31. Cybercrime Newsletter

27.10.2022

1) Smishing – Finanzbehörde warnt vor Betrugs-SMS

In einer SMS erhalten Handybesitzer derzeit einen Bescheid zur Steuerrückzahlung. Hinter der Nachricht stecken Betrüger, warnt eine Finanzbehörde.

Behörden warnen vor einer betrügerischen SMS im Namen des Bundesministeriums für Finanzen (BMF). In der Nachricht werde ein Erstattungsbetrag in Höhe von 254,33 Euro erwähnt, heißt es auf der Seite des Thüringer Finanzministeriums.

Um den Betrag zu erhalten, sollten sich die Empfänger unter einem in der SMS angegebenen Link verifizieren. Dem Finanzamt Jena seien bereits mehrere Fälle geschildert worden. Die Finanzverwaltung warnt davor, die per SMS geforderte Verifizierung durchzuführen.

Bei der SMS handelt es sich um sogenanntes Smishing. Der vom Wort Phishing abgewandelte Begriff bezeichnet ein Vorgehen von Betrügern, die an die Daten von Personen kommen wollen.

SMS-Massenversand an alle Kontakte

Klicken die Empfänger auf den Link in den Kurzmitteilungen, werden sie auf dubiose Webseiten geleitet, wo Apps heruntergeladen werden sollen.

Tatsächlich handelt es sich aber um Schadsoftware, die einen SMS-Massenversand an alle im Handy gespeicherten Kontakte und weitere Nummern auslöst.

Schadsoftware durch Betrugs-SMS mit der Smishing-Masche sind ein gravierendes Problem. Die Deutsche Telekom hatte im vergangenen Jahr etwa 30.000 Kundinnen und Kunden informiert, dass deren Geräte von Smishing-Angriffen betroffen seien.

Die Kundengeräte hätten Tausende SMS versendet und damit Schadprogramme in einem Schneeballsystem weiterverteilt. "In Summe haben deren Smartphones annähernd 100 Millionen Smishing-SMS verschickt – allein über unser Netz", sagte ein Telekom-Sprecher damals.

Quelle: https://www.t-online.de/digital/handy/id_100058182/vorsicht-vor-smishing-finanzbehoerde-warnt-vor-betrugs-sms.html

2) Hacker nutzten Powerpoint für Malware-Angriffe

Hacker lösen durch Mausbewegungen in Powerpoint-Präsentationen ein bösartiges Powershell-Skript aus.

Angeblich aus Russland stammende Hacker haben eine neue Technik zur Ausführung von Malware-Code entwickelt . Für den Angriff ist ein bösartiges Makro erforderlich, damit der Schadcode ausgeführt und die Nutzlast heruntergeladen werden kann. Das erreichen die Hacker über Mausbewegungen in Microsofts Präsentationssoftware Powerpoint.

Powerpoint-Datei mit Hyperlink

Wie das Sicherheitsunternehmen Cluster25 berichtet , sei diese Technik erstmals am 9. September 2022 zum Einsatz gekommen. Auf diese Weise hätten die Hackergruppe APT28 die Graphite-Malware verbreitet. Diese ermöglicht es Angreifern, andere Malware in den Systemspeicher zu laden. Ihren Opfern schickt die Hackergruppe eine Powerpoint-Datei, die angeblich von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) stammt. In dieser Datei werden auf zwei Folien in Englisch und Französisch die Dolmetscheroptionen in der Videokonferenz-App Zoom erklärt. In der PPT-Datei ist außerdem ein Hyperlink enthalten, über den das bösartige Powershell-Skript mit dem Dienstprogramm SyncAppvPublishingServer gestartet wird. Laut Cluster25 wurde die Kampagne von den Hackern bereits im Januar und Februar 2022 geplant. Aktiv waren die in den Angriffen verwendeten URLs dann im August und September.

Spionage-Kampagne in der EU und Osteuropa

Die Sicherheitsexperten von Cluster25 gehen davon aus, dass es sich bei den Angriffen um eine Spionage-Kampagne der russischen Regierung handelt. Als Ziel haben die Angreifer Einrichtungen im Verteidigungs- und Regierungssektor in Osteuropa und in der Europäischen Union ins Auge gefasst.

Quelle: https://www.pcwelt.de/news/Hacker-nutzten-Powerpoint-fuer-Malware-Angriffe-11301740.html?utm_source=security-automatisch&utm_medium=email&utm_campaign=newsletter&ext_id=3701061&pm_cat%5B0%5D=Productivity+Software&pm_cat%5B1%5D=Microsoft&pm_cat%5B2%5D=Virenschutz&pm_cat%5B3%5D=Cyberkriminalit%C3%A4t&pm_cat%5B4%5D=Security+allgemein&pm_cat%5B5%5D=Office+Software&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) So prüfen Sie, ob Ihre Mailadresse missbraucht wird und so schützen Sie sich

So überprüfen Sie sofort, ob Ihre Mailadresse im Internet geleakt wurde. So reagieren Sie richtig, wenn Sie betroffen sind.

Mit diesen kostenlosen Online-Tools überprüfen Sie sofort, ob Ihre Mailadresse im Internet geleakt wurde und in Zusammenhang mit gestohlenen Daten auftaucht.

haveibeenpwned von Troy Hunt

Sie können auf haveibeenpwned von dem Betreiber Troy Hunt Ihre Mailadresse daraufhin überprüfen lassen, ob diese im Internet in Zusammenhang mit geleakten Daten auftaucht. Die Seite zeigt Ihnen das Ergebnis der Überprüfung sofort an.

Das Ergebnis gibt Tipps dazu, wie Sie die Sicherheit des betroffenen Mailkontos verbessern und erklärt, in welchen Breaches Ihr Mailpasswort entdeckt wurde. Die Seite bietet zudem die Möglichkeit auch Telefonnummern daraufhin zu überprüfen, ob diese in Breaches vorkommen. Außerdem können Sie auch nach gestohlenen Passwörtern suchen lassen. Sie können sich auch automatisch benachrichtigen lassen, wenn Ihre bei haveibeenpwned hinterlegte Mailadresse in einem Breach auftaucht.

Wichtig: Selbst wenn Ihre Mailadresse in keinem Datenleak vorkommt, bedeutet das nicht, dass sie nicht bereits gehackt wurde oder nicht leicht zu hacken ist – zum Beispiel wegen eines schwachen Passwortes. Andererseits bedeutet es nicht zwangsläufig, dass Ihre Mailadresse bereits konkret missbraucht wird, wenn diese in einem Breach enthalten ist.

Betreiber Troy Hunt ist ein leitender Angestellter von Microsoft in Australien. Er betreibt auch einen Twitterkanal zu Datenleaks im Web.

Tipp: So vermeiden Sie Mail-Stalking und schützen Ihre Privatsphäre

Es ist zwar theoretisch richtig, dass haveibeenpwned unter Umständen dazu missbraucht werden kann, um herauszufinden, bei welchen Clouddiensten sich andere Personen mit ihrer Mailadresse registriert haben. Allerdings handeln Anwender, die sich bei potenziell verfänglichen Online-Diensten wie beispielsweise Porno-Portalen oder Online-Sexkontakte-Plattformen mit ihrer beruflichen oder hauptsächlich genutzten und allgemein bekannten Mailadresse anmelden, extrem leichtsinnig. Für solche Zwecke sollte man sich eine zusätzliche, gut getarnte Mailadresse zulegen, aus deren Bezeichnung nicht auf die eigene Identität geschlossen werden kann. Beispielweise mit Outlook.com: Gratis-Mail-Konto mit Outlook.com einrichten – so geht's .

Und schon können Sie Ihre Bekannten, Freude oder Kollegen nicht mehr über haveibeenpwned stalken.

Übrigens: Firefox Monitor nutzt ebenfalls haveibeenpwned.

HPI Identity Leak Checker des Hasso-Plattner-Instituts für Digital Engineering gGmbH

Der HPI Identity Leak Checker ist ein weiteres kostenloses Online-Tool, mit dem Sie Ihre Mailadresse daraufhin überprüfen lassen können, ob diese in Breaches auftauchen. Hier wird das Ergebnis der Überprüfung aber nicht direkt auf der Webseite von HPI Identity Leak Checker angezeigt, sondern stattdessen schickt der HPI Identity Leak Checker eine Mail mit dem Überprüfungsergebnis an die überprüfte Mailadresse.

Somit ist über den HPI Identity Leak Checker kein Stalking wie bei haveibeenpwned möglich.

Betreiber ist hier das Hasso-Plattner-Institut (HPI) der Universität Potsdam. In der FAQ erfahren Sie Details zur Funktionsweise. Wichtig: "Der Identity Leak Checker gibt lediglich Auskunft dazu, ob Ihr Kennwort in einem Leak gefunden wurde. Der Leak Checker sagt nichts darüber aus, ob dieses Kennwort für das betroffene Benutzerkonto noch funktioniert. Da Ihr Kennwort weiterhin in dem entsprechenden Leak zu finden ist, gibt die Webseite weiterhin eine Warnung aus."

Identity Leak Checker der Universität Bonn

Die Universität Bonn bietet ebenfalls einen Leak-Checker an. Er funktioniert genauso wie der des HPI: Sie geben die zu überprüfende Mailadresse ein und die Auswertung erhalten Sie dann an die eingegebene Mailadresse. Das verhindert also ebenfalls Stalking- beziehungsweise Ausspähversuche, wie es theoretisch bei haveibeenpwned möglich ist.

Der Bonner Leak-Checker entstand aus dem mit Bundesmitteln geförderten Projekt EIDI .

So reagieren Sie richtig

Falls Ihnen die oben genannten Tools anzeigen, dass Ihre Mailadresse in Datenleaks/Breaches auftaucht, dann sollten Sie sofort das Passwort dazu ändern. Haben Sie das gleiche Passwort, das Sie für Ihr Mailkonto verwenden, auch bei anderen Diensten verwendet, so sollten Sie dieses Passwort auch dort ändern.

Experten: So finden Sie ein wirklich sicheres Passwort

Ganz wichtig: Installieren Sie die Zweifaktor-Authentifizierung, sofern diese für Ihr Mailkonto unterstützt wird.

Gegebenenfalls nutzen Sie einen Passwortmanager wie Lastpass, um ein möglichst sicheres Passwort erstellen und speichern zu lassen.

Die besten Passwort-Manager im Test 2022

Woher stammen die gestohlenen Mailadressen?

Die meisten geklauten Mailadressen stammen aus Angriffen auf Unternehmensserver, auf denen Dienste laufen, bei denen Sie sich mit Ihrer Mailadresse registriert haben. Beispielsweise stahlen Cybergangster die Daten von mehreren Hunderttausend Kunden des hessischen Energieversorgers Entega, wie im Juli 2022 bekannt wurde. Diese Datenschätze werden von den Dieben dann in Internetforen beziehungsweise im Darknet zum Kauf angeboten. Weitere große Datendiebstähle auf Unternehmensebene waren zum Beispiel:

Facebook-Daten gestohlen: Hier sehen Sie, ob Sie betroffen sind

Mega-Leak: 773 Millionen Mail-Adressen im Netz

500 Mio. LinkedIn-Nutzerdaten im Netz - das sagt LinkedIn dazu

Sammelklage: Ashley Madison entschädigt Hack-Opfer

Hacker erpressen Sony Pictures mit geraubten Dateien

Ein schon länger zurückliegender, aber damals sehr spektakulärer Datendiebstahl: Im Jahr 2011 stahlen Cybergangster die Daten von rund 160 Millionen Sony-Kunden.

Gegen solche Datenleaks, die durch das Stehlen von Serverdaten verursacht werden, sind Sie machtlos, diese können Sie nicht verhindern.

Anmerkung der Redaktion: Illustrationen zu diesem Thema können unter dem u.g. Link abgerufen werden.

Quelle: https://www.pcwelt.de/ratgeber/So-pruefen-Sie-ob-Ihre-Mailadresse-missbraucht-wird-und-so-schuetzen-Sie-sich-11279352.html?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3700491&pm_cat%5B0%5D=Productivity+Software&pm_cat%5B1%5D=Kreativ+Software&pm_cat%5B2%5D=Web+allgemein&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Internetbetrug – Polizei warnt vor "Scamming" - das sollten Sie beachten

Reine Online-Bekanntschaften sind so eine Sache. Wird dann um finanzielle Unterstützung gebeten, sollte man vorsichtig sein, warnt die Polizei. Es könnte sich um Scamming handeln.

Das schnelle Geld, der Superjob, die Traumwohnung, ein Riesenerbe und natürlich die große Liebe: Betrügerinnen und Betrüger (Scammer) sind im Netz auf allen Kanälen mit vollmundigen Versprechen unterwegs.

Skeptisch sollte man immer dann werden, sobald es um Geld geht. Etwa, wenn Vorauszahlungen geleistet werden sollen, um das Versprochene zu erhalten, warnt die Polizeiliche Kriminalprävention der Länder und des Bundes.

Oberste Regel: Kein Geld an Unbekannte schicken

Betrüger versuchen immer wieder, Menschen in Notsituationen auszunutzen oder so viel emotionalen Druck auszuüben, dass die Opfer ihnen nachgeben. Geht es darum, Geld an andere zu überweisen oder sonstige private Daten oder Bankdaten weiterzugeben, sollte man immer skeptisch sein und lieber vorsichtig denn vorschnell handeln.

Grundsätzlich gilt: Man sollte Menschen, die man nie persönlich getroffen und kennengelernt hat, niemals Geld überweisen oder auf sonstige Forderungen eingehen.

Besonders perfide ist der sogenannte Love oder Romance Scam. Dabei tummeln sich die Betrügerinnen oder Betrüger oft in sozialen Netzwerken, bei Partnerbörsen oder Dating-Apps.

Dort täuschen sie die große Liebe vor und bringen ihre Opfer in emotionale Abhängigkeit. Erst in der vergangenen Woche berichteten wir über einen Love Scam, bei der eine Japanerin auf einen angeblichen Astronauten hereingefallen ist.

Die Polizei warnt: Scamming ist sehr weit verbreitet

Da Scamming weit verbreitet ist, hat die Polizei eine eigens auf Internetbetrug durch Scamming ausgerichtete Internetseite, auf der sie vor unterschiedlichen Betrugsvarianten warnt.

Vor folgenden Angeboten sollten Sie besonders aufpassen:

- **Vorgetäuschte Liebe:** Vor allem in Online-Partnerbörsen oder sozialen Netzwerken. Zumeist wird hier auch zu eine Zahlung aufgefordert, beispielsweise um sich Zugtickets für ein reales Treffen zu leisten.
- **Falsche Identität:** Menschen im Auslandseinsatz, die angeblich nicht an ihr privates Geld gelangen können und deswegen schnell eine Überweisung benötigen.
- **Geldversprechen:** "Nigeria Connection" – Geld aus einer Erbschaft oder einer angeblich super Investitionsmöglichkeit, nachdem man erst einen Vorschuss leisten musste.
- **Wohnungsangebote:** Vor allem in Metropolregionen, in denen der Wohnungsmarkt hart umkämpft ist – großartige Lage, super Ausstattung, spottbillige Miete – aber der Vermieter wohnt in Übersee. Kaution und erste Miete müssen auch im Voraus überwiesen werden.
- **Traumjob:** Stellenanzeigen, die einen Traumjob mit sehr guter Bezahlung anpreisen – man müsse aber noch eine Gebühr entrichten, beispielsweise für Arbeitskleidung.
- **Gefälschte Schecks:** Auf Bezahlung mit Schecks sollte aus Sicherheitsgründen generell verzichtet werden.

Auf der Scamming-Themenseite der Polizei finden sich für einige der Anwendungsfälle auch ausführliche Handlungsempfehlungen. Sollten Sie Opfer eines Scams oder Betrugsversuchs im Internet geworden sein, suchen Sie eine Polizeidienststelle in Ihrer Nähe auf.

Quelle: https://www.t-online.de/digital/internet-sicherheit/internet/id_100068800/polizei-warnt-vor-scamming-im-internet-das-sollten-sie-beachten.html

5) DHL-Kunden in Gefahr: Besonders perfide Betrugsmasche im Umlauf

DHL-Kunden werden aktuell vor einer besonders fiesen Betrugsmasche gewarnt. Cyberkriminell wollen dabei mit Hilfe von Phishing-Mails Ihre Daten abgreifen.

