungarischem Kennzeichen. Mit deutschem Kennzeichen zahlen Sie dort rund 60 Cent mehr pro Liter. Beim Superbenzin liegen derzeit nur Slowenien, Polen und Kroatien mit günstigeren Preisen vor Deutschland.
Beim Diesel kommen Tschechien und Luxemburg als Alternativen hinzu, Italien liegt auf dem Preisniveau von Deutschland. Der ADAC gibt an, dass man die ermittelten Werte nur als Richtschnur verwenden soll. Auch in anderen Ländern gibt es Preisschwankungen, außerdem sei die Datenbasis nicht immer perfekt, weil es großen Verzug bei den Preismeldungen gibt.

Spritpreise für 7 Länder einfach vergleichen

Benzinpreis-Blitz ist derzeit bei vielen Nutzern sehr beliebt, weil die App trotz des großen Nutzeransturms wie gewohnt schnelle und zuverlässige Ergebnisse liefert. Sie bietet auch nicht nur offizielle Spritpreisdaten aus Deutschland, sondern hat auch noch weitere Länder im Angebot:

- Österreich (nur Diesel, Super und CNG)
- Luxemburg
- Frankreich
- Portugal (ohne Madeira und die Azoren)

- Spanien
- Italien

Die Macher zapfen nur offizielle Quellen an, zum Beispiel die österreichische Schnittstelle bei E-Control. Deshalb gibt es in Österreich zum Beispiel auch keine Daten zu E10. Wichtig sind die rot und grün markierten Tankstellen. Rot bedeutet, dass an dieser Tanke Höchstpreise verlangt werden, grüne Einträge liefern den derzeit günstigsten Preis.

Anmerkung der Redaktion: Downloadmöglichkeit über den u.g. Link.

Quelle: https://www.chip.de/news/Tankrabatt-vs.-Tanken-im-Ausland-App-verraet-wo-Sprit-guenstiger-ist_184161748.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=04-07-2022%2B17%253A00%253A12&utm_content=nl_chipmob&utm_term=

8) Bevor die Rückkehr zum Albtraum wird: App vom Zoll verrät Ihnen, welche Souvenirs erlaubt sind

Eine echte Must-have-App für Urlaubsreisende: der Zoll bietet eine spannende Gratis-App zum Download. Damit wissen Sie immer, wie viel Alkohol, Parfum oder Tabakwaren Sie nach Deutschland einführen dürfen.

Golfschläger aus den USA, Schmuck aus Südafrika oder antike Münzen aus Griechenland: Das sind nur einige Beispiele von Gegenständen, die Sie nach Ihrem Urlaub beim Zoll anmelden oder eventuell sogar abgeben müssen. Neben diesen Exoten werden oft auch Tabak, Alkohol oder Bargeld mitgenommen – aber dafür gibt es Begrenzungen.

Damit Sie wissen, was rechtlich erlaubt ist, bietet das Bundesministerium der Finanzen die App Zoll und Reise zum kostenlosen Download an. Die gibt es sowohl für Android als auch für iOS.

"Zoll und Reise"-App: Unbesorgter reisen

Erlaubt oder nicht? Ein eigener Menüpunkt in der "Zoll & Reise"-App gibt Auskunft darüber, was Sie nach Deutschland einführen dürfen und was nicht. Wählen Sie dazu einfach erst das Land aus, aus dem Sie einreisen und danach die Waren, die Sie einführen wollen.

Zu jedem Land gibt es zudem immer den Punkt "Besondere Einschränkungen". Hier erfahren Sie, welche Sonderbestimmungen für das entsprechende Reiseland gelten.
Sollten Sie schon wissen, dass Sie Zoll entrichten müssen, hilft Ihnen der integrierte Abgaberechner dabei, den Endbetrag zu ermitteln. Ein umfangreicher FAQ-Bereich komplettiert die Zoll-App.

Spickzettel fürs Handgepäck

Wenn Sie lieber eine kompakte Übersicht bevorzugen, empfehlen wir Ihnen die Zollregeln als Spickzettels fürs Handgepäck. Die hat die Verbraucherzentrale in zwei Dokumenten zusammengetragen.

Auf einer bzw. zwei Druckseiten stehen die wichtigsten Zollregeln zusammengefasst für Reisen innerhalb und außerhalb der EU. Das ist für den Zoll eine der wichtigsten Unterscheidungsregeln.
Sie können direkt ablesen, wie es um die Mitnahme von Tabak, Alkohol, Kaffee, Medikamenten oder Bargeld steht. Auch Hinweise auf Ausnahmen oder teure Waren und Lebensmittel gibt es, sodass Sie nicht in Zollfallen treten.

Anmerkung der Redaktion: Downloadmöglichkeit über den u.g. Link

Quelle: https://www.chip.de/news/Bevor-die-Rueckkehr-zum-Albtraum-wird-App-vom-Zoll-verraet-Ihnen-welche-Souvenirs-erlaubt-sind_117674691.html?utm_source=nl_chipd-wy++&utm_medium=chip-newsletter&utm_campaign=03-07-2022%2B07%253A00%253A20&utm_content=nl_chipmob&utm_term=

9) Tipp: Signal-Nachrichten an Whatsapp weiterleiten

Es gibt zwei Möglichkeiten, wenn Sie eine Signalnachricht an Whatsapp weiterleiten wollen.

Problem: Sie sind von Whatsapp zu Signal gewechselt und wollen nun eine in Signal empfangene Nachricht an einen alten Whatsappkontakt weiterleiten. Doch da gibt es ein Problem.

Wenn Sie in Signal etwas länger auf eine vorhandene Nachricht tippen, erscheint zwar das Menü, mit dem Sie die Nachricht unter anderem weiterleiten können (das "Pfeil-nach-rechts-Icon"). Doch das geht nur innerhalb von Signal, Sie können die Nachricht also nur an einen anderen Signalkontakt weiterleiten.