Cyber-Kriminelle versenden derzeit wieder einmal Phishing-Mails an DHL-Kunden. Wie die Verbraucherzentrale berichtet, behaupten die Betrüger darin, dass Zollgebühren in Höhe von 1,89 Euro nicht bezahlt worden seien.

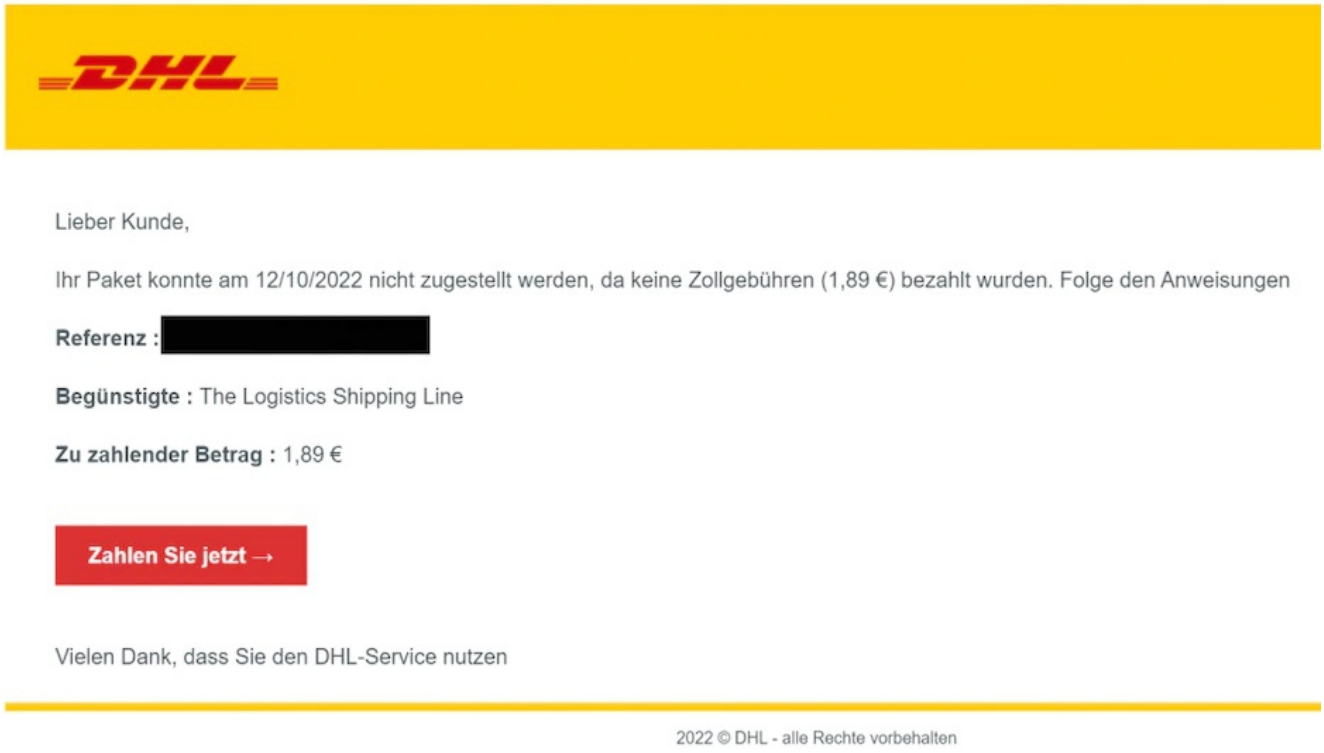
Ein Paket könne wegen der offenen Rechnung nicht zugestellt werden. Über den beigefügten Link könne man diese begleichen.

Gefahr für DHL-Kunden: So schützen Sie sich vor der Betrugsmasche

Tatsächlich wollen die Betrüger darüber aber nur die Daten der Betroffenen abgreifen. Eine offene Zoll-Gebühr existiert nicht. Mit den Information wollen die Angreifer wahrscheinlich weiteren Schaden anrichten.

Falls Sie eine solche Mail erhalten, sollten Sie daher niemals auf den Link klicken oder sogar

Daten angeben. Verschieben Sie die Nachricht daher unbeantwortet in den Spamordner.



Vor dieser Mail sollten sich DHL-Kunden in Acht nehmen. Quelle: Verbraucherzentrale

Quelle: https://www.chip.de/news/Neue-Betrugsmasche-DHL-Kunden-muessen-vorsichtig-sein_184476172.html

6) Vorsicht vor Whatsapp-Gewinnspiel: So läuft der Betrug

Whatsapp schickt Ihnen eine Mail. Sie haben bei einem Gewinnspiel unter allen bei Whatsapp registrierten Telefonnummern gewonnen. Ein gefährlicher Betrugsversuch.

Eine Mail macht derzeit die Runden, die vorgibt, von Whatsapp zu stammen. In der Mail steht zu lesen, dass man 960.000 US-Dollar gewonnen habe. Doch die Mail ist ein Betrugsversuch, wie das Sicherheitsportal Watchlist Internet warnt.

Angeblich sei die Telefonnummer des Empfängers der Mail bei einem Gewinnspiel namens “Whatsapp Global Awards-Programm” aus dem weltweiten Whatsapp-Handynummernverzeichnis ausgewählt worden. Damit die Bank den Gewinn auszahlen könne, solle man seine Kontaktdaten an Whatsapp schicken.

Konkret benötige Whatsapp folgende Daten: Name, Telefonnummer, Staatsangehörigkeit, Alter, Geschlecht, Familienstand, Beruf und Adresse. Diese Informationen soll der angebliche Gewinner an die Mailadresse “account.whatsapp@mail.com” schicken.

Zudem fordert Whatsapp den Gewinner auf, seinen Gewinn vorerst geheim zu halten. Damit wollen die Cybergangster vermutlich erreichen, dass der Empfänger nicht von Bekannten davor gewarnt wird, dass es sich bei dem angeblichen Gewinn um einen Betrug handeln würde.

Wer tatsächlich an die genannten Mailadresse schreibt, dem schicken die Betrüger eine erneute Mail, die über den weiteren Verlauf informiert. Vermutlich schicken die Cybergangster sogar eine Gewinnurkunde und Bankdokumente, die beweisen sollen, dass die Gewinnspielsumme bereits überwiesen wird. Vielleicht kommt es sogar zu einer Kommunikation mit der vermeintlichen Bank. Alle Mails vonseiten der Betrüger sind höflich

formuliert. Sollte der Empfänger aber zögerlich reagieren, dann kann es vorkommen, dass die Betrüger sich per Whatsapp oder sogar telefonisch melden, um Druck auszuüben.

Doch der Betrug ist mit dem Abgreifen Ihrer Daten noch nicht zu Ende. Denn nun fordern die Betrüger, dass die Opfer einen Geldbetrag überweisen. Damit sollen angeblich Anwaltskosten, Versicherungsgebühren, Steuern etc. abgedeckt werden. Erst wenn man diese Kosten bezahlt habe, könne der Gewinn ausbezahlt werden. Danach würden die von Ihnen bezahlten Gebühren wieder erstattet.

So reagieren Sie richtig

Antworten Sie nicht auf diese Mail. Sie würden durch eine Antwort nur Ihre Mailadresse gegenüber den Betrügern verifizieren und sich weiteren Angriffsversuchen aussetzen. Stattdessen löschen Sie die betrügerische Mail sofort.

Falls Sie bereits überwiesen haben

- Erstatten Sie sofort Anzeige bei der Polizei.
- Informieren Sie unverzüglich Ihre Bank, damit diese die Überweisung stoppt und versucht, das Geld zurückzuholen.
- Brechen Sie den Kontakt zu den Betrügern ab und blockieren Sie diese.
- Seien Sie vorsichtig vor weiteren Betrugsversuchen. Denn die Betrüger haben nun Ihre Daten.

Quelle: https://www.pcwelt.de/article/1361892/vorsicht-vor-whatsapp-gewinnspiel-so-lauft-der-betrug.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Vorsicht%20vor%20Whatsapp-Gewinnspiel%3A%20So%20l%C3%A4uft%20der%20Betrug&utm_campaign=Best-of%20PC-WELT&utm_term=PC-WELT%20Newsletters&utm_date=20221026113320&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Deutsche Bundesbank: So läuft eine neue Betrugsmasche

Cybergangster haben sich einen neuen Trick ausgedacht, um an Ihre Daten zu kommen. So läuft die neue Masche.

Die Verbraucherzentrale Schleswig-Holstein warnt vor einer völlig neuen Betrugsmasche: Gangster missbrauchen hierfür den renommierten Namen der Deutschen Bundesbank. Die Verbraucherschützer betonen, dass sie so eine Mail bisher nicht gesehen hätten.

Die Phishing-Mail gibt vor, von der Deutschen Bundesbank zu stammen. Die Mail fordert die Empfänger dazu auf, ihre Personalien und Kreditkarten-Informationen zu bestätigen. Da die Kredit- beziehungsweise Debitkarte nicht mehr der PSD2-Richtlinie der Europäischen Union entsprechen würde, so die Behauptung. Diese Bestätigung der Karten-Informationen müssten angeblich alle durchlaufen, die in den letzten 24 Monaten die Kreditkarte für eine Online-Transaktion verwendet haben.

Führe man die Bestätigung durch, könne man die Karte “ohne jegliche Unterbrechungen verwenden”, so das Versprechen. Führe man die Bestätigung allerdings nicht bis zum 31. Oktober 2022 aus, so müsse die Deutsche Bundesbank Sanktionen aussprechen und das Konto könne für 180 Tage gesperrt werden.

In der Mail befinden sich ein großer Button mit der Aufschrift “Personalien bestätigen”. Dieser führt zu einer Phishing-Seite, auf der Ihre Daten gestohlen werden.

Die Anrede in der Mail ist unpersönlich gehalten (“Guten Tag”), es handelt sich also um eine Phishing-Mail, die zufällig an bekannte Mailadressen verschickt wird, ohne dass ein konkreter Bezug zum Adressaten vorhanden ist. Einige Formulierungen im Text sowie die Schlussformel

legen die Vermutung nahe, dass die Mails aus dem Ausland verschickt und der Text dazu ins Deutsche übersetzt wurde.

So schützen Sie sich

Die Deutsche Bundesbank hat nichts mit ihrer Kredit- oder Debitkarte zu tun. Ansprechpartner dafür sind die ausstellenden Kreditinstitute. Löschen Sie diese Mail sofort.

Quelle: https://www.pcwelt.de/article/1355813/deutsche-bundesbank-so-lauft-eine-neue-betrugsmasche.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Deutsche%20Bundesbank%3A%20So%20l%C3%A4uft%20eine%20neue%20Betrugsmasche&utm_campaign=Security&utm_term=PC-WELT%20Newsletters&utm_date=20221026120523&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

8) Brennholz online kaufen – Verbraucherschützer warnen vor Fake-Shops

Kriminelle machen sich die gestiegenen Energiepreise zunutze, mahnen Verbraucherschützer. Bei Online-Shops für Brennholz und Pellets sei Vorsicht geboten.

Abzocke und Fake-Shops: Die Verbraucherzentrale Niedersachsen warnt vor dubiosen Angeboten von Brennmaterialien im Internet. Online seien nicht nur vermehrt Angebote zu horrenden Preisen, sondern auch zunehmend Fake-Shops zu finden, heißt es.

Dass mit den Energiepreisen auch die Nachfrage nach Kaminholz und Pellets spürbar gestiegen sei, machten sich Cyber-Kriminelle zunutze. "Schon in der Coronakrise haben wir gesehen, dass unseriöse Anbieter die Situation für sich ausnutzen", sagt Kathrin Körber von der Verbraucherzentrale Niedersachsen.

Damals habe es plötzlich vermehrt Fake-Shops zu Gartenartikeln, Strandkörben und Fahrrädern gegeben. Auch wurden etwa Desinfektionsmittel oder Atemschutzmasken zu überhöhten Preisen angeboten. "Jetzt erleben wir das gleiche Phänomen bei Kamin- und Brennholz sowie Holzpellets", so Körber.

Namen des Shops in der Google-Suche eingeben

"Wir können daher nur zur Vorsicht raten: Auch wenn das Angebot noch so verlockend ist, sollten Verbraucherinnen und Verbraucher genau hinschauen und den Shop vor der Bestellung überprüfen." Meist helfe es schon, den Namen des Shops zu googeln und nach Bewertungen zu suchen.

Beispiele für Fake-Shops seien aktuell etwa "buhler-energie.com" und "bitterlich-brennholz.com". Laut Körber sind die beiden Shops auf den ersten Blick seriös. "Bei genauerer Prüfung fällt jedoch auf, dass die Seiten nicht in Deutschland gehostet werden, erst seit kurzer Zeit online sind und zudem bereits mehrfach als Fake-Shops gelistet wurden." Außerdem sei jeweils bei der im Impressum angegebene Adresse eine andere Firma zu finden.

Quelle: https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100061808/betrug-mit-brennholz-verbraucherschuetzer-warnen-vor-fake-shops.html

9) "Sextortion" – Polizei warnt vor Erpressung mit Nacktbildern

Mit einer speziellen Masche versuchen Kriminelle, an das Geld junger Männer zu kommen. Dabei spielen sie mit ihren Gefühlen und setzen sie emotionaler Erpressung aus.

Immer wieder versuchen Betrüger, junge Männer in Thüringen mit der angedrohten Veröffentlichung von Nacktfotos oder -videos zu erpressen. Zuletzt meldete sich im Oktober etwa ein 19-Jähriger aus Sondershausen bei der Polizei und zeigte eine Erpressung an.

Er erhielt über Instagram die Nachricht, dass ein Video von ihm existiere, auf dem er nackt zu sehen sei. Wolle er nicht, dass dieses geteilt und veröffentlicht werde, sollte er laut Polizei 9.000 Euro zahlen. Auch junge Männer in Bad Salzungen und Hildburghausen sollten im Oktober und September hohe Summen zahlen.

Andernfalls würden heimlich aufgezeichnete Videos veröffentlicht werden. Die Polizei nennt das "Sextortion". Das Kofferwort besteht aus den Begriffen "Sex" und "extortion", was im Englischen für Erpressung steht.

Von nettem Chat zu knallharten Forderungen

In den meisten Fällen, wie auch in Bad Salzungen, lernen die Männer bei Dating- oder anderen Plattformen junge Frauen kennen, die den Kontakt mit ihnen schnell intensivieren. Bald schon bitten die Frauen darum, sensible Fotos zu bekommen oder vor der Webcam sexuelle Handlungen zu teilen.

Dabei zeichnen sie diese sexuellen Handlungen auf. "Sobald dies geschehen ist, wandelt sich der Gesprächsverlauf schnell von sanftem Wortlaut in knallharte Forderungen", heißt es in einer Mitteilung der Polizei.

Scham spielt entscheidende Rolle

Es ist kein neues Phänomen: In Thüringen wurden im Zeitraum April bis August 2018 bereits 139 Fälle von "Sextortion" zur Anzeige gebracht. Die Polizei warnt eindringlich davor, Geldforderungen nachzugehen. "Die Erpressung hört in den meisten Fällen nach der Zahlung nicht auf", informiert die Thüringer Polizei. Betroffene Männer sollten den Chatverlauf mittels Screenshot sichern und sich bei der Polizei melden.

Der sogenannte Enkeltrickbetrug und die Betrugsmasche mit falschen Chats via Whatsapp kommen nach Angaben einer Polizeisprecherin in Thüringen deutlich häufiger vor. Trotzdem seien hier ähnliche Dynamiken im Spiel. Bei vielen Senioren wie auch vielen jungen Männern spiele die Scham eine wichtige Rolle bei der Entscheidung, zur Polizei zu gehen. Viele trauten sich einfach nicht, Anzeige zu erstatten. Die Dunkelziffer sei also unklar.

Quelle: https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100071732/sextortion-polizei-warnt-vor-erpressung-mit-nacktbildern.html

10) News – Die aktuell 10 gefährlichsten Spam-Rufnummern

Von diesen Rufnummern gingen im September 2022 die meisten Spam-Anrufe an. Und so wehren Sie sich dagegen!

Täglich werden unzählige Verbraucher von Telefonbetrügern mit Spamanrufen belästigt. Clever Dialer, ein Anbieter von Spamschutz-Lösungen für Telefone, hat am Montag die Top 10 der Rufnummern veröffentlicht, von denen im September 2022 die meisten Telefonspam-Anrufe ausgingen.

Berliner Rufnummer auf Platz 1 der Telefonspammer

Auf dem ersten Platz landet im September erneut die Berliner Telefonnummer **03016637169**, bei der die Anrufer mit einer Gewinnspiele-Masche versuchen, die Angerufenen hereinzulegen. 19,08 Prozent aller bei Clever Dialer registrierten Telefonspam-Anrufe gingen auf das Konto dieser Rufnummer.

Auf dem zweiten Platz landet mit 16,09 Prozent die Mobilfunknummer **015215173526**, hier werden die Angerufenen mit angeblichen Reisegutscheinen und Lottogewinnen dazu aufgefordert, ihre privaten Daten preiszugeben, um sie dann damit in eine Kostenfalle zu locken. So berichtet ein Betroffener beispielsweise:

> *„Angeblich hätte meine Tochter Lotto gespielt. Sechs Monate lang würden jetzt 1200 € von ihrem Konto abgebucht werden.“*

Registriert wird, dass die Telefonspammer immer aggressiver vorgehen. So berichten Betroffene darüber, dass sie von den Spammern beleidigt oder sogar angeschrien werden. Wie etwa bei Anrufen von der Rufnummer **04029996106**, bei der ebenfalls eine Kostenfalle lauert.

Die komplette Top 10 der Spam-Telefonnummern im September 2022

Platz	Vorwahl	Nummer	Typ
1	+49	03016637169	Andere
2	+49	015215173526	Kostenfalle
3	+49	069244375048	Andere
4	+44	+442920028363	Kostenfalle
5	+49	015210126963	Gewinnspiel
6	+49	06966102716	Andere
7	+49	04029996106	Kostenfalle
8	+49	01782482471	Gewinnspiel
9	+49	04042237949	Andere
10	+49	045033568906	Andere

So wehren Sie sich gegen Telefonspam

Wie Sie sich gegen Telefonbetrug wehren können, erläutern wir in diesem Beitrag: So wehren Sie sich gegen Telefon-Spam. Wie Sie auf der Fritzbox mit Tellows einen Anrufschutz einrichten können, erfahren Sie in diesem Artikel:
Tellows Anrufschutz für Fritz Box: Test, Howto & neue Funktionen

Quelle: https://www.pcwelt.de/article/1346885/die-aktuell-10-gefahrlichsten-spam-rufnummern.html

Anwenderinformationen:

1) Update 2.27 – Corona-Warn-App: Neue Version zeigt Maskenpflicht an

Die neue Version der Corona-Warn-App zeigt an, ob an dem jeweiligen Ort des Nutzers eine Maskenpflicht besteht. Es gibt weitere neue Funktionen.

Maskenpflicht ja oder nein: Diese Information lässt sich künftig über die Corona-Warn-App anzeigen, wie die Entwickler der Anwendung mitteilen. "Ab Version 2.27 zeigt Ihnen die Corona-Warn-App im Bereich 'Zertifikate' den aktuellen Maskenstatus als entsprechendes Symbol, falls politische Regelungen es erfordern", heißt es.

Mit dem Symbol können Nutzer sich von der App anzeigen lassen, ob sie in dem Bundesland, in dem sie sich befinden, an bestimmten Orten von der Maskenpflicht befreit sind. Die entsprechende Anzeige der Maskenpflicht erscheint allerdings erst in der App, wenn mindestens ein Bundesland erweiterte Regeln zur Maskenpflicht beschließt, heißt es.

Das Symbol haben die Entwickler über den QR-Code des Zertifikats eingefügt. Besteht an dem jeweiligen Ort eine Maskenpflicht, zeigt die Anwendung ein Maskensymbol. Daneben steht das Wort "Maskenpflicht". Andernfalls ist das Maskensymbol durchgestrichen. "Keine Maskenpflicht", heißt es dann daneben.

Anzeige des Status-Nachweises wurde entfernt

Zudem ist mit der neuen Version der Corona-Warn-App die Anzeige des Status-Nachweises wie 3G, 3G+, 2G und 2G+ auf den digitalen Covid-Zertifikaten entfernt worden, teilen die Entwickler mit. Der Grund: Derzeit gebe es "keine Maßnahmen und Vorgaben, die an den G-Status gekoppelt sind".

Eine Textbox in der App soll die Nutzer entsprechend informieren: "Der Status-Nachweis ist zurzeit nicht relevant und wird daher nicht von der App ausgewiesen", heißt es künftig in der Anwendung.

Mit dem Update 2.27 passen die Entwickler ihre App an das neue Covid-19-Schutzgesetz an, das ab dem 1. Oktober 2022 gelten soll und durch das bis zu 12 Millionen Deutsche ihren Corona-Impfstatus verlieren.

Quelle: https://www.t-online.de/digital/handy/id_100059276/corona-warn-app-neue-version-zeigt-maskenpflicht-an.html

2) Diese Gebühren werden bei der Paypal-Nutzung fällig

Wir erklären, ob und welche Gebühren bei der Nutzung von Paypal genau anfallen. Und wie Sie sparen können.

Das einfach und schnelle Online-Bezahlsystem Paypal erfreut sich auch in Deutschland großer Beliebtheit. Während die meisten Transaktionen für Sie, als Privatanwender, kostenlos sind, werden für bestimmte Aktivitäten Gebühren fällig.

Keine Paypal-Gebühren beim Kauf – weder online noch im Shop

Eine häufige Frage, die uns erreicht: Fallen eigentlich Gebühren bei der Nutzung von Paypal an

oder ist Paypal kostenlos? Die Frage lässt sich ganz einfach beantworten: Nicht nur das Anlegen und die Nutzung eines Paypal-Kontos ist für Verbraucher kostenlos. Auch wenn Sie Waren oder Dienste beim Online-Shopping per Paypal bezahlen, dann fallen für Sie als Verbraucher keinerlei Gebühren an. Es gibt allerdings Händler und Verkäufer, die ihre Kosten für Paypal (siehe weiter unten) an die Kunden weitergeben.

Gebühr für Echtzeit-Abbuchung von Paypal-Guthaben

Wer Geld-Guthaben bei Paypal hat, der kann es sich in Echtzeit auf sein Konto zurück überweisen. Bei einer solchen Sofort-Überweisung fällt allerdings eine Gebühr in Höhe von 1 % des Betrags an, mindestens allerdings 0,25 Euro und maximal 10 Euro. Der Vorteil: Sie haben Ihr Geld von Ihrem Paypal-Konto binnen weniger Minuten auf Ihrem Bankkonto.

Gebührenfrei ist die Standard-Abbuchung. Hier dauert es dann aber auch zwei bis drei Werktage, bis Sie den von ihrem Paypal-Guthaben gesendeten Betrag auf Ihr Bankkonto erhalten. Hinweis: Standardmäßig ist die Sofort-Abbuchung aktiviert, um Kosten zu vermeiden, müssen Sie bei der Abbuchung aktiv auf "Standard" umstellen.

Geld-Versand an Paypal-Freunde in der EU kostenlos

Beim Versenden von Geld an Familienangehörige, Freunde oder Bekannte fallen **keine Extrakosten** an, wenn das Geld innerhalb der EU versendet wird **und** keine Währungsumrechnung stattfindet. Solche "persönlichen Zahlungen" sind also kostenlos, unabhängig von der verwendeten Zahlungsquelle (bestehendes Guthaben, Bankkonto, Kreditkarte, etc.).

Für alle anderen persönlichen Zahlungen berechnet Paypal eine Gebühr in Höhe von 5 Prozent der Transaktionssumme, wobei mindestens Kosten in Höhe von 0,99 Euro und maximal 3,99 Euro pro Transaktion berechnet werden. Die Gebühr zahlt dabei grundsätzlich der Absender. Paypal informiert Sie aber vor der Zahlung über die anfallenden Gebühren.

Generell gilt also: Der Empfänger des Geldes bezahlt bei "persönlichen Zahlungen" in keinem Fall irgendwelche Gebühren.

Im Paypal-Währungsrechner können Sie den aktuell von Paypal für Transaktionen genutzten Wechselkurs überprüfen.

Gibt es Paypal-Gebühren bei Google-Pay-Zahlungen übers Handy?

Paypal können Sie in Verbindung mit Google Pay (jetzt Google Wallet) nutzen. Dazu müssen Sie das Paypal-Konto mit Google Pay (wallet) verknüpfen. Anschließend können Sie überall unterwegs mit dem Smartphone zahlen, wo kontaktlose NFC-Zahlungen mit Mastercard akzeptiert werden. Gebühren fallen keine für den Käufer an. Auch nicht im Ausland!

Als Zahlungsquelle wird jedes für das Paypal-Konto bestätigtes Bankkonto unterstützt. Zunächst wird aber das Paypal-Guthaben für Google-Wallet-Zahlungen via Paypal aufgebraucht, ehe das Bankkonto belastet wird. In Paypal hinterlegte Kreditkarten werden für Google-Wallet-Zahlungen derzeit noch nicht unterstützt.

Paypal Käuferschutz: Berechnet Paypal hier Gebühren?

Auch bei Paypal-Zahlungen mit Käuferschutz muss der Käufer keinerlei Gebühren bezahlen. Für Händler gelten klare Regeln, für welche Produkte eine Paypal-Zahlung mit Käuferschutz erlaubt ist. Paypal untersagt es den Händlern in den Nutzungsbedingungen ausdrücklich, die anfallenden Käuferschutz-Gebühren an die Kunden weiterzugeben. Entsprechend sollten die Kunden auch darauf achten und Händler melden, die gegen diese Regel verstoßen.

Gebührenrechner: Diese Gebühren müssen Verkäufer bei Paypal zahlen

Gebühren muss grundsätzlich jeder Verkäufer zahlen, der seinen Kunden Paypal als Bezahloption für die von ihm angebotenen Waren und Dienstleistung anbieten möchte. Wie hoch diese Gebühren sind, hängt von unterschiedlichen Faktoren ab. Der Paypal-Gebührenrechner ist ein praktisches Online-Tool, um die Gebühren schnell zu berechnen. Hier können Händler unter "Restbetrag" auch den Betrag eingeben, den sie nach Abzug aller Paypal-Gebühren erhalten wollen.

Die Gebühr beim Zahlungsempfang liegt zunächst bei 2,49 Prozent der empfangenen Summe plus 0,35 Euro für Waren und Dienstleistungen. Seit dem 1. August 2022 zahlen Händler eine Gebühr von 2,99 Prozent plus 0,39 Euro pro Transaktion, wenn Sie Online-Zahlungen akzeptieren. Wer noch bis zum 31. Dezember 2022 zu Paypal Checkout wechselt, der reduziert seine Gebühren, wie sie vor der Anpassungen waren: eben 2,49 Prozent und 0,35 Euro Festgebühr.

Innerhalb der EWG (also der Europäischen Wirtschaftsgemeinschaft; Anm. d. Red.: Diese veraltete Bezeichnung verwendet Paypal tatsächlich) gibt es keine Zusatzgebühr. Seit **November 2021** gibt es eine Änderung auch aufgrund des Brexits, die Paypal hier dokumentiert hat . Händler in Großbritannien müssen eine zusätzliche Gebühr in Höhe von 1,29 Prozent zahlen und Händler in den USA und Kanada eine Gebühr in Höhe von 1,99 Prozent. Händler in anderen Märkten zahlen eine Gebühr in Höhe von 2,99 Prozent für Waren und Dienstleistungen, für internationale geschäftliche Transaktionen 1,99 Prozent.

Die Verkäufer haben aber auch die Möglichkeit, sich als Händler bei Paypal anzumelden und individuelle Gebühren zu erhalten, die sich von den allgemeinen Konditionen unterscheiden. Hierbei hängen die Gebühren vom jeweiligen Transaktionsvolumen des vorherigen Monats ab. Solche individuellen Konditionen sind häufig wie folgt gestaffelt:

Monatliches Transaktionsvolumen	Variable Gebühr	Gebühr pro Transaktion
< 2.000 Euro	2,49 Prozent	0,35 Euro
2.000,01 bis 5.000 Euro	2,19 Prozent	0,35 Euro
5.000,01 bis 25.000 Euro	1,99 Prozent	0,35 Euro
25.000,01 bis 100.000 Euro	1,79 Prozent	0,35 Euro
> 100.000 Euro	1,49 Prozent	0,35 Euro

Bei einem monatlichen Transaktionsvolumen von 5.000 bis 25.000 Euro über das Paypal-Konto fallen dann beispielsweise eine variable Gebühr in Höhe von 1,99 Prozent plus 0,35 Euro pro Transaktion an. Bei einem monatlichen Transaktionsvolumen von über 25.000 Euro reduziert sich die variable Gebühr auf 1,79 Prozent plus den 0,35 Euro pro Transaktion. Weitere Infos finden Sie auf dieser Paypal-Seite unter "Händler-Gebühren".

Für Mikrozahlungen berechnet Paypal seit dem 1. August 2022 eine Gebühr in Höhe von 4,99 Prozent + 0,09 Euro pro Transaktion. Ebenfalls neu: Dynamische Mikrozahlungsgebühren, wodurch bei Transaktionen entweder 4,99 Prozent + 0,09 Euro pro Transaktion oder 2,99 Prozent + 0,39 Euro abgerechnet werden, je nachdem, was für die Transaktion günstiger ist.

Voraussetzung ist, dass Sie als Händler diese dynamischen Gebühren beantragen.

Bei Spenden liegt die Gebühr bei 2,49 Prozent plus 0,35 Euro.

Bei Händlern, die Paypal Plus verwenden, gelten derzeit die folgenden Konditionen:

- 2,49 Prozent + 0,35 Euro: bei weniger als 5.000 Euro Transaktionsvolumen
- 2,09 Prozent + 0,35 Euro: bei einem Transaktionsvolumen zwischen 5.001 und 25.000 Euro
- 1,79 Prozent + 0,35 Euro: bei einem Transaktionsvolumen von über 25.000 Euro

Lesetipp: Kann ich bei Amazon mit PayPal bezahlen? Die Antwort

Quelle: https://www.pcwelt.de/a/diese-gebuehren-werden-bei-der-paypal-nutzung-faellig,3387410?utm_source=best-of-pc-welt-manuell&utm_medium=email&utm_campaign=newsletter&ext_id=3387410&pm_cat%5B0%5D=eCommerce&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Tipps zur Sicherheit – Malware auf dem Smartphone - was tun?

Unerwünschte Werbung, Trojaner und Viren: Malware macht sich längst auch auf dem Smartphone breit. So werden Sie die Schadprogramme wieder los.

Nicht nur am PC, auch auf Android-Smartphones machen sich Schadprogramme (so genannte Malware) breit. Sie zeigt unerwünschte Werbung an, errechnet virtuelle Münzen in Währungen wie Monero oder überträgt vertrauliche Daten an Kriminelle.

Wird Ihr Handy ständig heiß (auch wenn Sie es gar nicht benutzen), leert sich der Akku rasch oder steigt der Datenverbrauch rapide an, dann ist Ihr Gerät mit hoher Wahrscheinlichkeit infiziert. Grundsätzlich gilt die Empfehlung, dass Sie ein von Malware infiziertes Gerät auf die Werkseinstellungen zurücksetzen und ganz neu einrichten sollten.

Muss ich meine Passwörter ändern?

Im Rahmen der auf den so genannten „Factory Reset“ folgenden Neuinstallation müssen (!) Sie auch **alle Passwörter** für die von Ihnen auf dem Handy verwendeten Benutzerkonten ändern. Nur durch diese - zugegebenermaßen zeitraubende - Prozedur bekommen Sie die Folgen einer Infektion mit Sicherheit in den Griff.