Lösung

Falls Sie die Signalnachricht aber zum Beispiel via Whatsapp an einen Kontakt weiterleiten wollen, bleiben Ihnen zwei Möglichkeiten:

- Sie drücken länger auf die Signal-Nachricht und wählen aus dem erscheinenden Menü das Icon zum Kopieren aus (die beiden überlappenden Blätter mit dem eingeknickten rechten oberen Eck). Dann öffnen Sie Whatsapp und fügen den Text dort ein, indem Sie etwas länger auf das Eingabefeld drücken. Das klappt nicht nur mit Text, sondern auch mit Fotos. Dann drücken Sie auf Versenden. Fertig.
- Sie erstellen einen Screenshot des Bildschirms und fügen diese Bilddatei in Whatsapp ein und leiten sie weiter. Screenshots erstellen Sie bei einem Android-Smartphone, indem Sie Sie Einschalt-Taste und die Leiser-Taste gedrückt halten. Bei einem iPhone X, 11 oder 12 drücken Sie die Ein-/Aus-Taste und die Lauter-Taste. Bei älteren iPhones drücken Sie dagegen den Einschalt-Knopf und den Home-Button. Achtung: Schauen Sie sich den Screenshot genau an. Nicht dass sich darauf etwas Peinliches befindet, das Sie nicht weiterschicken möchten. Gegebenenfalls schneiden Sie das Bild also vor dem Versenden noch zu.

Diese App zeigt, welche Messenger Ihre Freunde nutzen

How-to: Umstieg von Whatsapp auf Signal

Die besten Whatsapp-Alternativen: Signal, Telegram, Threema etc

Die besten Signal-Tipps

- Signal: So verschicken Sie verschwindende Nachrichten
- So geht's: Signal für Notizen nutzen - einfacher als bei Whatsapp
- Signal Desktop: Messenger am PC nutzen - so geht’s mit Windows, Linux & Mac
- How-to: Umstieg von Whatsapp auf Signal

Quelle: https://www.pcwelt.de/tipps/Tipp-Signal-Nachrichten-an-Whatsapp-weiterleiten-10976957.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3659608&pm_cat%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

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

So speichern Sie sofort Filme aus den Mediatheken von ARD und ZDF auf Ihrem Rechner ab. Ohne Extra-Tool. Ein Browser reicht.

Die durch Ihren Rundfunkbeitrag mitfinanzierten Filme, Sendungen und Serienfolgen von ARD, ZDF und den anderen öffentlich-rechtlichen Sendern stehen in den Mediatheken nur für begrenzte Zeit zum Anschauen zur Verfügung. Doch Sie wollen spannende Filme dauerhaft abspeichern und sie danach jederzeit wieder anschauen können? Kein Problem, eine kostenlose Webseite macht den Download kinderleicht. So geht’s.

Suchen Sie nach der gewünschten Sendung

Öffnen Sie die Seite mediathekviewweb in Firefox, Chrome, Edge oder Safari oder in einem anderen kompatiblen Browser. Sie benötigen für die Nutzung dieser Seite kein Login und müssen dafür auch nicht zahlen. Geben Sie oben in das Feld neben „Suche“ den gewünschten Suchbegriff ein. Idealerweise haben Sie vorher im Web nach dem genauen Namen der Sendung gesucht und geben diesen nun ein.

Mediathekviewweb liefert Ihnen bereits bei der Eingabe in Echtzeit die passenden Treffer von ARD, ZDF, BR, HR und vielen anderen öffentlich-rechtlichen Sender. Darunter auch Beiträge von den spannenden Spartenkanälen wie ZDF Info, Arte oder Phoenix. Besonders ZDF Info ist für historisch Interessierte eine wichtige Informationsquelle.

Diese Optionen haben Sie

Zu jedem Treffer sehen Sie neben dem Sender und dem Titel auch das Erstveröffentlichungsdatum, die Uhrzeit und die Dauer. Wenn Sie auf das kleine blaue Dreieck hinter dem Titel klicken, bekommen Sie eine Kurzbeschreibung des Inhalts. Ganz am rechten Rand sehen Sie hinter einem blauen Film-Symbol die Optionen, die Ihnen nun zur Verfügung stehen. Klickern Sie darauf. Sie können den Film jetzt direkt im Browser streamen, vor allem aber können Sie den Film sofort herunterladen.

So starten Sie den Download

Sie haben beim Download die Wahl zwischen unterschiedlichen Dateigrößen. Sofern es Ihre Internetverbindung zulässt, sollten Sie die höchste Qualität nutzen. Klicken Sie dann auf das Diskettensymbol. Das Video startet jetzt in Firefox. Klicken Sie nun mit der rechten Maustaste auf das Video und wählen dann „Video speichern unter…“. Jetzt wählen Sie noch den Speicherort und schon startet der Download. Teilweise entfällt auch der Zwischenschritt mit dem Starten des Videos und Sie können das Video direkt aus Mediathekviewweb herunterladen.

Wenn Sie mehrere Downloads gleichzeitig starten, kann es etwas dauern, bis alle Downloads anlaufen und dann abgeschlossen sind. Gerade in der Zeit zwischen den Feiertagen Ende 2021 zog sich der Abschluss der Download mitunter etwas hin, wie unser Test zeigte. Da hilft dann nur: Geduld haben. Denn Mediathekviewweb arbeitet sehr zuverlässig. Doch derzeit scheint dieses Problem nicht zu bestehen, jüngste Tests zeigten, dass die Downloads ruck,zuck durchgeführt werden.

Such-Optionen

Für die Suche auf Mediathekviewweb stehen diverse Filter und Operatoren zur Verfügung, die hier erklärt werden.

Der Vorteil gegenüber der Mediathek-App von ARD und ZDF

Zwar bieten die Apps der Mediatheken von ARD und ZDF für iOS und Android auch eine „Download-Funktion“. Doch dabei handelt es sich nur um eine Offline-Anschauen-Funktionen und nicht um einen wirklichen Download. Denn sobald besagter Film aus der Mediathek entfernt wird, lässt er sich auch nicht mehr in der App betrachten. Zudem können Sie solche Filme immer nur innerhalb der Mediathek-App anschauen. Laden Sie dagegen den Film mit Mediathekviewweb auf Ihren Rechner herunter, dann steht Ihnen dieser zeitlich unbefristet zum Anschauen auf allen Geräten zur Verfügung.