Alternativ können Sie die Malware mit der folgenden Anleitung gezielt **deinstallieren**. Der Vorteil: alle anderen Apps, Daten und Einstellungen bleiben erhalten. Gerade bei „einfacher“ Malware, die zum Beispiel nur Werbung einblendet, kann diese Methode ratsam sein. Perfekte Sicherheit bietet sie aber ausdrücklich nicht.

Schritt 1: Im abgesicherten Modus neu starten

Starten Sie Ihr Handy als erstes im abgesicherten Modus neu. Dabei lädt Android ausschließlich die Apps, die zum Betriebssystem gehören beziehungsweise vom Hersteller vorinstalliert wurden. So verhindern Sie, dass die Malware schon beim Neustart geladen wird. Häufig ist auch nur dadurch die Deinstallation möglich, zu der wir gleich kommen.

Der Weg zum abgesicherten Modus hängt davon ab, welches Gerät Sie verwenden. Bei **Original-Android**, wie es sich zum Beispiel auf Googles Pixel-Geräten findet, halten Sie zunächst den Power-Knopf gedrückt. Erscheint dann der „Ausschalten“-Knopf auf dem Display, halten Sie diesen gedrückt. Jetzt werden Sie gefragt, ob Sie beim Neustart in den sicheren Modus wechseln möchten. Ist das Handy schon aus, dann schalten Sie es ein, warten bis das Android- beziehungsweise Hersteller-Logo erscheint und halten dann den Leiser-Knopf

gedrückt. Um den abgesicherten Modus zu verlassen starten Sie Ihr Handy neu.

Bei **Samsung** heißt der abgesicherte Modus kurz „Sicherer Modus“ und lässt sich auf vielen Geräten aktivieren, indem Sie beim Einschalten die Leiser-Taste gedrückt halten, bis die PIN abgefragt wird. Auch hier reicht ein Neustart zum Verlassen des sicheren Modus. Andere Samsung-Geräte erfordern mehrfaches Antippen des Menü-Buttons (versteckt links von der Home-Taste) um zum sicheren Modus zu gelangen beziehungsweise ihn wieder zu verlassen.

Funktioniert keine der geschilderten Methoden, dann suchen Sie am besten im Web nach einer Anleitung, zum Beispiel mit dem Namen Ihres Handys und dem Stichwort „Abgesicherter Modus“ oder „Safe Mode“.

Schritt 2: Werbung gezielt ausblenden

Malware landet in der Regel als App auf dem Handy. Dem entsprechend lässt sie sich wieder beseitigen, indem Sie die **App deinstallieren**. Häufig tarnen sich Schadprogramme aber mit harmlosen Namen. Androids Rechteverwaltung hilft bei der Identifikation: speziell Malware, die mit **Werbebannern** nervt, blendet diese häufig über anderen Apps ein.

Apps, die dieses Recht beanspruchen, listet Android in einer eigenen Rubrik der Einstellungen, aber sehr versteckt. Öffnen Sie die Einstellungen und tippen auf „**Apps & Benachrichtigungen**“. Dann gehen Sie ganz unten auf „Erweitert“ und tippen anschließend auf „Spezieller App-Zugriff“. Nun tippen Sie auf „Über anderen Apps einblenden“.

Nun sehen Sie eine Liste aller Apps mit der entsprechenden Berechtigung. Prüfen Sie sie auf **verdächtige Einträge**. Anschließend können Sie die App deinstallieren (dazu gleich mehr, merken Sie sich nur den Namen). Je nach App kann es auch schon reichen, wenn Sie Ihr die „Einblendung über anderen Apps“ verbieten. Dazu tippen Sie den Knopf hinter dem Recht an.

Schritt 3: App deinstallieren

Wie Sie Apps deinstallieren wissen Sie sicherlich. Sie halten das App-Symbol in der App-Übersicht gedrückt und ziehen es auf den Papierkorb. Oder Sie öffnen die Einstellungen, wechseln auf „**Apps & Benachrichtigungen**“, tippen die App an und gehen auf „Deinstallieren“.

Manche Apps wehren sich allerdings gegen die Deinstallation. Sie fragen schon bei der Installation nach Administratorrechten (auch „Geräte-Administrator“ oder „Geräte-Verwaltung“ genannt). Gerade wenn sich Malware als Virenscanner oder Diebstahlschutz tarnt scheint das auch nachvollziehbar, wird bei der Deinstallation aber zum Problem.

Um solche Apps zu deinstallieren öffnen Sie als erstes die Einstellungen und gehen dort auf „**Sicherheit & Standort**“ und auf „Apps zur Geräteverwaltung“. In der folgenden Übersicht finden Sie alle Apps, die auf Ihrem Gerät als Administrator eingetragen sind. Entfernen Sie die Malware hier. Anschließend können Sie sie wie gewohnt deinstallieren.

Nach der Deinstallation überprüfen Sie den Erfolg Ihrer Maßnahmen, indem Sie Ihr **Handy neu starten** - diesmal nicht im abgesicherten Modus.

Quelle: https://www.connect.de/ratgeber/smartphone-malware-entfernen-tipps-3198419.html?utm_source=connect-NL&utm_medium=newsletter

4) Abo-Mitgliedschaft – YouTube Premium: Drastische Preiserhöhung angekündigt

Schlechte Nachrichten für Abonnenten von YouTube Premium: Ab November steigen die Preise deutlich. In manchen Ländern verdreifachen sich die Gebühren.

YouTube Premium wird deutlich teurer. Die Preiserhöhung der Abo-Mitgliedschaft für seine Videoplattform hat Google in einer E-Mail an seine Nutzerinnen und Nutzer offiziell angekündigt. So müssen Kunden aus Argentinien mit der größten Kostensteigerung rechnen – das Einzelabo wird dort mehr als doppelt, das Familienabo fast dreimal so teuer wie zuvor.

Bislang wurde für Deutschland noch keine Preissteigerung angekündigt, diese könnte in nächster Zeit aber noch folgen. In den USA steigen die Abo-Preise für die Familienmitgliedschaft um 5 US-Dollar, in Deutschland wäre eine Preiserhöhung um 5 Euro pro Monat also nicht unwahrscheinlich. Bereits in der Vergangenheit fielen europaweite Preissteigerungen ähnlich hoch aus wie in den Vereinigten Staaten. Derzeit kostet hierzulande das Einzelabo noch 11,99 Euro, das Familienabo 17,99 Euro.

In Kraft treten wird die Änderung zum 21. November 2022 – Kunden, für die die Preissteigerung zu hoch ausfällt, haben also noch genug Zeit, ihre Mitgliedschaft zu kündigen. Das funktioniert über den Bereich "Kostenpflichtige Mitgliedschaften" im eigenen YouTube-Konto.

Was ist YouTube Premium?

Bei YouTube Premium handelt es sich um eine kostenpflichtige Mitgliedschaft auf Googles Videoplattform YouTube. Diese wird größtenteils durch das Einblenden von Werbung finanziert. Abonnenten können den Service jedoch ohne die Einblendung von Werbevideos und Werbeanzeigen nutzen.

Darüber hinaus können sie Videos herunterladen und offline ansehen (auf Mobilgeräten) und Videos auch im Hintergrund laufen lassen. Bei Gratiskunden bricht die Wiedergabe ab, sobald die App in den Hintergrund verschoben wird.

Darüber hinaus profitieren Kunden auch von YouTubes Streamingdienst "YouTube Music", auf der Millionen Songs ohne Werbeunterbrechungen angehört werden können. Zudem lässt sich die Musik in der zugehörigen Music-App auch herunterladen und offline abspielen.

Quelle: https://www.t-online.de/digital/internet-sicherheit/internet/id_100069160/kostenexplosion-fuer-abonnenten-youtube-premium-wird-deutlich-teurer.html

5) TeleGuard statt Telegram oder WhatsApp: Schweizer Messenger holt Ihre Privatsphäre zurück

Der Schweizer Messenger TeleGuard vereint die besten Funktionen von WhatsApp & Co. und verspricht höchste Sicherheit. Was die App kann, lesen Sie hier.

WhatsApp ist zweifelsohne noch immer der Platzhirsch unter den Messengern, obwohl schon länger bekannt ist, dass die Anwendung in Sachen Datenschutz ziemlich problematisch ist. Mit Telegram, Threema und Signal stehen bekannte Alternativen zur Verfügung, doch keine davon ist wirklich perfekt.

Die kostenlose App TeleGuard aus der Schweiz möchte die besten Funktionen der verschiedenen Apps vereinen. Der Messenger ist verschlüsselt, kostenlos und erfordert keine Telefonnummer oder E-Mail zur Anmeldung – damit ist er zum Beispiel bestens für den Einsatz an Schulen oder Kitas geeignet.

TeleGuard Update: Neue Funktionen

Mit der aktuellsten Version bekommt die TeleGuard die erste Bezahlfunktion hinzu, die aber nur optional ist. Der Hersteller will so neben den eingehenden Spenden die Entwicklung der App finanzieren.
So können Sie sich ab sofort personalisierte TeleGuard-IDs zulegen. Damit wird die Anwendung

auch für den professionellen Einsatz mit hohem Datenschutz attraktiver, zum Beispiel:

- in Schulen
- für Arztpraxen
- bei Beratergruppen

Die sich dann statt der zufälligen Kombination aus Buchstaben und Zahlen auch spezifische Namen anlegen können, zum Beispiel "ZahnarztSchulzeTreptow".

TeleGuard: Ohne Anmeldung und Telefonnummer

Laden Sie die TeleGuard-App für Android oder iOS zunächst kostenlos auf Ihr Smartphone. Beim ersten Start legen Sie einfach einen Nutzernamen fest, die individuelle TeleGuard-ID wird automatisch vergeben – neben der manuellen Eingabe dieser Nummer lassen sich neue Kontakte auch per QR-Code hinzufügen. Tippen Sie dazu auf beiden Geräten auf das QR-Symbol und fotografieren Sie den Bildschirm des Gegenübers ab. Danach können Sie miteinander chatten.

Die Anruf- und Videocall-Funktion erreichen Sie oben über den Telefonhörer oder das Kamera-Symbol. Wie bei allen modernen Messengern lassen sich Bilder, Videos und Dokumente problemlos als Anhänge verschicken und auf dem Gerät des Empfängers abspeichern. Durch Tippen und Halten des Mikrofons neben dem Textfeld nehmen Sie auch Sprachnachrichten wie gewohnt auf.
Tipp: Der Emoji-Button von TeleGuard zeigt leider nur sehr altbackene Emojis an, die Sie vielleicht noch aus ICQ oder MSN kennen. Für Retro-Feeling ganz nett, aber wir empfehlen, dass Sie einfach die Emojis Ihrer Smartphone-Tastatur verwenden. Hier gibt es eine größere Auswahl.

TeleGuard: Gruppenchats, Channels und Einstellungen

Sie können eigene Gruppenchats zu erstellen oder so genannten Channels beitreten. Der Unterschied: Bei Gruppenchats können alle Mitglieder gleichberechtigt an den Unterhaltungen teilnehmen, bei einem Channel darf nur der Inhaber Posts veröffentlichen. Die Abonnenten haben dann lediglich die Option, Herzen oder Daumen runter zu vergeben.

Da sämtliche Server in der Schweiz stehen, ist der Hersteller nicht gemäß EU-Richtlinien verpflichtet, Daten herauszugeben. Gleichzeitig sei TeleGuard aber DSGVO-Konform. Somit haben etwa Lehrer die Möglichkeit, Ankündigungen an die gesamte Klasse zu schicken oder den digitalen Austausch zwischen Schülern zu fördern, ohne gegen geltende Datenschutzregeln zu verstoßen.

Tipp: Anders als bei Telegram existieren in TeleGuard bei den Channels Community-Richtlinien. Diesen müssen Sie vor der Erstellung eines eigenen Channels zustimmen. Der Entwickler möchte damit verhindern, dass in den öffentlichen Kanälen Hetze, verfassungsfeindliche Inhalte oder Mobbing verbreitet werden.
Der Hersteller verspricht, Inhalte permanent von einem Team zu prüfen und alles, was nicht konform ist mit den Bedingungen für Channels, umgehend zu löschen.

Anmerkung der Redakion: Weitere Infos, sowie die Anwendung können unter dem u.g. Link abgerufen werden.

Quelle: https://www.chip.de/news/TeleGuard-statt-Telegram-oder-WhatsApp-Schweizer-Messenger-holt-Ihre-Privatsphaere-zurueck_183620790.html?utm_source=nl_chipd-wy&utm_medium=chip-newsletter&utm_campaign=23-10-2022%2B07%253A00%253A01&utm_content=nl_chipmob&utm_term=

6) Mit Malware verseucht – Schleunigst löschen: Diese 14 Apps schaden Ihrem Handyakku extrem

Nürnberg - Wer ein Smartphone mit Android-Betriebssystem nutzt, sollte schleunigst einen Blick auf seine Apps werfen. Im Playstore entdeckten Experten eine ganze Reihe an dubiosen Anwendungen, die Malware enthalten und die Leistung drosseln.

Wie *Computerbild* berichtet, geht es um 14 Apps, die sich in den Google Playstore geschlichen haben. Die Schadsoftware tarnt sich als vermeintlich harmlose Applikation. Wer eine dieser Anwendungen auf dem Handy hat, muss damit rechnen, dass der Akku ungewöhnlich schnell an Saft verliert und überhöhter mobiler Datenverbrauch stattfindet.

Schadsoftware wird durch Installation aktiviert

Zwar hat Google die Android-Apps laut *McAfee* inzwischen bereits aus seinem App-Store entfernt, rund 20 Millionen mal wurden sie jedoch in der Zwischenzeit von Nutzern heruntergeladen. Betroffen sind insbesondere Programme, die vermeintlich das Android-Betriebssystem optimieren sollen, darunter vor allem sogenannte Cleaner-Apps, die den Usern vorgaukeln, nicht benötigten Datenmüll zu löschen und das System so schneller zu machen.

In der Praxis poppt allerdings meist nur Werbung auf. Und das mitunter sogar dann, wenn die App gar nicht geöffnet ist. Eine Installation genügt, um die Malware zu aktivieren. Besonders perfide: Um nach der Installation nicht mehr einfach deinstalliert werden zu können, ändern die Apps ständig ihren Namen und ihr App-Symbol. Dabei geben sie sich auch als Einstellungs-App oder sogar Google Playstore selbst aus.

Welche Apps u. a. betroffen sind

Besonders häufig heruntergeladen wurden die Apps in Südkorea, Japan und Brasilien. Deutschland verzeichnete laut *McAfee* nur vergleichsweise wenige Fälle. Wer dennoch eine der folgenden Apps auf sein Smartphone heruntergeladen hat, sollte sie umgehend entfernen:

- Junk Cleaner
- EasyCleaner
- Power Doctor
- Super Clean
- Full Clean
- Clean Cache
- Fingertip Cleaner
- Quick Cleaner
- Keep Clean
- Windy Clean
- Carpet Clean
- Cool Clean
- Strong Clean
- Meteor Clean

Quelle: https://www.nordbayern.de/ratgeber/technik/schleunigst-loschen-diese-14-apps-schaden-ihrem-handyakku-extrem-1.12645775

7) How-To – eSIM erklärt: Alle Vorteile und Nachteile im Überblick

Die klassische SIM-Karte könnte bald ausgedient haben. Die Branche setzt zunehmend auf die neue eSIM. Das hat Vorteile – aber auch Nachteile.

Mini, Micro, Nano: Das fummelige Herumstöpseln mit immer kleineren SIM-Karten könnte bald ein Ende haben: Mit der neuen eSIM steht eine komfortable und sichere Alternative zur Verfügung. Aktuelle Smartphones wie das iPhone 14, aber auch Geräte anderer Hersteller und einige Smartwatches sind damit bereits kompatibel. Das Wichtigste haben wir für Sie zusammengefasst.

Anders als die klassische SIM-Karte wird eine eSIM (embedded SIM) nicht manuell in einen Kartenslot im Handy gesteckt. Neuere Smartphones und Smartwatches haben die Chipkarte bereits an Bord, sie ist dort fest integriert. Um sich gegenüber Netzbetreibern damit zu identifizieren, können die Karten individuell programmiert werden, das klappt im Handumdrehen.

Vorteile der eSIM

In der täglichen Nutzung gibt es keine großen Unterschiede zur klassischen SIM. Vorteil ist, dass Sie nach einem Vertragsabschluss nicht mehr warten müssen, bis der Provider die SIM-Karte per Post schickt, sondern Sie können Ihren Mobilfunkvertrag mit der eSIM direkt nutzen. Im Grunde ist die eSIM also eine Weiterentwicklung der SIM, die Nutzern Arbeitsschritte erspart und Prozesse komfortabel verkürzt. Sie hat aber noch weitere Vorteile. Probleme mit falschen Karten-Formaten entfallen und eSIMs können mehrere Profile gleichzeitig speichern. Bis zu sechs Profile dürfen das etwa beim neuen iPhone sein – auch wenn dann nur maximal zwei gleichzeitig aktiv sein können. Zum Freischalten eines Vertrages genügt bei der eSIM das Scannen eines QR-Codes.

Auch die Nutzung von Mobilfunkverträgen kann die eSIM flexibler machen. Anpassungen oder Kündigungen sind einfacher und schneller möglich als bisher, zudem lassen sich mehrere Rufnummern verwalten. Der neue Standard könnte den Mobilfunk auch insgesamt günstiger machen. Zudem lassen sich Funklöcher damit leicht umgehen, etwa mit einem schnellen Netzwechsel. Wer viel im Ausland unterwegs ist oder verschiedene Tarife fürs Telefonieren und für Datendienste nutzt, hat es mit der eSIM leichter, weil der Netzwechsel damit so einfach möglich ist.

Auch für Hersteller mobiler Geräte bringt der neue Standard einen Vorteil. Wenn er die alte SIM-Karte ersetzt, dann steht im Gehäuseinneren etwas mehr Platz zur Verfügung und eine potenzielle Fehler- und Schadensquelle entfällt.

Nachteile der eSIM

Dabei handelt es sich um eine Form des Identitätsdiebstahls: Wenn ein böswilliger Akteur es schafft, sich beim Provider als jemand anderes auszugeben, dann könnte er per eSIM quasi direkt den fremden Vertrag nutzen, denn er muss sich die SIM ja nicht erst an die eigene Adresse schicken lassen. Nutzer können mit der eSIM auch nicht mehr so leicht physisch offline gehen, indem sie wie früher ihre SIM aus dem Gerät ziehen. Überwachungssoftware oder Spionageprogramme könnten das theoretisch ausnutzen.

Weil die eSIM im Gerät fest verbaut ist, kann man auch nicht ohne Weiteres auf ein Ersatzgerät umsteigen, wenn das Smartphone kaputt geht oder der Akku leer ist. Auch die Betrugsmasche SIM-Swapping wäre mit der eSIM womöglich einfacher.

Ein potenzieller Nachteil für Mobilfunkanbieter ist aber wiederum ein Vorteil für Verbraucher: Der Wechsel zu einem neuen Provider oder in andere Tarife ist mit der eSIM viel einfacher.

Diese Geräte unterstützen den neuen Standard

Viele aktuelle Geräte unterstützen das neue Verfahren bereits. Bei Apple beginnt der Support beispielsweise beim iPhone XS, damit ist auch das aktuelle iPhone 14 eSIM-tauglich. Zumindest in den USA liefert Apple das neueste iPhone schon gar nicht mehr mit dem alten SIM-Kartenslot aus, dort wird nur noch eSIM unterstützt. Das dürfte die Verbreitung der fest verbauten Chipkarte weiter beflügeln.

Bei Google wird eSIM ab dem Pixel 3 unterstützt. Samsung hat die Funktionen ab den Modellen der S20-Reihe spendiert – so haben auch die Galaxy-S22-Modelle eine eSIM an Bord. Auch einige Smartwatches der Koreaner beherrschen den neuen Standard. Bei Huawei kann man die eSIM aktuell mit den Smartphones Huawei P40, Huawei P40 Pro und dem Huawei Mate40 Pro nutzen.

So aktivieren Sie eine eSIM

Wenn Sie das neue Verfahren nutzen möchten, erhalten Sie nach Abschluss eines neuen Vertrages vom Provider in der Regel einen QR-Code. Der wird etwa im Kundenprofil online angezeigt und Sie können ihn dann direkt nutzen. Das ist aber noch nicht überall der Fall: Teilweise müssen Sie auch noch Servicepersonal kontaktieren, eine Niederlassung aufsuchen oder gar darauf warten, dass der QR-Code per Post kommt – das macht manche Vorteile der eSIM natürlich gleich wieder zunichte. Mit der Zeit dürfte die Einrichtung aber immer einfacher werden und standardmäßig über Kundenprofile möglich sein.

Nächster Schritt: iSIM

Während die eSIM die klassischen SIM-Karten womöglich gerade ablöst, steht die nächste Technologie bereits vor der Tür: die iSIM. Anders als die eSIM, die ja nur fest ins Gerät eingebettet ist („embedded“ SIM), soll die iSIM („integrated“ SIM) das Konzept einer physischen SIM-Karte komplett ablösen.

Dabei handelt es sich um eine rein virtuelle Lösung, die direkt in den Hauptprozessor eines Gerätes integriert werden kann. Vodafone und Qualcomm haben die iSIM-Technologie prototypenmäßig in einem Galaxy Z Flip 3 bereits demonstriert. Bis das brandneue Verfahren ausgerollt wird, wird es aber wohl noch eine Weile dauern: Jetzt kommt erst einmal die eSIM zum Zug.

Quelle:https://www.pcwelt.de/article/1355091/was-ist-eine-esim.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20eSIM%20erkl%C3%A4rt%3A%20Alle%20Vorteile%20und%20Nachteile%20im%20%C3%9Cberblick&utm_campaign=Best-of%20PC-WELT&utm_term=PC-WELT%20Newsletters&utm_date=20221024100556&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

8) How-To – Kindersicherung der Fritzbox einrichten – so geht’s

Die Fritzbox umfasst einige interessante Funktionen, mit denen sich die Internetnutzung von Kindern und Jugendlichen gezielt einstellen und detailliert regeln lässt.

1. Zeitraum der Internetnutzung festlegen

Die Fritzbox besitzt eine integrierte Kindersicherung, mit deren Hilfe sich die Internetnutzung verbundener Geräte recht detailliert regeln lässt. Um an die Optionen zu gelangen, klicken Sie in der Konfigurationsoberfläche auf „Internet“, wählen „Filter“ und bringen das Register „Kindersicherung“ nach vorne.

In der daraufhin angezeigten Liste sind alle Geräte aufgeführt, die den Internetzugang der Fritzbox nutzen. In der Grundeinstellung kommt das Zugangsprofil „Standard“ zum Einsatz. Wollen Sie einem der Geräte die Internetnutzung komplett verwehren, wählen Sie im Ausklappmenü die Option „Gesperrt“. Alle Netzwerkgeräte, die sich neu an der Fritzbox anmelden, erhalten automatisch das Zugangsprofil „Standard“. Klicken Sie auf das blaue Stift-Symbol, um das Zugangsprofil an Ihre Bedürfnisse anzupassen.

In der Grundeinstellung sind die Zeitbeschränkung eingeschaltet und die Option „Immer“ voreingestellt. Sinnvoller ist es, ein benutzerdefiniertes Zugangsprofil anzulegen. Im Register „Zugangsprofile“ klicken Sie auf „Neues Zugangsprofil“ und geben eine Bezeichnung ein, zum Beispiel „Kindersicherung Hannah“. Klicken Sie auf das Stift-Symbol zur Bearbeitung des Profils. Anschließend aktivieren Sie unter „Zeitraum“ die Option „eingeschränkt“ und entscheiden sich über die jeweiligen Schaltflächen für „Internetnutzung erlaubt“ oder „Internetnutzung gesperrt“.

Im folgenden Fenster setzen Sie Häkchen vor die jeweiligen Wochentage und legen das Zeitfenster von bis als Uhrzeit fest. Klicken Sie dann auf „Zeitraum hinzufügen“, um die getroffenen Einstellungen in den Kalender einzutragen. Alternativ positionieren Sie den Mauszeiger am Startzeitpunkt. Drücken Sie die linke Maustaste und ziehen Sie den Mauszeiger bis zum gewünschten Ende der Nutzungszeit. Sollen die nachfolgenden Tage dieselbe Markierung erhalten, dann ziehen Sie den Mauszeiger einfach nach unten.

2. Online-Zeit beschränken

Eine andere Möglichkeit zum Einschränken der Online-Nutzungszeit nehmen Sie unter „Zeitbudget“ vor. Klicken Sie auf „eingeschränkt“ und geben Sie an, wie viele Stunden mit dem Profil täglich im Internet verbracht werden dürfen. Nicht vergessen dürfen Sie, „Nutzung des Gastzugangs gesperrt“ zu aktivieren, damit das Gerät nicht darüber online gehen kann. Mit einem Klick auf die Schaltfläche „OK“ speichern Sie das Profil, das Sie dann beliebigen Geräten zuweisen können.

3. Filter für Internetseiten aktivieren

Reicht Ihnen für die Familienmitglieder die zeitliche Einschränkung der Internetnutzung nicht aus, steht Ihnen in der Fritzbox-Konfigurationsmaske mit „Filter für Internetseiten“ eine weitere praktische Funktion zur Auswahl bereit. Aktivieren Sie sie, indem Sie ein Häkchen setzen. Anschließend werden darunter zusätzliche Optionen eingeblendet. Über die Filterlisten legen Sie fest, welche Internetseiten beim Aufruf im Webbrowser erlaubt („Whitelist“) oder gesperrt („Blacklist“) sind. Treffen Sie für das neue Profil die gewünschte Auswahl – in unserem Beispiel „Internetseiten sperren (Blacklist) (Liste anzeigen).“ Die jeweiligen Listen müssen Sie über „Internet“, „Filter“ und „Listen“ selbst füllen, da in der Grundeinstellung keinerlei Webseiten hinterlegt sind. Klicken Sie auf „bearbeiten“, tippen Sie die Internetadressen der gesperrten Webseiten ein und speichern Sie die Änderungen per Klick auf „OK“.

4. Netzwerkanwendungen sperren

Falls erforderlich, können Sie auch die gesperrten Netzwerkanwendungen im Profil festlegen. Dazu öffnen Sie das Ausklappmenü bei „Netzwerkanwendung sperren“ und wählen einen Eintrag aus, etwa „FTP-Server“. Möchten Sie sich nicht mit Details auseinandersetzen, entscheiden Sie sich im Ausklappmenü bei „Netzwerkanwendung sperren“ für „alles außer Surfen und Mailen“.

Alternativ erstellen Sie auch eigene Netzwerkanwendungen, die gesperrt werden sollen. Gehen Sie dazu zu „Filter –› Listen“ und klicken Sie auf den blauen Link „Netzwerkanwendungen“. Über „Netzwerkanwendung hinzufügen“ nehmen Sie eine beliebige Anwendung in die Liste auf.

Vergeben Sie im Eingabefeld „Netzwerkanwendung“ einen Namen und wählen das Protokoll und den Port aus. Klicken Sie zum Speichern der Einstellungen auf „OK“. Danach können Sie den neuen Eintrag aus der Liste auswählen.

Anmerkung der Redaktion: Weitere Infos können unter dem u.g. Link abgerufen werden

Quelle: https://www.pcwelt.de/article/1183304/kindersicherung-der-fritzbox-fuer-mehrere-geraete-nutzen.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Kindersicherung%20der%20Fritzbox%20einrichten%20%E2%80%93%20so%20geht%27s&utm_campaign=Best-of%20PC-WELT&utm_term=PC-WELT%20Newsletters&utm_date=20221024101339&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

9) FritzBox erhält über 100 neue Funktionen: Gratis-Update FritzOS 7.50 mit vielen Highlights

AVM veröffentlicht in Kürze FritzOS 7.50 ein großes Update für seine WLAN-Router mit über 100 neuen Funktionen. Wir zeigen die Neuheiten und wie Sie diese bereits jetzt ausprobieren können.

Das nächste große Update für die FritzBox-Firmware wird **FritzOS 7.50** sein. Es bringt gratis über 100 Neuheiten für verschiedene FritzBox-Modelle. Wann das fertig ist? Recht bald, doch einen offiziellen Starttermin hat AVM noch nicht verraten.

Fakt ist aber, dass die Beta-Versionen aktuell in schneller Folge Updates kriegen, AVM macht also noch Feinschliff. Auf diesen Geräten lässt sich das neue FritzOS bereits jetzt vorab testen:

- FritzBox 7590 AX, 7590
- FritzBox 6591 Cable, 6660 Cable, 6690 Cable
- FritzBox 7530 AX, 7530
- FritzBox 6850 LTE, 6890 LTE
- FritzRepeater 2400, 3000

Wenn Sie den Start von FritzOS 7.50 nicht mehr abwarten können, können Sie schon jetzt in die Neuheiten reinschnuppern. Voraussetzung ist die Labor-Firmware 7.39. Die ist sozusagen die Testumgebung für alles, was AVM mit FritzOS 7.50 kriegen möchte. Einmal aktualisiert, können Sie die Neuheiten von FritzOS 7.50 vorab nutzen und kommen auf Wunsch auch schnell wieder auf die finale Firmware zurück.

FritzOS 7.50: WireGuard VPN und Mesh-WLAN

FritzOS 7.50 wird ein richtig großes Release, das die FritzBox an vielen Stellen aufwerten wird. Rund 20 Neuheiten und fast 100 Verbesserungen nennt AVM. Die wichtigsten Neuheiten:

- **WireGuard:** Die FritzBox kriegt Support für das WireGuard VPN-Protokoll und damit einfachen, schnellen und sicheren VPN-Zugriff.
- **Neue Optik:** Die FritzBox-Oberfläche kriegt ein Optik-Update mit frischen Farben, schicken Icons und größeren Abständen. Das sieht nicht nur moderner aus, sondern ist auch übersichtlicher.
- **Suche:** Die FritzBox kriegt immer mehr Funktionen, über eine neue Stichwortsuche lassen sich die aufspüren.
- **Telefonbuch:** Rufumleitungen und Rufsperren können auf "Nicht im Telefonbuch" enthaltene Anrufer angewendet werden.
- **FritzFon:** Es gibt eine Ansage für Anrufe, Wecker und Termine. Außerdem wird ein Terminkalender auf den FritzFon unterstützt.
- **Smarthome:** Smarthome-Vorlagen mit zusätzlichen Komfortfunktionen sind Teil von

FritzOS 7.50. Hinzu kommen Szenarien und Routinen.

- **Festplatten:** Es werden exFAT-formatierte Speichermedien an den USB-Schnittstellen der FritzBox unterstützt.
- **Mesh-WLAN:** Umfangreich geht AVM auch das Thema Mesh-WLAN an. So gibt es Verbesserungen bei der Datenrate und bei der automatischen Kanalwahl.
- **Speed-Verteilung:** Ein neuer Modus zur Steuerung der Geschwindigkeit im Heimnetz soll die verfügbare Bandbreite auf alle aktiven Geräte gerecht verteilen.
- **Gastnetz:** Gäste soll man gut behandeln, FritzOS 7.50 spendiert für Gastzugänge höhere Download-Geschwindigkeiten.
- **Ausfallsicherung:** Eine neue Option erlaubt beim Ausfall des DNS-Servers die automatische Umschaltung auf öffentliche Server.
- **DSL:** Verbesserungen bei Interoperabilität gegenüber ADSL2+ und VDSL-Gegenstellen.
- **Kabel:** Auch das Zusammenspiel mit DOCSIS wurde bei Kabelmodellen verbessert. FritzBoxen zeigen jetzt auch das genutzte Spektrum im Detail an.
- **Sperrlisten:** Es wird eine IP-Sperrliste für eingehende Datenpakete angeboten.
- **Apps:** Der Zugriff auf die Oberfläche ist für Apps optimiert worden. Damit lassen sich dann auch neue Funktionen nutzen, etwa die Priorisierung von Anwendungen.
- **Repeater-Update:** Kommt eine FritzBox als Mesh-Repeater zum Einsatz, kann sie mit FritzOS 7.50 beide WLAN-Frequenzbänder für den Uplink nutzen.
- **Migrations-Assistent:** Mit dem neuen Migrations-Assistenten wird es einfacher, FritzBox-Modelle zu wechseln und möglichst viele Daten und Einstellungen mitzunehmen.