Vorteil gegenüber Mediathekview

Mediathekview gibt es auch als Gratis-Tool. Doch bei Mediathekviewweb müssen Sie im Unterschied zu Mediathekview keine Software installieren, sondern benötigen nur einen kompatiblen Browser. Bequemer geht es nicht. Zumal Mediathekview in der Vergangenheit immer mal wieder Probleme bereitete. Falls Sie aber trotzdem lieber das Tool nutzen wollen, dann lesen Sie hier weiter: Videos aus ZDF Mediathek direkt herunterladen.

ARD Retro: ARD Mediathek zeigt ab sofort viele historische TV-Aufnahmen

Quelle: https://www.pcwelt.de/ratgeber/ARD-und-ZDF-Mediathek-Filme-sofort-herunterladen-so-geht-s-11159865.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3681885&pm_cat%5B0%5D=Productivity+Software&pm_cat%5B1%5D=Apps&pm_cat%5B2%5D=Kreativ+Software&pm_cat%5B3%5D=Suche&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

11) Gratis: Vier geniale Hotspot-Finder

Sie sind unterwegs immer auf der Suche nach einem Hotspot für Ihr Notebook? Mit unseren vier kostenlosen Wlan-Tools spüren Sie jeden verfügbaren Hotspot auf.

Easy WiFi Radar

Das Wlan-Tool Easy WiFi Radar scannt die Umgebung Ihres Notebooks und listet alle verfügbaren WLAN-Zugänge auf einem "Radarschirm" auf. Access Points, die abgesichert sind, werden als rote Punkte dargestellt, offene Access Points markiert Easy WiFi Radar grün.

Praktisch: Easy WiFi Radar öffnet den Browser, sobald es einen neuen offenen Zugang entdeckt. Sie müssen dann nur noch Ihre Zugangsdaten eintippen und lossurfen.

Easy WiFi Radar ist eine deutschsprachige Freeware für Windows XP, Vista und Windows 7.

Download Easy WiFi Radar

NetStumbler

NetStumbler findet alle aktiven Wlans und zeigt diese zusammen mit der SSID (Service Set Identifier) an. Zusätzlich nennt NetStumbler zu allen aufgespürten Wlans die Verschlüsselungsmethode und den Funkkanal.

Das englischsprachige NetStumbler ist für die private Nutzung kostenlos. Vistumbler ist eine Alternative.

Download NetStumbler

Boingo

Boingo findet rund um den Globus HotSpots und verbindet Sie nahezu vollautomatisch mit den entsprechenden Zugängen, gegebenenfalls müssen Sie nur noch Ihr Passwort eingeben. Das

Profil zu dem entdeckten Zugang können Sie in Boingo abspeichern.

Boingo nutzt hierfür eine eigene Datenbank, in der US-amerikanische und europäische Hotspots eingetragen sind. Darunter befinden sich auch Hotspots für mehr als 1700 Orte in Deutschland.

Boingo ist eine englischsprachige Freeware für Windows XP und Vista, Windows 8.1 und Windows 10.

Download Boingo

Online Manager der Telekom

In den Online Manager der Telekom ging vor Jahren der "HotSpot Manager" auf. Er listet alle verfügbaren Access Points in Ihrer Umgebung auf. Sie können sich mit dem Online Manager (Hotspot Manager) aber auch vor Beginn einer Reise darüber informieren, welche Access Points am Einsatzort verfügbar sind. Das Tool nutzt hierzu seine integrierte Datenbank.

Download Online Manager.

Quelle: https://www.pcwelt.de/ratgeber/Wlan-Tools-Vier-geniale-Hotspot-Finder-441648.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=2105336&pm_cat%5B0%5D=Notebook+Ultrabook&pm_cat%5B1%5D=Betriebssystem&pm_cat%5B2%5D=LAN+WAN+WLAN&pm_cat%5B3%5D=Productivity+Software&pm_cat%5B4%5D=Netzwerktechnologie&pm_cat%5B5%5D=Kreativ+Software&pm_cat%5B6%5D=Microsoft&pm_cat%5B7%5D=Netzwerke+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

12) Wenn nix mehr funktioniert: Notfall-IP für den Router kennt kaum jemand

Manchmal ist der WLAN-Router unerreichbar. Dann kann die sogenannte Notfall-IP helfen – doch das Ganze hat einen Haken, denn längst nicht alle Hersteller bieten diese praktische Funktion.

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

Wenn Sie die Standardeinstellungen nicht geändert haben, können Sie eine FritzBox auch immer über die IP-Adresse **192.168.178.1** erreichen. Bei den meisten FritzBoxen dürfte diese Einstellung unangetastet sein. Wenn Sie einen Reset ausführen, ist das immer die vorgegebene IP-Adresse. Doch Sie können die IP-Range auch anpassen, sodass diese Adresse ins Leere läuft.
Bei Fehlkonfigurationen oder wenn Sie die IP-Adresse vergessen haben, gibt es auch immer noch eine Notfall-IP. Diese ist für alle FritzBoxen gleich. Standard ist so eine Notfall-IP in der Router-Welt zwar nicht, der ein oder andere Hersteller baut sie aber auch ein.

FritzBox Notfall-IP nutzen

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

Das kann zum Beispiel dann nützlich sein, wenn Sie mit FritzBox und Repeatern ein Mesh-

Netzwerk aufgebaut haben und die Konfiguration Probleme macht. Über die Notfall-IP sollten Sie dann immer bei der FritzBox oder dem angedockten FritzRepeater landen. Außerdem ist die Notfall-IP nützlich bei DNS- oder DHCP-Fehlern.

Dass FritzBoxen keine schlechte Wahl sind, sehen Sie in unserer Bestenliste WLAN-Router. Doch nicht jeder hat ein AVM-Gerät als WLAN-Router zu Hause stehen. Wir zeigen, wie Sie die Konfigurationsoberflächen anderer WLAN-Router per URL und Standard-IP erreichen und ob es dort auch Notfall-IPs gibt.

Anmerkung der Redaktion: WLAN-Router Konfigurationsoberflächen können unter dem u.g. Link abgerufen werden.

Quelle: https://www.chip.de/news/Wenn-nix-mehr-funktioniert-Notfall-IP-fuer-den-Router-kennt-kaum-jemand_184311389.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=27-06-2022%2B17%253A00%253A18&utm_content=nl_chipmob&utm_term=

13) Ist diese Datei gefährlich? Die besten Online-Virenscanner schaffen Klarheit

Wenn Sie sich unsicher sind, ob ein Download Viren enthalten könnte, dann greifen Sie am besten zu kostenlosen Online-Scannern. Diese wissen, welche Dateien vertrauenswürdig sind.

"Better safe than sorry" heißt es im Englischen. Frei übersetzt sollte man lieber vorsichtig sein, als später das Nachsehen zu haben. Dasselbe gilt auch bei Downloads im Internet, die Sie keinesfalls voreilig anklicken und installieren sollten – insbesondere dann nicht, wenn diese aus unbekannten Quellen stammen.

Wenn Sie auf den Windows Defender schwören und kein Antivirus-Programm nutzen wollen, können Sie sich mit schnellen Malware-Prüfungen im Browser trotzdem eine zweite Sicherheitsbarriere einrichten. Wir stellen Ihnen drei top Online-Virenscanner vor, mit denen Sie alle Dateien in wenigen Sekunden analysieren.

VirusTotal: 69 Antivirus-Programme scannen Files

Die wohl bekannteste und zuverlässigste Lösung ist VirusTotal. Obwohl die Web-Anwendung nur auf Englisch verfügbar ist, lässt sie sich sehr leicht bedienen: Sie müssen lediglich die fragliche Datei (bis 650 MB) per Drag-and-drop in den Browser ziehen und schon beginnt der Scan.

Nach wenigen Sekunden wird das Ergebnis angezeigt. Ist der Kreis komplett grün, können Sie das fragliche Programm bedenkenlos installieren – in den meisten Fällen werden aber zumindest ein paar Antivirus-Programme einen Alarm geben. Schauen Sie hier, ob es sich um namhafte AV-Hersteller handelt oder eher unbekannte, anschließend können Sie immer noch etwas tiefer recherchieren.
Erst wenn sehr viele Einträge in der Liste rot gefärbt sind, stimmt mit einer Datei garantiert etwas nicht. Dann sollten Sie lieber die Finger davon lassen. Übrigens können Sie bei VirusTotal unter dem Reiter "URL" auch vor dem Download einfach den Link zu einer EXE-Datei einfügen, um diese zu scannen. Damit sparen Sie sich bereits das Risiko, nicht vertrauenswürdige Links überhaupt anzuklicken.

Alternative: Jotti's Malware Scan

Ganz ähnlich wie VirusTotal funktioniert die Alternative Jotti's Malware Scan, die Sie etwa verwenden können, um sich eine zweite Meinung einzuholen. Den kostenlosen Dienst gibt es

schon seit über 15 Jahren, er verwendet ebenfalls mehrere Engines zum Scannen von Dateien. Dabei konzentriert sich der Dienst auf die wichtigsten Hersteller und erlaubt den gleichzeitigen Upload von bis zu fünf Dateien.

Praktisch dabei ist, dass die Anwendung auf Deutsch ist und die Ergebnisse des Scans damit glasklar zu erkennen sind. Ebenfalls wie bei VirusTotal gibt es eine Suchfunktion für den Hash eines Scans, der Link zum Ergebnis einer untersuchten Datei lässt sich leicht kopieren und verschicken – schicken Sie diesen zum Beispiel an eine fachkundige Person in Ihrem Bekanntenkreis.

Im Ernstfall: Online-Scanner von AV-Herstellern

Haben Sie einen Verdacht, dass es eine unerwünschte Software doch auf Ihr System geschafft hat, helfen kostenlose Online-Scanner von namhaften Herstellern wie ESET oder F-Secure auf die Schnelle weiter. Hier laden Sie einfach eine kleine EXE-Datei herunter und starten diese per Doppelklick – ganz ohne Installation scannen die Tools dann Ihr komplettes System durch.

Sollten dabei Malware, Trojaner oder Viren gefunden werden, entfernen die Online-Scanner diese sogleich. Allerdings klappt dies in der Regel nicht bei brandaktuellen Bedrohungen, sondern nur bei bereits bekannten. Da hilft am Ende nur eine richtige Antivirus-Suite.

Anmerkung der Redaktion: Die entsprechenden Programme können unter dem u.g. Link downgeloaded werden.

Quelle: https://www.chip.de/news/Ist-diese-Datei-gefaehrlich-Die-besten-Online-Virenscanner-schaffen-Klarheit_183547319.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=27-06-2022%2B17%253A00%253A18&utm_content=nl_chipmob&utm_term=

Allgemeines:

1) Musterfeststellungsklage gegen Primastrom & Voxenergie geplant – so nehmen Sie teil

Die Verbraucherzentrale Bundesverband plant eine Musterfeststellungsklage gegen Primastrom und Voxenergie. So nehmen Sie als betroffener Strom-Kunde teil.

Der Verbraucherzentrale Bundesverband (vzbv) plant eine Musterfeststellungsklage gegen die Strom- und Gasversorger Primastrom und Voxenergie wegen deren Preiserhöhungen. Die Verbraucherschützer begründen ihr Vorhaben folgendermaßen: "Die Energieanbieter hatten immer wieder die Preise erhöht, obwohl im Vertrag etwas anderes festgelegt war. Der vzbv hält das für unzulässig. Verbraucher sollen nur die Preise zahlen, die vertraglich vereinbart sind und pocht auf die Einhaltung der Verträge."

Die Verbraucherschützer erheben schon länger Vorwürfe gegen Primastrom und Voxenergie. Seit Monaten würden sich Kunden von Primastrom und Voxenergie bei der Verbraucherzentrale über die beiden Stromlieferanten beschweren. Auch pcwelt.de berichtete darüber, dass Verbraucherschützer vor diesen beiden Stromlieferanten warnen würden. Wir baten damals Primastrom und Voxenergie um eine Stellungnahme. Nach rund einer Woche erreichte uns statt der Stellungnahme einer Pressestelle ein rechtsanwaltliches Schreiben: Voxenergie & primastrom – Antwort auf Vorwürfe der Verbraucherschützer. Diese Vorgehensweise von Primastrom und Voxenergie ist völlig unüblich und entspricht nicht der gängigen Praxis von Unternehmen.