FritzBox Labor-Firmware nutzen

Ein Labor-Update für die FritzBox ist mit Vorsicht zu genießen und sicher nichts, was sich alle Nutzer einfach mal installieren sollten. Der Status entspricht dem einer Betaversion und AVM übernimmt für Probleme keine Haftung. Über "System|Update|FRITZ!OS-Version" kommen Sie übrigens auch immer zurück zum offiziellen FritzOS.

Wenn Sie die Laborversion von FritzOS einspielen wollen, sollten Sie vorab einen Update-Durchlauf starten, um die letzte stabile Version auf der Box zu haben. Dann suchen Sie sich den Download für Ihr FritzBox-Modell.

- Klicken Sie auf "Download" und speichern Sie die Datei auf Ihrem Computer.
- Entpacken Sie die Zip-Datei mit der Firmware.
- Führen Sie das Update über die Benutzeroberfläche der FritzBox durch und wählen Sie in der Fußzeile "Ansicht: Erweitert" aus.
- Wählen Sie im Menü "System|Update".
- Klicken Sie die Registerkarte "FRITZ!OS-Datei" an. Sichern Sie die Einstellungen Ihrer FritzBox.
- Geben Sie dann den Namen der Laborversion samt Pfad in das Eingabefeld ein (z. B. C:\Dokumente und Einstellungen\Benutzername\Desktop\FRITZ!Box-Labor-xxxx.image).
- Klicken Sie auf "Update starten".
- Folgen Sie den Anweisungen auf dem Bildschirm.
- Während des Update-Vorgangs blinkt die Leuchtdiode "Info" Ihrer FritzBox. Diese erlischt, wenn der Update-Vorgang abgeschlossen ist. Sobald das Update abgeschlossen ist, wird die FritzBox neu gestartet und ist anschließend wieder betriebsbereit.

Quelle: https://www.chip.de/news/FritzBox-erhaelt-ueber-100-neue-Funktionen-Gratis-Update-FritzOS-7.50-mit-vielen-Highlights_184048568.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=20-10-2022%2B17%253A00%253A09&utm_content=nl_chipmob&utm_term=

10) News – Firefox 106: So ersetzt Firefox teure Software

Die neueste Aktualisierung des Firefox-Browsers bringt interessante Funktionen mit wie die direkte Bearbeitung von PDFs und eine variable Tab-Verwaltung.

”Mit Firefox 106 können Sie direkt in Browser-PDFs tippen”, heißt es im Blogpost von Mozilla auf “The Register”, danach gleich eine“ Entschuldigung“ an Adobe, denn die User könnten nun im Browser in PDFs direkt hinein schreiben oder auch zeichnen, so auch etwa mit der eigenen Unterschrift. Zwar kann Firefox wie auch andere Browser PDFs längst im eigenen Fenster anzeigen, auch Formulare ließen sich bereits ausfüllen, doch nun habe man den eingebauten Javascript-basierten PDF-Viewer aktualisiert, sodass Mozilla weitere Funktionen direkt zur Verfügung stellt. Zum Beispiel können User nun PDF-Dokumente mit Anmerkungen versehen, also ohne Umwege über andere lokale PDF-Programme in ein PDF-Dokument tippen oder schreiben, wobei sich auch Parameter wie Farbe, Größe, Linienstärke, Deckkraft auswählen lassen. Dieses bearbeitete und ergänzte PDF-Dokument lässt sich auf der Festplatte oder auf einem anderen Medium speichern und teilen. Außerdem zeigt Firefox ab Version 106 auf anderen Plattformen erstellte Kommentare in PDF-Dateien an, was auch in anderen PDF-Viewern nicht immer anstandslos funktioniert. Hier aber schon?

Der neue Firefox im Mini-Test

Wir laden uns als erstes die neueste Version von Firefox für den Mac herunter (tatsächlich haben wir auf dem Beta-Kanal bereits die Version 107). Dann öffnen wir wahllos verschiedene PDFs, indem wir sie einfach auf das Firefox-Fenster ziehen. Diese werden problemlos dargestellt. Nun findet man oben rechts im Firefox-Menü verschiedene neue Werkzeuge. Damit lässt sich in der Tat ganz einfach in beliebige Stellen des geöffneten PDFs schreiben, die Größe regelt man über einen Schieberegler, die Farbe lässt sich wie gewohnt auswählen, nur die Schrift kann man nicht selbst bestimmen. Beim direkt daneben liegenden Zeichen-Tool, das wie gesagt auch für die eigene Signatur/Unterschrift wichtig ist, wählt man ebenfalls die Farbe im Farbpicker, bestimmt die Dicke des Striches und auch die Transparenz, dies alles geht auch noch nachträglich.

Die PDF – Datei lässt sich speichern und dann beispielsweise im Apple-Programm Vorschau betrachten. Alle unsere Veränderungen werden problemlos angezeigt. Nun machen wir es umgekehrt und fügen in Vorschau Kommentare, Anmerkungen und eine Sprechblase hinzu, speichern dies und öffnen es in Firefox auf dem Mac – ebenfalls kein Problem, nur bei den Notizen ist die Anzeige nicht so einwandfrei, aber hier haben wir auch in Vorschau selbst schon ein Problem vorliegen.

Ganz zufrieden sind wir noch nicht. So öffnen wir dasselbe PDF unter Windows 11, schon im Explorer sehen wir im Vorschaubild, dass unsere Anmerkungen und Kommentare einwandfrei zur Anzeige kommen, ebenso in den dann benutzten PDF-Programmen unter Windows. Hier tippen wir noch einen weiteren Text ein, speichern wiederum und sehen, dass dies auch auf dem Mac unverändert vorhanden ist.

Der Browser liest auch Text aus Bildern heraus

Interessant ist ferner die Möglichkeit, aus Fotos Text innerhalb des Browsers zu extrahieren. Dazu heißt es in dem Blog: ”Der PDF-Viewer kann auch auf die verborgene Textebene zugreifen, die in einigen PDFs eingebettet ist, etwa durch OCR-Anwendungen – und er kann diesen Text weiterleiten, so an Bildschirmleseprogramme wie Voiceover für Nutzer mit Sehbehinderungen. Er kann auch Text aus Bildern extrahieren.”

Die letztere Funktion probieren wir an einem einfachen Beispiel aus. Nämlich mit dem Bild des Macwelt-Morgenmagazins vom Donnerstag. Dort sieht man einen schönen Sonnenuntergang

am Strand. Uns interessiert jetzt aber lediglich die Schrift: “Macwelt Morgenmagazin“. Mit einem Rechtsklick auf das Bild erscheint die Option, ”Text aus Grafik kopieren”. Genau das machen wir, und schon haben wir die beiden Wörter in unserer Zwischenablage. In Apples Vorschau, wenn man das Foto gespeichert hat, lässt sich dies zwar fast noch leichter herauskopieren. Doch eben – man muss weitere Schritte wie das Herunterladen und erneut öffnen dazwischen legen. Das ist jetzt mit Firefox, sofern es mit dem gegebenen Foto möglich ist, direkt gegeben.

Fazit

Wer den Firefox-Browser ohnehin nutzt, muss nicht lange nachdenken – die aktuelle Version ist nicht nur sicherer als Vorgänger, sondern enthält die beschriebenen neuen Funktionen. Dazu kommt ebenfalls neu die Firefox-Ansicht (View), die einen schnellen Überblick über kürzlich (laut T3N bis zu 25 auf dem Desktop) geschlossene Tabs gibt und die User auch Seiten auswählen lässt, die diese bei aktiver Synchronisierung auf Firefox Mobile lesen – exklusive den Aktivitäten in privaten Fenstern. Die weiteren Neuerungen finden sich in den Release Notes mit Beispielen. Zum Download für den aktuellen Firefox-Browser von Mozilla geht es über diesen Link, sowohl für Mac als auch Windows. Eine Menge Neues also in dem einmal sehr erfolgreichen, jetzt gegenüber Chrome etwas weniger beachteten Browser – besonders für PDF-Bearbeiter unbedingt einen Versuch wert.

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

Quelle: https://www.macwelt.de/article/1358361/firefox-106-so-ersetzt-firefox-teure-software.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Firefox%20106%3A%20So%20ersetzt%20Firefox%20teure%20Software&utm_campaign=Macwelt%20Daily&utm_term=Macwelt%20Newsletters&utm_date=20221024103449&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

11) Android-Tipps – Android sicher machen: 10 Tipps, die Sie beachten sollten

So schützen Sie Ihr Android-Smartphone vor Angriffen und schotten Ihre Daten ab: Mit diesen zehn Tipps machen Sie Ihr Smartphone sicher.

Egal ob Hackerangriffe, Schadsoftware oder Phishing. Cyberkriminelle versuchen es auf vielen Wegen, an Ihre Daten zu kommen. Wenn man sich überlegt, wie viele Informationen auf dem Smartphone heutzutage gespeichert sind, ist das Mobilgerät natürlich auch eine attraktive Angriffsfläche für Betrüger.

Kontodaten, Adressen und unzählige Kontakte, in Zukunft sogar Identitätsnachweise per Führerschein oder Ausweis - all das sollte gut geschützt sein. Wir haben für Sie 10 Tipps, die Ihre Daten auf einem Android-Smartphone schützen.

Tipp 1: Displaysperre einrichten

Ohne Sperre öffnen Sie Angreifern die Tür zu all Ihren Daten. Die SIM-Karte ist standardmäßig mit einer PIN geschützt. Wenn nicht, aktivieren Sie diese unter *Einstellungen/ Sicherheit* und *SIM-Sperre*. Außerdem sollten Sie eine Display-Sperre einrichten. Dann kann nur auf das Handy zugreifen, wer Code, Passwort oder das passende Muster kennt. Die meisten aktuellen Smartphones haben auch einen Fingerabdruck-Sensor oder Gesichtserkennung an Bord, die Sie ebenfalls zur Absicherung verwenden können. Sie stellen die Sperre in den Einstellungen unter Sicherheit und Displaysperre ein.

Tipp 2: Updates sofort installieren

Achten Sie darauf, dass sowohl Betriebssystem als auch alle Programme immer aktuell sind,

und installieren Sie Updates umgehend. Die Entwickler liefern mit Aktualisierungen nicht nur neue Funktionen, sondern schließen auch Sicherheitslücken. Wenn es eine neue Android-Version gibt, bekommen Sie eine Benachrichtigung. Bei Apps sollten Sie automatische Updates erlauben. Rufen Sie dazu den Play Store auf und tippen auf die drei Striche oben links. Wählen Sie dann *Einstellungen* und aktivieren *Automatische Updates* – am besten aber nur über WLAN, sonst müssen Sie womöglich für die Datenübertragung zahlen.

Tipp 3: Nur im Play Store downloaden

Laden Sie Apps nur aus dem offiziellen Play Store von Google herunter, nicht von möglicherweise dubiosen Webseiten. Denn dort fangen Sie sich mit größerer Wahrscheinlichkeit Viren und Schad-Software ein. Um ganz sicher zu gehen, sollten Sie auf Ihrem Handy die Installation von Apps unbekannter Herkunft unterbinden. Das geht bei älteren Android-Versionen unter *Einstellungen* und *Sicherheit*. Ab Android 8.0 finden Sie den Menüpunkt in den Einstellungen unter *Apps/Spezieller Zugriff*. Ganz unten steht *Unbekannte Apps installieren*. Tippen Sie darauf, sehen Sie alle bereits installierten Apps. Prüfen Sie, ob bei allen steht: Nicht zulässig. Ansonsten tippen Sie darauf und verschieben den Regler.

Tipp 4: Auf Berechtigungen achten

Überprüfen Sie bei jeder App, die Sie installieren, welche Berechtigungen sie sich einräumen will. Das steht auf der App-Seite im Play Store unter Berechtigungsdetails. Eine Taschenlampen-Funktion benötigt zum Beispiel keinen Internet-Zugriff. Bei schon installierten Apps entziehen Sie einzelne Berechtigungen unter *Einstellungen/ Apps/App-Berechtigungen*.

Tipp 5: Das Smartphone verschlüsseln

Falls ein Fremder trotz aller Sicherheitsaktionen Ihr Handy in die Hand bekommt, sollte er sensible Daten nicht auslesen können – so wie E-Mails, Kontakte oder Zugangsdaten. Davor schützt die Verschlüsselung des Geräts. Bei den meisten Mobiltelefonen müssen Sie diese einmalig selbst anstoßen. Tippen Sie dazu auf *Sicherheit/Verschlüsselung* und wählen dort die Option *Smartphone verschlüsseln*.

Tipp 6: Obacht im offenen WLAN

Im offenen WLAN im Café oder am Flughafen surfen Sie kostenlos. Aber seien Sie vorsichtig: Mit relativ einfachen Mitteln können andere Sie ausspionieren und mitlesen. Sie sollten deshalb dort nie Online-Banking machen. Seien Sie zudem zurückhaltend bei allen Seiten, bei denen Sie sich einloggen müssen, so wie E-Mail oder Amazon. Zumindest sollten die Seiten eine SSL-Verschlüsselung beim Login geben, erkennbar am https://. Noch besser: Surfen Sie über eine sichere VPN-Verbindung.

Tipp 7: Verbindungen deaktivieren

Apps können über GPS und WLAN-Netze Ihren Standort ermitteln und Bewegungsprofile erstellen. Sie sollten deshalb alle Netzwerk-Funktionen deaktivieren, wenn Sie sie nicht ständig benutzen. Dazu gehören auch Bluetooth und NFC, denn die Schnittstellen können Angreifern potenzielle Einfallstore bieten. Sie schalten all diese Funktionen in den Einstellungen ab – unter *Drahtlos und Netzwerke* und unter *Standort*. Schieben Sie jeweils den virtuellen Regler auf die Aus-Position.

Tipp 8: Diebstahlschutz aktivieren

Es hat aber auch Vorteile, wenn Sie die Standortermittlung einschalten: Sie können dann Ihr Handy orten, falls es verloren geht. Zudem lassen sich dann aus der Ferne alle Daten löschen. Sie müssen die Funktion natürlich vor dem Geräteverlust eingeschaltet haben. Erlauben Sie die

Standortermittlung unter *Einstellungen/Nutzer und Standort*. Dann aktivieren Sie *Sicherheit* und *Mein Gerät finden*. Im Notfall rufen Sie im Browser https://accounts.google.com auf und melden sich dort mit Ihrem Google-Konto an.

Tipp 9: Regelmäßige Backups

Wenn das Smartphone den Geist aufgibt, sind alle Daten weg – außer, Sie sichern sie regelmäßig. Ein Backup der Fotos klappt am einfachsten mit Cloud-Diensten wie Google Drive oder OneDrive, die diese automatisch speichern. Die Einstellungen und Daten von Apps, WLAN-Passwörter oder den Anrufverlauf sichert Google. Aktivieren Sie das über *Einstellungen/Sichern & zurücksetzen* und *Meine Daten sichern*.

Tipp 10: Sicherheits-App verwenden

Bereits die kostenlosen Sicherheits-Apps etwa von Kaspersky, Avira oder Bitdefender schützen vor Malware und scannen neue Programme auf Bedrohungen. Manche bringen sogar Funktionen zur Diebstahlsicherung mit. Ab Android 8.0 aktivieren Sie in den Einstellungen zudem als Zusatz-Schutz die Funktion Play Protect, die installierte Apps auf Sicherheitslücken überprüft.

Quelle: https://www.connect.de/ratgeber/android-smartphone-sicherheit-tipps-einstellungen-3198367.html?utm_source=connect-NL&utm_medium=newsletter

12) Apple veröffentlicht neues macOS: Ventura überrascht mit bisher nicht bekannten Funktionen

Das diesjährige Apple-Update für macOS ist richtig spannend. Die Funktions-Highlights von macOS 13 "Ventura" stellen wir Ihnen hier vor.