So nehmen Sie an der Musterfeststellungsklage teil

"Mit einer Klage soll festgestellt werden, dass die Verbraucher lediglich die vertraglich vereinbarten Preise zahlen müssen", sagt Patrick Langer, Referent im Team Musterfeststellungsklagen. "Zur Vorbereitung der Klage sucht der vzbv jetzt Betroffene, die ihren Fall auf musterfeststellungsklagen.de/primastrom-und-voxenergie einreichen."

Die Verbraucherschützer betonen: Musterklagen sind für Verbraucher kostenfrei.

In dieser FAQ informieren die Verbraucherschützer über Primastrom und Voxenergie.

Bundesnetzagentur leitet Aufsichtsverfahren gegen Primastrom und Voxenergie ein

Bereits am 24. Mai 2022 teilte die Bundesnetzagentur mit, dass sie ein Aufsichtsverfahren gegen die beiden Unternehmen eingeleitet habe: "Wir prüfen, ob die Unternehmen Preiserhöhungen vorgenommen haben, ohne die gesetzlich vorgesehenen Ankündigungsfristen einzuhalten. Auch in Phasen einer angespannten Marktsituation müssen sich die Verbraucher darauf verlassen können, dass sie rechtzeitig über Vertragsänderungen informiert werden", sagt Klaus Müller, Präsident der Bundesnetzagentur. Laut Bundesnetzagentur bestehe gegen Primastrom und Voxenergie der Verdacht unzulässiger Preiserhöhungen. Die Bundesnetzagentur erklärt: " *Es besteht der Verdacht, dass die voxenergie GmbH und die primastrom GmbH die Unterrichtung der Kunden über eine Preiserhöhung nicht rechtzeitig vor Eintritt der beabsichtigten Änderung vorgenommen haben. Grundlage sind Beschwerden von Verbrauchern bei der Bundesnetzagentur und den Verbraucherzentralen.*

Die Unternehmen verschickten am 28. Dezember 2021 Ankündigungsschreiben zur Erhöhung der vereinbarten Preise. Die höheren Preise sollten bereits ab dem 1. Januar 2022 gelten.

Gesetzlich vorgeschrieben ist, dass Haushaltskunden über Preisänderungen spätestens einen Monat und alle übrigen Letztverbraucher spätestens zwei Wochen vor Eintritt der beabsichtigten Änderung unterrichtet werden. Kunden haben im Falle einer Preiserhöhung ein Sonderkündigungsrecht, das bis zum Zeitpunkt des Wirksamwerdens der Änderung auszuüben ist. "

Quelle: https://www.pcwelt.de/news/Musterfeststellungsklage-gegen-Primastrom-Voxenergie-geplant-so-nehmen-Sie-teil-11261777.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3690271&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

2) VW Multivan: Kopfairbags können versagen & Brandgefahr - zurück in die Werkstatt

Der neue VW Multivan muss in die Werkstatt. Da sein Airbag versagen und das Fahrzeug im schlimmsten Fall sogar Feuer fangen kann. Alle Informationen zum Rückruf.

Volkswagen Nutzfahrzeuge VWN muss erneut einen Rückruf für den T7 Multivan einleiten. Aus einem ernsten Grund: Der Kopfairbag kann versagen. Das berichtet unter anderem das Fachportal Kfz-Vogel .

Der Rückruf hat sogar zwei Gründe, die beide die Funktionssicherheit der Airbags betreffen. Erstens "könnten Clips zur Befestigung der Bauteile nicht richtig gesetzt worden sein" Und zweitens "besteht die Möglichkeit, dass Leitungsstränge im Bereich des Kopfairbags fehlerhaft verlegt worden sind". Das könnte dazu führen, dass der Kopfairbag nicht optimal schützt, falls er ausgelöst wird.

Die verlegten Dachleitungsstränge könnten außerdem zu "diversen Funktionsstörungen" führen. So könnte deswegen sogar das Fahrzeug liegen bleiben und es bestehe sogar eine erhöhte Brandgefahr. Beides klingt für sich allein genommen nicht gerade erfreulich und in Zusammenhang mit einem potenziell lebensrettenden Bauteil ist das ganz besonders beunruhigend.

Diese Fahrzeuge sind betroffen

Betroffen sind von beiden Airbag-Mängeln T7 aus den Fertigungszeiträumen September 2021 bis März 2022 (so weit es die Clips betrifft) beziehungsweise bis Mai 2022 (so weit es die Leitungsproblematik betrifft), wie KFZ Vogel schreibt.

In Deutschland müssen deshalb knapp 4300 T7 Multivan für rund vier Stunden in die Werkstatt, weltweit fast 8000 Fahrzeuge. Der interne Aktionscode dafür laut "69DP". Die Mitarbeiter bauen den "Formhimmel" im T7 ab und überprüfen, ob die Befestigungschips korrekt verbaut sind. Außerdem überprüfen die Mitarbeiter, ob die Leitungen korrekt verbaut sind. Zusätzlich schützen die Mitarbeiter den Leitungssatz mit zusätzlichem Vliesklebeband im Bereich der Halterposition. Dieses nachträgliche Anbringen von Klebebändern erinnert fast schon an die nachträglichen improvisierten Reparaturen von Tesla…

Studie: Tesla baut die Autos mit den meisten Fehlern

VW Multivan T7 eHybrid muss in die Werkstatt - Brandgefahr

Bereits der zweite Rückruf für den T7

Das ist bereits der zweite Rückruf für den im Jahr 2021 vorgestellten T7 Multivan, der ein völlig anderes Fahrzeug ist als der Vorgänger T6x. Denn bereits im April 2022 rief Volkswagen eine Reihe von Plugin-Hybrid-Fahrzeugen zurück, darunter auch den T7: VW ruft Fahrzeuge zurück - ein neuer Golf brannte aus . Damals brannte ein neuer T7 Multivan sogar aus.

Quelle: https://www.pcwelt.de/news/VW-Multivan-Kopfairbags-koennen-versagen-Brandgefahr-zurueck-in-die-Werkstatt-11262702.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3699915&pm_cat%5B0%5D=Karriere+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

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

Ab dem 6. Juli 2022 muss eine Reihe von Assistenzsystemen in neuen Autos verbaut werden. Um diese Systeme handelt es sich.

Mit Stichtag 6. Juli 2022 müssen in Fahrzeugen, die neu entwickelt auf den Markt kommen (Typzulassung), bestimmte Assistenzsysteme als Serienausstattung vorhanden sein. Ab 2024 müssen die genannten Assistenzsysteme dann in allen Neuwagen verbaut sein. Konkret handelt es sich laut TÜV Nord um die folgenden Assistenzsysteme.

Notbremsassistent

Erkennen die Kameras – eventuell auch Radar- oder Lidarsensoren, sofern vorhanden – eine Kollisionsgefahr mit einem stehenden oder sich bewegenden Hindernis (derzeit gilt das nur für Autos, in Zukunft sollen aber auch Fußgänger und Radfahrer zuverlässig erkannt werden), dann bremst der Notbremsassistenz das Fahrzeug automatisch ab oder verlangsamt zumindest dessen Geschwindigkeit deutlich bis zur Kollision. Der Fahrer kann diesen Assistenten von Hand deaktivieren, er ist aber bei einem Neustart automatisch wieder eingeschaltet.

Aktiver Notfall-Spurhalteassistent

Dieser Assistent erkennt, wenn das Fahrzeug ungewollt die Fahrspur verlässt und lenkt dann aktiv gegen. Der TÜV Nord betont: "Der Notfall-Spurhalteassistent schaltet sich automatisch ab, wenn er 'insbesondere aufgrund von Mängeln in der Straßeninfrastruktur' so der Verordnungstext, nicht zuverlässig arbeiten kann. Der Fahrer erhält dann im Cockpit einen Hinweis. Nach dem Fahrzeugstart ist der Notfall-Spurhalteassistent wieder aktiv."

Geschwindigkeitsassistent

Er warnt, wenn die geltende Geschwindigkeit überschritten wird. Seine Daten für das geltende Tempolimit bezieht er aus der Verkehrszeichenerkennung und aus Positionsdaten. Mit dem Einschalten der Zündung aktiviert sich das System, der Fahrer kann es aber manuell abschalten.

Notbremslicht/adaptives Bremslicht

Bei einer gewöhnlichen Bremsung leuchten die Bremslichter wie gehabt. Bei einer Notbremsung jedoch – also bei einer Bremsung mit einer Verzögerung von über 6 m/s und einem Tempo von über 50 km/h – blinken die Bremslichter mehrmals pro Sekunde und warnen so die Verkehrsteilnehmer hinter dem bremsenden Fahrzeug. Das Notbremslicht schaltet sich außerdem dazu, solange das ABS-System regelt. Steht das Fahrzeug nach einer derartigen Vollbremsung, dann schaltet sich die Warnblinkanlage zu, das Bremslicht leuchtet dauerhaft.

Seine Auslösedaten bezieht das Notbremslicht von Steuergeräten, Pedaldruck, Bestätigungstempo des Bremspedals, ESP- und ABS-Eingriffen und dem Tempo des Fahrzeugs. Zudem wird die Reifenhaftreibung ermittelt, wie der TÜV Nord schreibt.

Unfalldatenspeicher/ereignisbezogene Datenaufzeichnung/Black-Box

Dieses System speichert Daten (Geschwindigkeit, Bremsung, Position, Neigung, Daten aus dem eCall) unmittelbar vor, während und nach einem Zusammenstoß. Diese Daten sind zwecks Datenschutz anonymisiert und können nationalen Behörden zum Zweck der Unfallforschung zur Verfügung gestellt werden. Der Fahrer kann den Unfalldatenspeicher nicht deaktivieren.

Müdigkeits- und Aufmerksamkeitswarner

Das System soll den gefährlichen Sekundenschlaf verhindern. Hierzu erfasst eine Kamera durchgehend die Augen- und Lidbewegungen. Zusätzlich oder als Ersatz können die Lenkbewegungen ausgewertet werden. Erkennt das System Hinweise für Müdigkeit, dann erinnert es den Fahrer akustisch und optisch daran, eine Pause zu machen.

Rückfahrassistent

Der Assistent erkennt Passanten oder Hindernisse hinter dem Fahrzeug und warnt den Fahrer, wenn das Auto rückwärts fährt. Das System wertet dafür Ultraschallsensoren und Kameras aus.

Reifendrucküberwachung

Reifendruck-Kontrollsysteme sind bereits seit 2014 in neu zugelassenen Pkws Pflicht. Ab 2022 müssen aber auch Nutzfahrzeuge, LKWs und Busse damit ausgestattet werden, ebenso große Lkw-Anhänger.

Vorrichtung zum Einbau einer alkoholempfindlichen Wegfahrsperre

Alle Neuwagen müssen über eine standardisierte Schnittstelle verfügen, die das Nachrüsten

einer alkoholempfindlichen Wegfahrsperre ermöglicht. Das Kontrollgerät (beispielsweise ein Atemalkohol-Gerät) selbst muss aber noch **nicht** verbaut werden.

Folgen für die Fahrzeugbesitzer

Die oben beschriebenen Systeme sind in vielen Fahrzeugen, insbesondere solchen der gehobenen Preisklasse, oft schon seit Jahren verbaut. Jedenfalls sind solche Assistenten längst schon gegen Aufpreis erhältlich. Die Assistenzsysteme sollen Unfälle verhindern oder zumindest abmindern beziehungsweise deren Rekonstruktion ermöglichen. Das ist unbestritten wünschenswert, um die Zahl der Verkehrsopfer weiter senken zu können.

Doch für die Fahrzeughalter resultieren daraus Mehrkosten. Nicht nur, weil die Automobilhersteller die genannten Systeme vermutlich zum Anlass nehmen, um die Neuwagenpreise anzuheben. Sondern vor allem langfristig bei der Wartung: denn jede in einem Auto verbaute Technik geht einmal kaputt und muss dann ersetzt werden. Und sie muss schon allein deswegen ersetzt werden, weil die Funktionsfähigkeit der Assistenzsysteme alle zwei Jahre bei der TÜV-Untersuchung überprüft wird. Stellt sich dann heraus, dass die Komponenten eines Fahrerassistenzsystems defekt sind – beispielsweise eine Kamera oder ein Sensor – dann steht eine teure Reparatur an, um die begehrte TÜV-Plakette doch noch zu bekommen.