Microsoft macht es jetzt auch so wie Apple: Einmal pro Jahr gibt es ein großes Update für das Betriebssystem, kostenlos versteht sich. Das neue macOS Ventura steht ab sofort zum Download bereit.

Laut Apple hat man sich bei der neuen Version vor allem auf zwei Dinge konzentriert: Steigerung der Produktivität sowie Verbesserung der Zusammenarbeit mit anderen Apple-Geräten.

Stage Manager: Bühne frei für den neuen Fenstermanager

Die neue Funktion Stage Manager organisiert automatisch geöffnete Programme und Fenster am linken Bildschirmrand. Zweck der Übung: Nutzer sollen sich auf die aktuelle geöffnete Arbeit konzentrieren können und trotzdem alles andere gut im Überblick behalten.

Das Fenster, in dem gerade gearbeitet wird, wird prominent in der Mitte angezeigt, und andere geöffnete Fenster erscheinen auf der linken Seite. Mit der Maus können Nutzer dann schnell und einfach zwischen den Aufgaben wechseln, inklusive netter Animation versteht sich. Fenster können aber auch gezielt zusammen organisiert werden, etwa wenn Sie an einem Projekten arbeiten, für das unterschiedliche Programme nötig sind. Stage Manager versteht sich auch mit anderen macOS Fenster-Tools wie Mission Control und Spaces.

iPhone als Webcam

Mit der Funktion Kameraübergabe können Mac-Nutzer ein iPhone als Webcam einsetzen. Macs erkennen automatisch die Kamera auf dem iPhone und binden sie ein, wenn das iPhone in der Nähe ist. Dazu muss das Handy nicht mal aufgeweckt werden.

Sie können dann die iPhone-Features der Kamera auf dem Mac nutzen, etwa den Porträtmodus und das neue Studio Light – ein Effekt, der das Gesicht einer Person perfekt ausleuchtet und den Hintergrund abdunkelt. Zusätzlich nutzt die Kamera bei der Zusammenarbeit die Ultraweitwinkelkamera des iPhone, um die Schreibtischansicht zu aktivieren, die gleichzeitig das Gesicht und eine Draufsicht auf den Schreibtisch zeigt.

Weitere Neuheiten in macOS Ventura

- **Safari:** Über geteilte Tabgruppen lassen sich Lieblingsseiten im Browser mit Freunden und Familie teilen.
- **Mail:** Das E-Mail-Programm kriegt eine überarbeitete Suche spendiert. E-Mails, Kontakte, Dokumente, Fotos und mehr sollen sich damit schneller aufspüren lassen. Mails lassen sich planen und einige Sekunden nach dem Absenden sogar zurückholen.
- **Spotlight:** Die Suche hat ein überarbeitetes Design bekommen, das die Navigation vereinfacht. Nutzer finden ihre Fotos jetzt in der Fotomediathek systemübegreifend und im Netz. Man kann Fotos sogar nach Ort, Personen, Szenen oder Objekten suchen und mit Live Text nach Text innerhalb von Fotos. Außerdem startet die Suche jetzt Aktionen, stellt etwa Timer, macht ein neues Dokument auf oder feuert Kurzbefehle ab.
- **Passwörter:** Mit Passkey will Apple Passwörter überflüssig machen. Anmeldungen laufen dann mit Touch ID oder Face ID und werden über den iCloud Schlüsselbund zwischen Mac, iPhone, iPad und Apple TV synchronisiert.
- **Live Text:** Die Live-Text-Funktion soll jetzt auch in Videos klappen.
- **Wetter & Uhr:** Die Programme für Wetter und Uhr Apps erhalten jetzt auch auf dem Mac alle Funktionen von iOS.
- **Systemeinstellungen:** Apple hat Design und Navigation vereinfacht und an die Anordnung von iOS angepasst.
- **Updates:** Über Rapid Security Response soll es zwischen den regulären Updates auch kleinere Updates geben, die auch ohne Neustart des Computers für aktuellen Schutz sorgen.

macOS Ventura Release: Diese Macs und MacBooks kriegen das Update

Weiterhin fährt Apple zweigleisig und bedient mit macOS Ventura die neuen Geräte mit Apple Silicon sowie Intel-Macs. Unterstützt werden folgende Modelle:

- iMac ab 2017
- Mac Pro ab 2019
- iMac Pro ab 2017
- Mac Studio ab 2022
- Mac mini ab 2018
- MacBook Air ab 2018
- MacBook ab 2017
- MacBook Pro ab 2017

Quelle: https://www.chip.de/news/Apple-veroeffentlicht-neues-macOS-Ventura-ueberrascht-mit-bisher-nicht-bekannten-Funktionen_184291495.html?utm_source=nl_chipn-wy&utm_medium=chip-newsletter&utm_campaign=26-10-2022%2B08%253A00%253A10&utm_content=nl_chipn-wy&utm_term=

13) Schnell handeln – EC-Karte verloren: So sperren Sie Ihre Girocard

Einmal nicht aufgepasst – und plötzlich haben Sie Ihre EC-Karte verloren. In diesem Fall heißt es: Sperren Sie Ihre Girocard schnellstmöglich. So geht's.

Es ist immer ärgerlich, wenn Sie Ihre EC-Karte verloren haben. Umso wichtiger ist es, dass Sie richtig und vor allem schnell reagieren.

Denn ansonsten kann es sein, dass sich jemand an Ihrem Konto bedient. Wir zeigen Ihnen, wie Sie Ihre Karte sperren können und was Sie sonst noch beachten sollten.

Wie kann ich meine Karte sperren lassen?

Wenn Sie Ihre Girocard verloren haben oder sie gestohlen wurde, lassen Sie sie umgehend sperren. Dazu können Sie Ihre Bank direkt anrufen. Jede Bank hat eine eigene Nummer für die Kartensperrung. Diese Nummer benötigen Sie auch, wenn Sie die Karte wieder entsperren lassen wollen.

Falls Sie die Nummer gerade nicht parat haben, wenden Sie sich an folgende **Sperr-Rufnummer**: **116 116 (gebührenfrei innerhalb Deutschlands)**

Dieser Sperr-Notruf gilt auch für andere sperrbare Medien wie Visa- oder Mastercard-Kreditkarten sowie zur Sperrung der elektronischen Identitätsfunktion des neuen Personalausweises.

- **Schnell erklärt:** Wie die EC-Karte richtig heißt
- **Girokonto kündigen:** Das sollten Sie unbedingt beachten

Welche Informationen muss ich bei der Sperrung bereithalten?

Beim Sperr-Notruf müssen Sie keine persönlichen Daten wie Name, Kontonummer oder Passworte nennen. Es wird lediglich danach gefragt, welche Bank die Karte ausgestellt hat.

Nach der Weitervermittlung an die Bank – oder wenn Sie sich direkt an Ihre Bank gewandt haben – benötigen Sie einige Informationen.

Ein Überblick:

- Personalausweis
- Kontonummer
- Ort, Datum, Uhrzeit des Verlusts
- Eventuell: Hinweise darauf, dass bereits Geld unbefugt abgehoben wurde

EC-Karte sperren: Welche Kosten entstehen?

Bei den meisten Banken ist das Sperren der Karte kostenlos. Was jedoch Geld kostet, ist das Ausstellen einer neuen Karte samt PIN. Dafür berechnen viele Banken Gebühren von bis zu 30 Euro. Die Kosten sind je nach Bank unterschiedlich hoch.

Tipp: Wenn Sie die Hoffnung haben, Ihre Karte bald wiederzufinden, warten Sie noch mit dem Beantragen einer neuen Karte. So sparen Sie sich die Gebühren, müssen allerdings solange ohne Karte auskommen.

Was tun, wenn ich die Karte im Ausland verloren habe?

Wenn Sie Ihre Girocard im Ausland verloren haben oder sie Ihnen gestohlen wurde, sollten Sie ebenfalls schnell handeln. Sie können Ihre Bank anrufen, sofern Sie die Sperrnummer des Finanzinstituts parat haben. Schneller geht es womöglich mit einem Anruf an folgenden **Sperr-Notruf** samt Vorwahl für Deutschland: **+49 116 116 (gebührenpflichtig aus dem Ausland)**

Um im Ausland eine neue Karte zu bekommen, bieten einige Banken einen **Expressversand der EC-Karte** innerhalb von 48 Stunden an. Doch das kann sehr teuer werden – und ergibt womöglich nur Sinn, wenn Sie noch länger im Ausland bleiben möchten.

Günstiger ist es in der Regel, wenn Sie sich Bargeld von einer Person aus Deutschland schicken lassen. Anbieter von **Bargeldtransfers** sind etwa **Western Union** oder **Moneygram**. Vor Ort müssen Sie das Bargeld in einer Filiale des Anbieters abholen und sich dabei ausweisen.

Wer haftet für die Schäden einer verlorenen Karte?

Bis die Karte gesperrt ist, haften Sie **mit bis zu 50 Euro**. Ob Sie über diesen Betrag hinaus haften, kommt darauf an, ob Sie beim Verlust **grob fahrlässig** gehandelt haben.

Das könnte der Fall sein, wenn Sie die PIN auf einem Zettel im Portemonnaie notiert haben und dieses Ihnen samt EC-Karte gestohlen wurde. Wenn Sie Ihre Karte sperren lassen, werden Sie daher oft dazu befragt. Generell liegt die Beweislast bei Ihnen.

Tipp: Bewahren Sie die PIN nie in der Nähe der EC-Karte auf. Die Wahrscheinlichkeit, dass der Finder der Karte die PIN nach drei Versuchen errät, ist sehr gering. Nach diesen Versuchen wird die Karte automatisch gesperrt. Machen Sie es dem neuen Besitzer also nicht zu leicht!

Quelle: https://www.t-online.de/finanzen/geld-vorsorge/sparen-finanzieren/id_45994980/ec-karte-verloren-so-sperren-sie-ihre-girocard.html

14) WLAN perfekt ausrichten: Smartphone-App erstellt Heatmap-Radar-Karte für jeden Raum

Schnelles Internet will doch jeder haben, am besten in jedem Winkel der eignen Wohnung. Mit der Gratis-App WiFiman messen Sie das problemlos aus und sehen die Schwachstellen auf einer Heatmap.

Wenn Sie noch keine haben, dann sollten Sie sich unbedingt eine WLAN-App holen. Keine Sorge, die Dinger sind gratis, AVM hat zum Beispiel eine gute Auswahl für FritzBox-Nutzer am Start. Doch Abseits davon gibt es auch coole Alternativen, etwa WiFiman.

Die Gratis-App bündelt wichtige Funktionen unter einer Haube, etwa Speedtest, Übersichten über WLAN-Details, Nachbar-WLANs und angemeldete Geräte kombiniert mit einer coolen Heatmap zur Signalabdeckung. Vor allem Android-Nutzer sollten die App unbedingt ausprobieren. Die iOS-Version kann noch nicht so viel.

Heatmap für Signalstärke und Latenz

Ein Hingucker ist die Heatmap-Funktion in der Android-Version, mit der Sie Signalstärke und Latenz anzeigen lassen können. Sie finden die Funktion im Bereich "Status" unter "Signal Mapper". Schalten Sie den AR-Modus ein und wandern Sie damit durch Ihre Wohnung. Sie können damit die Werte live und schön eingefärbt verfolgen. So sollten Sie auf jeden Fall Ecken ausmachen können, die noch nicht optimal mit WLAN versorgt sind.

Für die Durchsatzanzeige ist spezielle Hardware nötig, angegeben ist dafür eine UniFi Dream

Machine Pro, die für den Unternehmenseinsatz gedacht ist. Unter Android sollte aber der Rest auch mit beliebigem Equipment funktionieren. Zum Beispiel können Sie Standortinfos eintippen und so ganz einfach Vergleichsmessungen mit unterschiedlichen Router- oder Repeater-Standorten machen. Dieses kurze Video zeigt das ganz anschaulich.

Speedtest machen und Nachbar-WLANs prüfen

Vor allem die Android-Version von WiFiman ist ein Tausendsassa: Ein Speedtest ist integriert, den Sie durch einen einfachen Fingertipp starten können. Praktisch auch, Sie können die Geschwindigkeit zwischen zwei Geräten messen. Dazu installieren Sie WiFiman einfach auf einem zweiten Smartphone.

Gut gelungen ist auch die WLAN-Übersicht: Dort erkennen Sie Nachbar-WLANs und die App stellt auch übersichtlich die belegten Kanäle dar. So können Sie sehen, wenn zu viel Gedrängel in einem bestimmten Funkbereich herrscht.

iPhone-Version eingeschränkt

Beachten Sie, dass die iOS-Version den Signal-Mapper gar nicht anbietet, wenn nicht die passende Hardware im Netzwerk steckt. Auch die Kanalbelegung lässt sich auf einem iPhone nicht darstellen. Hier gibt es nur Speedtest, Infos zum eigenen WLAN und eine Liste mit verbundenen Geräten. Das geht schon in Ordnung, mit der üppigen Ausstattung der Android-Version kann die iPhone-App aber nicht mithalten.

Anmerkung der Redadktion: Die o.g. App kann unter dem u.g. Link downgeloaded werden.

Quelle: https://www.chip.de/news/WLAN-perfekt-ausrichten-Smartphone-App-erstellt-Heatmap-Radar-Karte-fuer-jeden-Raum_184103324.html?utm_source=nl_chipn-wy&utm_medium=chip-newsletter&utm_campaign=19-10-2022%2B08%253A00%253A03&utm_content=nl_chipn-wy&utm_term=

15) Fakeshop-Finder: Verbraucherschutzministerium fördert Projekt zum sicheren Online-Shopping

Mit einer Förderung des Landes in Höhe von rund 250.000 Euro hat die Verbraucherzentrale NRW ein neues Tool zur Überprüfung von Online-Shops entwickelt.

Mit einer Förderung des Landes in Höhe von rund 250.000 Euro hat die Verbraucherzentrale NRW ein neues Tool zur Überprüfung von Online-Shops entwickelt. Verbraucherinnen und Verbraucher können mit dem kostenlosen „Fakeshop-Finder“ Online-Shops vor der Bestellung auf Echtheit kontrollieren: Einfach die Internet-Adresse unter www.fakeshop-finder.nrw eingeben und das Tool prüft, ob der Online-Shop typische Merkmale eines unseriösen Anbieters aufweist. Im Ergebnis erhalten die Nutzenden binnen weniger Sekunden eine Einschätzung als Ampel: Rot bei einer eindeutigen Warnung, Gelb als Hinweis, vor der Bestellung genauer hinzusehen, und Grün, wenn alles in Ordnung ist.

Silke Gorißen, Ministerin für Landwirtschaft und Verbraucherschutz: „Gut und sicher im Internet einkaufen, klappt jetzt noch leichter dank neuem Fakeshop-Finder! Das bundesweit neue Selbsthilfe-Tool bringt alles mit, um rasch zum festen Begleiter beim sorgenfreien Online-Shopping zu werden. Mit wenigen Klicks können Verbraucherinnen und Verbraucher schnell und kostenlos herausfinden, ob ein Online-Shop seriös ist. Der Fakeshop-Finder der Verbraucherzentrale NRW kann entscheidend dazu beitragen, dass es beim Einkauf im Internet keine bösen Überraschungen gibt. Das fördern wir gerne.“

Wolfgang Schuldzinski, Vorstand der Verbraucherzentrale NRW: „Fakeshops sind eines der großen, dauerhaften Probleme im Verbraucheralltag und die Zahl der Beschwerden steigt stetig

an. Im Jahr 2020 wurden in den Verbraucherzentralen rund 1.000 Verbraucherbeschwerden über Fakeshops erfasst, in 2021 hat sich die Zahl auf knapp 3.000 verdreifacht. Mit dem Fakeshop-Finder bieten wir eine schnelle Orientierung beim Online-Einkauf, damit künftig weniger Menschen in die Falle unseriöser Anbieter tappen."