Obendrein müssen Sie natürlich alle Sensoren wie Kameras, Ultraschall und Radar/Lidar sauber und frei von Schmutz, Schnee oder Eis halten, damit diese funktionieren können. Übrigens macht die ganze Sicherheitstechnik die Autos immer schwerer .

- Trotz Elektronik: Das sind Deutschlands tödlichste Straßen - so überleben Sie
- Weniger Verkehrstote als je zuvor - mit einer Ausnahme
- Verkehrstote 2020: Fußgänger & Radfahrer flop, Auto- & Motofahrer top
- 2019: So wenig Verkehrstote wie nie zuvor, aber...
- Auto- und Motorradfahrern drohen jetzt tödliche Unfälle mit Mähdreschern

Quelle: https://www.pcwelt.de/news/Ab-6.7.-Diese-Systeme-werden-jetzt-Pflicht-im-Auto-mehr-Sicherheit-hoehere-Kosten-11258258.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3690155&pm_cat%5B0%5D=Hardware+allgemein&pm_cat%5B1%5D=Datenbank&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Überblick & Tool: Diese Porto-Preise gelten für Briefe, Postkarten, Pakete etc.

Die Deutsche Post hatte zum 1. Januar 2022 das Briefporto erhöht. Für Pakete gelten ab 1.7.2022 neue Preise. Alle neuen Preise in übersichtlichen Tabellen. Plus: Dieses Online-Tool berechnet sofort das Porto.

1. Briefe und Postkarten: Seit dem 1. Januar 2022 gelten diese Portopreise

- Der Standardbrief kostet 0,85 Euro – fünf Cent teurer als zuvor
- Der Kompaktbrief kostet 1 Euro – fünf Cent teurer
- Der Großbrief kostet 1,60 Euro – fünf Cent teurer
- Der Maxibrief kostet 2,75 Euro – fünf Cent teurer
- Die Postkarte kostet 0,70 Euro und damit zehn Cent mehr als bisher

- Die Preise für das Einschreiben und Einschreiben Einwurf steigen um 15 Cent auf 2,65 Euro bzw. 2,35 Euro.

Passende Briefmarken

Die Deutsche Post bietet passend zur Portoerhöhung neue Briefmarken sowie Ergänzungsmarken an. Diese sind seit dem 2. Dezember 2021 in den Postfilialen und online unter www.deutschepost.de erhältlich. Sie benötigen also beispielsweise 0,05-Cent-Briefmarken, um vorhandenen 80-Cent-Briefmarken fit zu machen für das neue Porto für den Standardbrief. Oder 10-Cent-Briefmarken, um vorhandene 60-Cent-Briefmarken für das neue 70-Cent-Porto für Postkarten geeignet zu machen.

Kunden können das Porto für ihre Briefe und Postkarten weiterhin auch über die Post & DHL App kaufen oder die Sendungen mit der mobilen Briefmarke über die App frankieren. Vorhandene Briefmarken wie auch noch vorhandene Ergänzungsmarken aus den Vorjahren können für die Frankierung von Sendungen mit der Deutschen Post weiter verwendet werden. Ein Umtausch ist nicht nötig.

Tipp: Porto ganz einfach berechnen

Dieses Online-Tool berechnet das Porto für Briefe, Postkarten, Päckchen und Pakete.

Weitere Portoerhöhungen

Daneben erhöhte die Deutsche Post auch einige Preise für Produkte, die anders als die oben genannten Briefporti nicht der vorherigen Genehmigung durch die Bundesnetzagentur bedürfen. So stiegen auch die Preise für die **Bücher- und Warensendung** um fünf Cent auf 1,95 Euro für die "Bücher- und Warensendung 500" und auf 2,25 Euro für die "Bücher- und Warensendung 1000".

Beim **Nachsendeservice** stieg der Online-Preis für das 12-Monate-Produkt von 26,90 Euro für Privatkunden auf 30,90 Euro. Der Online-Preis für die 6-Monate-Variante bleibt dagegen unverändert bei 23,90 Euro (Privatkunden). Kunden können den 6-Monate-Service künftig auch in der Filiale beauftragen können, dann allerdings zu höheren Preisen als online: 26,90 Euro.

2. Paketpreise für Geschäftskunden

Die Deutsche Post DHL erhöhte mit Wirkung zum 1.1.2022 auch die **Paketpreise für Geschäftskunden.** Diese Preiserhöhungen gelten sowohl für Geschäftskunden mit Listenpreisen als auch für Geschäftskunden mit individuell vereinbarten Konditionen. Die Preiserhöhung betrifft in besonderem Maße schwere Paketsendungen über 20 Kilogramm. Die Post begründete das damit, dass damit in der Sortierung und bei der Auslieferung ein deutlich höherer Aufwand erforderlich sei. Die Erhöhungen betreffen aber nicht das nationale und internationale DHL Express-Geschäft.

3. Paketpreise für Privatkunden

Ab dem 1. Juli 2022 gelten auch für Privatkunden neue Preise, wie Sie hier lesen: DHL – Viele Päckchen und Pakete werden teurer. Mit einer wichtigen Ausnahme **.** Dort finden Sie auch alle Preistabellen.

Langes Genehmigungsverfahren

Der Portoerhöhung war ein längeres Genehmigungs- und Prüfverfahren vorausgegangen, mehr dazu lesen Sie in der Meldung Deutsche Post darf Brief-Porto erhöhen: Das kosten Briefe ab 1.1.2022. Die Bundesnetzagentur hatte schließlich am 10. Dezember 2021 "die

neuen Briefporti der Deutschen Post AG ab 1. Januar 2022 vorläufig genehmigt. Die endgültige Genehmigung erfolgt voraussichtlich im Frühjahr", schrieb damals die Bundesnetzagentur.

Begründung für Preiserhöhung

Die Deutsche Post nannte als Grund für die Preisanpassungen „Kostensteigerungen durch höhere Lohn- und Transportkosten sowie die in den vergangenen Monaten stark gestiegene Inflationsrate. Auch Pandemie-bedingte Zusatzaufwendungen in den Betriebsstätten und in der Zustellung, die eine sichere Postversorgung für alle Kunden in Deutschland ermöglichen, haben die Deutsche Post mit erheblichen Kosten belastet."

Anmerkung der Redaktion: Die jetzt gültigen Preistabellen können über den u.g. Link abgerufen werden.

Quelle: https://www.macwelt.de/news/Ueberblick-Tool-Diese-Porto-Preise-gelten-fuer-Briefe-Postkarten-Pakete-etc.-11152209.html?utm_source=macwelt-daily-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=0&pm_cat%5B0%5D=Apps&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057edd57f800a8db1ca4e20d8a3858ac410c4c4

5) Landeskriminalamt rät: So schützen Sie Ihr Geld im Urlaub am besten

Besonders im Urlaub sollten Sie darauf achten, welches Zahlungsmittel Sie wie einsetzen. Das LKA gibt hilfreiche Tipps, wie sich Urlauber vor Betrug und Diebstahl schützen können.

Unbeschwert den Urlaub genießen und einmal nicht an Geld denken – das wünschen sich viele. Doch genau das macht Touristen anfällig für Diebstahl und Abzocke.

Damit Sie Ihren Urlaub auch wirklich genießen können, sollten Sie also zumindest ein paar grundlegende Dinge beim Bezahlen beachten, besonders wenn Sie sich im Ausland befinden. Zum Beispiel kann nicht überall die Girocard genutzt werden, in anderen Ländern ist oft eine Visa- oder Mastercard nötig. Auch an Gebühren für Abhebungen und Zahlungen im Ausland sowie an Schutzmaßnahmen gegen Diebstahl und Betrug sollten Sie denken.
Wie Sie alles Wichtige im Blick behalten und im Urlaub sicher und ohne Probleme bezahlen können, zeigt das Landeskriminalamt (LKA) Niedersachsen.

Die richtige Vorbereitung: Bezahlen im Auslandsurlaub

Bevor es in den wohlverdienten Urlaub geht, sollten ein paar Vorbereitungen getroffen werden.

Ein häufiger Fehler: Zu viel Bargeld mitnehmen. Auch wenn sich viele mit mehreren hundert Euro in der Tasche besser vorbereitet fühlen – wenn das Portemonnaie direkt am Flughafen geklaut wird, ist der Urlaub schon vor Abflug futsch.
Besser: Geringe Geldbeträge in bar mitnehmen. Am besten in kleinen Scheinen, um Schwierigkeiten beim Rückgeld zu vermeiden. Statt viel Bargeld rät das LKA zu einem Mix an Zahlungsmitteln.
Mindestens zwei gültige Bankkarten sollten Sie dabei haben, für den Fall das eine Karte nicht angenommen wird oder defekt ist. Selbstverständlich: Die PIN nicht mit der Karte aufbewahren, sondern auswendig lernen.
Außerdem sollten Sie sich vorher darüber informieren, ob Sie Ihre Girocard im Ausland einsetzen können und welche Gebühren Sie die Auslandsnutzung kostet.

Während des Urlaubs: So schützen Sie sich vor Betrug und Diebstahl

Mit wenig Bargeld in kleinen Scheinen, mindestens zwei funktionsfähigen Bankkarten und einem Überblick über Kosten für die Auslandsnutzung kann der Urlaub nun losgehen.

Im Zielland angekommen warten aber bereits die nächsten Fallstricke. Besonders an touristischen Orten kommt es immer wieder zu Diebstahl und Kreditkarten-Betrug. Im dichten Gedränge, etwa auf Märkten, Festen oder vollen Stränden lauern die meisten Taschendiebe, hier sollten Sie besonders gut auf Ihre Wertsachen achten.
Um bestmöglich vor Diebstahl geschützt zu sein, tragen Sie Geldbeutel und andere Wertsachen immer nah am Körper, am besten verteilt in verschiedenen, verschlossenen Innentaschen Ihrer Kleidung oder in einem Brustbeutel.
Auch in vermeintlich sicheren Orten wie Hotelzimmer oder Ferienwohnung sollten Sie Ihren Geldbeutel nie unbeaufsichtigt zurücklassen, schon gar nicht im Mietwagen.

Sicher im Urlaub bezahlen

Beim Bezahlen mit der Karte rät das LKA zu folgendem:

- Die PIN-Eingabe immer verdeckt und mit ausreichend Abstand zu anderen Personen vornehmen
- Die Bankkarte nie aus dem Blick verlieren und darauf achten, dass Sie die eigene Karte zurückbekommen
- Immer in Landeswährung bezahlen, nicht in Euro umrechnen lassen (gilt auch am Geldautomaten)

Zahlen Sie lieber in bar, sollten Sie auch das in Landeswährung tun. Die fremde Währung sollten Sie dabei möglichst nur in Geldinstituten wie Banken oder offiziellen Wechselstuben tauschen.
Kleine Wechselstübchen am Straßenrand bieten zwar oft verlockend günstige Wechselkurse an, ziehen Ihnen mit horrenden Bearbeitungsgebühren aber schnell das Geld aus der Tasche.

Karte geklaut: So reagieren Sie richtig

Wenn Ihnen trotz allem die Kreditkarte geklaut wurde, sollten Sie diese sofort sperren lassen. Rufen Sie dafür am besten den zentralen Sperr-Notruf (+49 116 116) an.

Alternativ können Sie auch die SperrApp für Android und iOS nutzen. Haben Sie Ihre Bankkarte darin hinterlegt, können Sie diese direkt aus der App heraus sperren. Übrigens: Viele Banken bieten ein solches Feature auch direkt in Ihren hauseigenen Banking-Apps.
Außerdem rät das LKA, den Diebstahl umgehend zur Anzeige zu bringen – sowohl bei der lokalen Polizei als auch in Deutschland. Denn die deutsche Polizei kann Ihre Girocard für das elektronische Lastschriftverfahren sperren.
Trotzdem sollten Sie nach einem Diebstahl Ihre Kontobewegungen gut im Auge behalten. Entdecken Sie unrechtmäßige Lastschrift-Abbuchungen, sollten Sie sofort aktiv werden und die Rückbuchung der Lastschrift fordern.

- Sparkasse: Lastschrift zurückbuchen – so geht's

Quelle: https://www.chip.de/news/Landeskriminalamt-raet-So-schuetzen-Sie-Ihr-Geld-im-Urlaub-am-besten_184316482.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=30-06-2022%2B17%253A00%253A11&utm_content=nl_chipmob&utm_term=