Mit ausgefeilten Algorithmen sucht der Fakeshop-Finder ständig gezielt nach Fakeshops im Internet. Rückgrat des Fakeshop-Finders bildet eine wachsende Domänendatenbank. Geben Verbraucherinnen und Verbraucher eine Adresse ein, die noch nicht in der Datenbank vorhanden ist, sucht er die eingegebene Adresse auf und scannt die Seite nach Merkmalen, die sehr oft bei unseriösen Shops zu finden sind. Das können ein fehlendes Impressum sein, eine Umsatzsteuer-ID, die es gar nicht gibt, aber auch technische, linguistische und strukturelle Merkmale, die aus Kundensicht nicht direkt zu erkennen sind. Auch öffentliche Listen von bekannten falschen Shops kennt der Fakeshop-Finder. Aus diesen Kriterien errechnet die Anwendung die Wahrscheinlichkeit, ob es sich bei der eingegebenen Adresse um einen unseriösen Anbieter handelt.

Der Fakeshop-Finder ist ein Projekt der Verbraucherzentrale NRW. Das Ministerium für Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen fördert das Projekt im Jahr 2022 mit 249.467 Euro.

Hintergrund

Hinter Online-Shops mit besonders günstigen Preisen verbergen sich nicht selten Fakeshops. Die angebotenen Produkte werden in der Regel gar nicht ausgeliefert, Kreditkarten mehrfach belastet oder die eingegebenen persönlichen Daten missbräuchlich genutzt. Betrügerische Shops sind oft so programmiert, dass sie sich kaum von realen Online-Angeboten unterscheiden. Außerdem erfolgt die Erstellung von Fakeshops mittlerweile nahezu vollständig automatisiert. Oft sind solche Adressen nur wenige Wochen im Netz, bevor sie durch neue ersetzt werden. Fakeshop-Listen im Internet veralten daher leider schnell. Das alles sorgt dafür, dass Verbraucherinnen und Verbraucher immer wieder irrtümlicherweise bei neuen Fakeshops im Internet einkaufen.

Links

- www.fakeshop-finder.nrw
- Weitere Informationen und nützliche Tipps zu Fakeshops finden Sie unter hier.

Anmerkung der Redaktion: Unter der o.g. Adresse www.fakeshop-finder.nrw besteht die Möglichkeit vor einem Internetkauf den Anbieter auf Seriosität hin zu überprüfen. Einfach mal ausprobieren und gegebenenfalls als Lesezeichen abspreichern.

16) Das passiert, wenn dein Handy-Ladegerät in der Steckdose bleibt

Wer den Smartphone-Akku richtig laden will, sollte auf ein ungewöhnliches Detail achten. Dazu gehört nämlich auch, was danach mit Ladekabel und Stecker geschieht.

Viele begehen einen unscheinbaren Fehler nach der Stromversorgung des Mobiltelefons. Sie ziehen zwar das Gerät vom Stecker, aber das **Handy-Ladekabel** bleibt in der Steckdose. Genau diese Angewohnheit kann am Ende Folgen haben. Um den Akku richtig zu laden, achte auf Folgendes.

Handy-Ladekabel: Darum sollte es nie in der Steckdose bleiben

Gleich zwei mögliche Konsequenzen drohen, wenn das Handy-Ladekabel regelmäßig in der

Steckdose verbleibt. Vor allem in Zeiten der Energiekrise kann es hilfreich sein, darauf zu achten. Selbst wenn es sich dabei nur um ein kleines Gerät mit überschaubarem Verbrauch handelt. Dazu kommen Sicherheitsaspekte, aus denen du am besten den Stecker ziehen solltest.

#1 Kostenfalle Ladegerät

So einfach es klingt, aber es kann dich in erster Linie Geld kosten, dein Ladekabel in der Steckdose zu lassen. Das liegt daran, dass weiter Strom transformiert wird, wenn kein Handy angeschlossen ist. Es entstehen dir also permanent Stromkosten, solange du das Gerät nicht vom Netz trennst.

Um deinen Handy-Akku richtig zu laden, ohne unnötigen Geld zu verbrennen, ist dies die einfachste Methode. Das gilt insbesondere, wenn du nicht nur ein Ladegerät verwendest, sondern mehrere Ladekabel in der Steckdose verbleiben.

Willst du herausfinden, ob dein Ladegerät auch ohne dein Handy Strom frisst, kannst du einen einfachen Test machen. Ist der Stecker warm, fließt auch Strom. Bei Geräten mit höherer Leistung kannst du zusätzlich ein elektrisches Summen hören.

Natürlich kommen dabei keine enormen Beträge zusammen, mehrere Kilowattstunden schafft ein Ladekabel, das du in der Steckdose gelassen hast, aber dennoch. Geht das Gerät am Ende vielleicht noch durch Überladung kaputt, musst du zusätzliches Geld für ein neues ausgeben. Es lohnt sich demnach doppelt, deinen Handy-Akku richtig zu laden.

#2 Brandgefahr durch Ladekabel

Tatsächlich kann es unter bestimmten Umstände aber auch gefährlich werden, das Ladekabel in der Steckdose zu lassen. Das gilt, wenn das Gerät einen Defekt hat und nicht mehr reibungslos funktioniert. Da ein solcher Fehler nicht immer sofort zu erkennen ist, kann es also passieren, dass dein Ladegerät überhitzt und Brandgefahr besteht.

Vor allem billige No-Name-Produkte können hier zur Gefahrenquelle werden. Um deinen Akku richtig zu laden, solltest du also nicht nur auf die Ladegeräte deines Handyherstellers zurückgreifen, sondern auch nie übermäßig lange dein Ladekabel in der Steckdose lassen.

Fazit: Ein kleines Detail mit großer Wirkung

Ja, es kann gefährlich, aber auch teuer werden, dein Ladekabel in der Steckdose zu lassen. Willst du deinen Handy-Akku richtig laden, gehört es also auch dazu, auf solche Details zu achten.

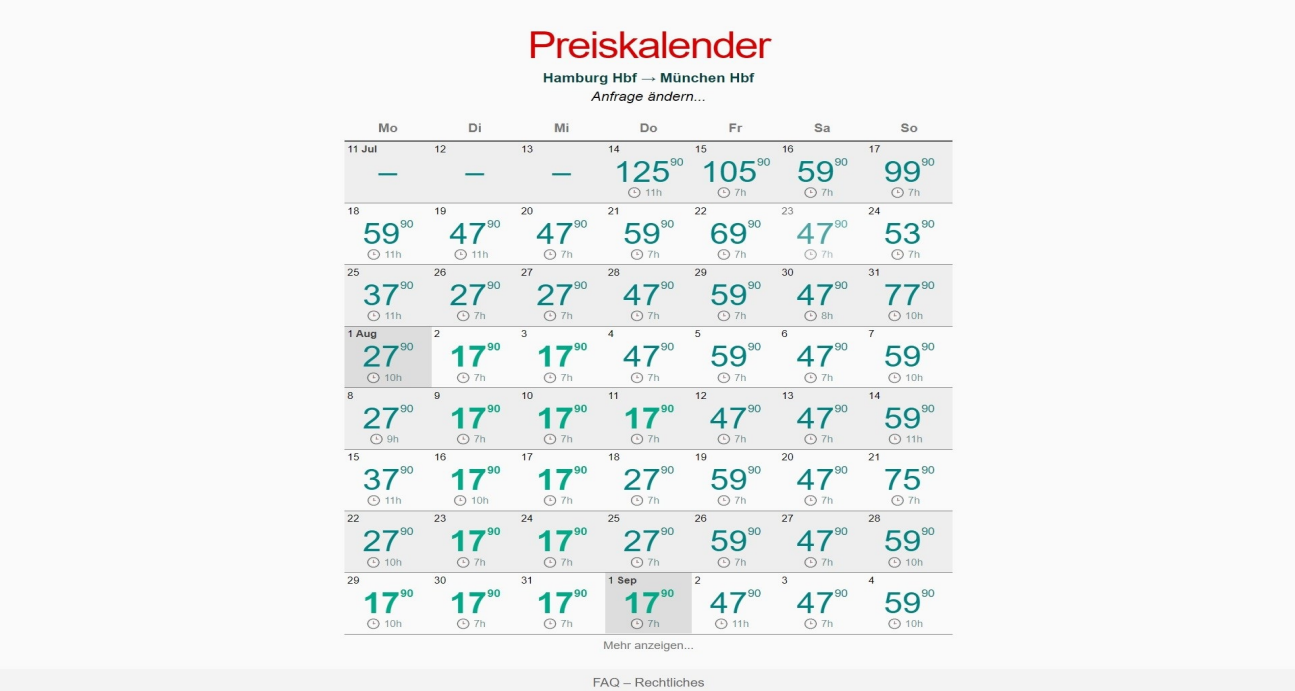
Quelle: https://www.futurezone.de/digital-life/article396455/das-passiert-wenn-dein-handy-ladegeraet-in-der-steckdose-bleibt.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

17) Bahn-Guru Preiskalender

Informationen zu Bahn-Guru Preiskalender

Der kostenlose „Bahn-Guru Preiskalender“ präsentiert Ihnen die günstigsten Zugticketpreise der Deutschen Bahn in einem übersichtlichen Kalender. Bahnreisende müssen lediglich den Startbahnhof und den Zielbahnhof in die Gratis-Web-App eingeben und erhalten direkt eine Preisauskunft als Monatsansicht. So bekommen Sie schnell einen Überblick, an welchem Tag Sie besonders preiswert mit der Bahn reisen und wie lang die Fahrzeit beträgt. Wenn Sie auf einen Termin klicken, zeigt Ihnen der „Bahn-Guru Preiskalender“ eine detaillierte Übersicht aller an dem Tag fahrenden Züge, die die gewählte Bahnverbindung bedienen. Der Preiskalender verlinkt außerdem weiter zur Reiseauskunft der Deutschen Bahn, wo Sie das Ticket schließlich

buchen können. Als Web-App ist der „Bahn-Guru Preiskalender“ mit jedem Internetbrowser nutzbar, etwa am Computer, Handy oder Tablet. Der Hersteller weist darauf hin, dass alle Preisdaten unverbindlich sind und bittet darum, die Suchergebnisse über die Webseite der Deutschen Bahn vorsorglich zu überprüfen.



Quelle: https://www.computerbild.de/download/Bahn-Guru-Preiskalender-33071731.html

18) How-To – So prüfen Sie, ob Ihre Mailadresse missbraucht wird und so schützen Sie sich

So überprüfen Sie sofort, ob Ihre Mailadresse im Internet geleakt wurde. So reagieren Sie richtig, wenn Sie betroffen sind.

Mit diesen kostenlosen Online-Tools überprüfen Sie sofort, ob Ihre Mailadresse im Internet geleakt wurde und in Zusammenhang mit gestohlenen Daten auftaucht.

haveibeenpwned von Troy Hunt

Sie können auf haveibeenpwned von dem Betreiber Troy Hunt Ihre Mailadresse daraufhin überprüfen lassen, ob diese im Internet in Zusammenhang mit geleakten Daten auftaucht. Die Seite zeigt Ihnen das Ergebnis der Überprüfung sofort an.

Das Ergebnis gibt Tipps dazu, wie Sie die Sicherheit des betroffenen Mailkontos verbessern und erklärt, in welchen Breaches Ihr Mailpasswort entdeckt wurde. Die Seite bietet zudem die Möglichkeit auch Telefonnummern daraufhin zu überprüfen, ob diese in Breaches vorkommen. Außerdem können Sie auch nach gestohlenen Passwörtern suchen lassen. Sie können sich auch automatisch benachrichtigen lassen, wenn Ihre bei haveibeenpwned hinterlegte Mailadresse in einem Breach auftaucht.

Wichtig: Selbst wenn Ihre Mailadresse in keinem Datenleak vorkommt, bedeutet das nicht, dass sie nicht bereits gehackt wurde oder nicht leicht zu hacken ist – zum Beispiel wegen eines schwachen Passwortes. Andererseits bedeutet es nicht zwangsläufig, dass Ihre Mailadresse

bereits konkret missbraucht wird, wenn diese in einem Breach enthalten ist.

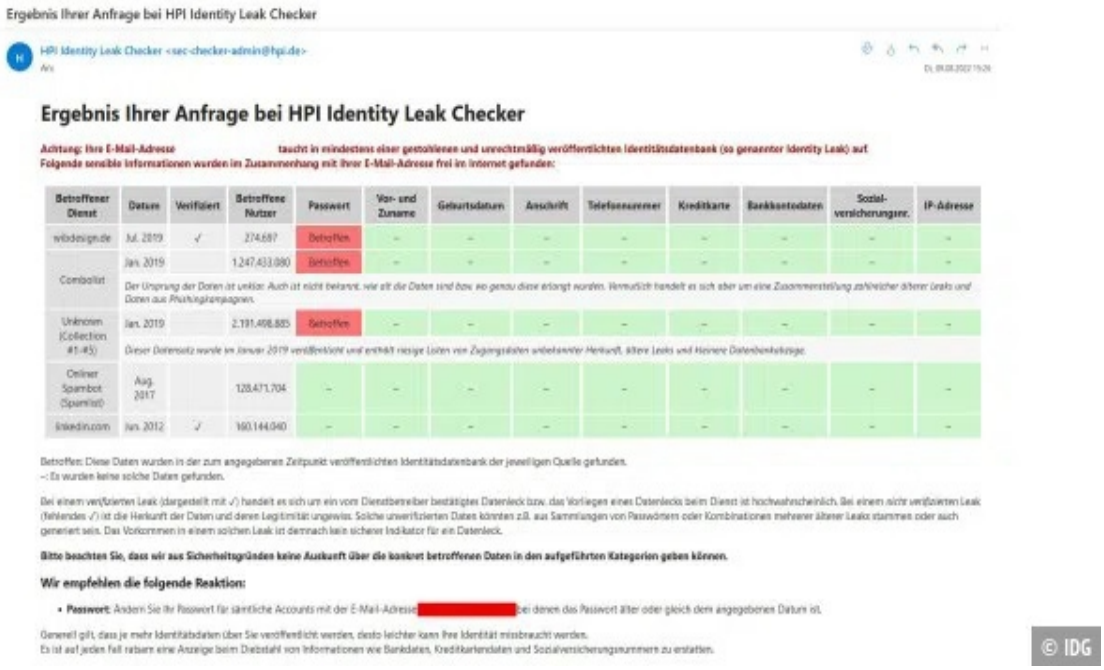
Tipp: So vermeiden Sie Mail-Stalking und schützen Ihre Privatsphäre

Es ist zwar theoretisch richtig, dass haveibeenpwned unter Umständen dazu missbraucht werden kann, um herauszufinden, bei welchen Clouddiensten sich andere Personen mit ihrer Mailadresse registriert haben. Allerdings handeln Anwender, die sich bei potenziell verfänglichen Online-Diensten wie beispielsweise Porno-Portalen oder Online-Sexkontakte-Plattformen mit ihrer beruflichen oder hauptsächlich genutzten und allgemein bekannten Mailadresse anmelden, extrem leichtsinnig. Für solche Zwecke sollte man sich eine zusätzliche, gut getarnte Mailadresse zulegen, aus deren Bezeichnung nicht auf die eigene Identität geschlossen werden kann. Beispielweise mit Outlook.com: Gratis-Mail-Konto mit Outlook.com einrichten – so geht's .

Und schon können Sie Ihre Bekannten, Freude oder Kollegen nicht mehr über haveibeenpwned stalken. Übrigens: Firefox Monitor nutzt ebenfalls haveibeenpwned.

HPI Identity Leak Checker des Hasso-Plattner-Instituts für Digital Engineering gGmbH

Der HPI Identity Leak Checker ist ein weiteres kostenloses Online-Tool, mit dem Sie Ihre Mailadresse daraufhin überprüfen lassen können, ob diese in Breaches auftauchen. Hier wird das Ergebnis der Überprüfung aber nicht direkt auf der Webseite von HPI Identity Leak Checker angezeigt, sondern stattdessen schickt der HPI Identity Leak Checker eine Mail mit dem Überprüfungsergebnis an die überprüfte Mailadresse, siehe Screenshot:



So sieht die Mail aus, die HPI Identity Leak Checker an das überprüfte Mailkonto schickt.

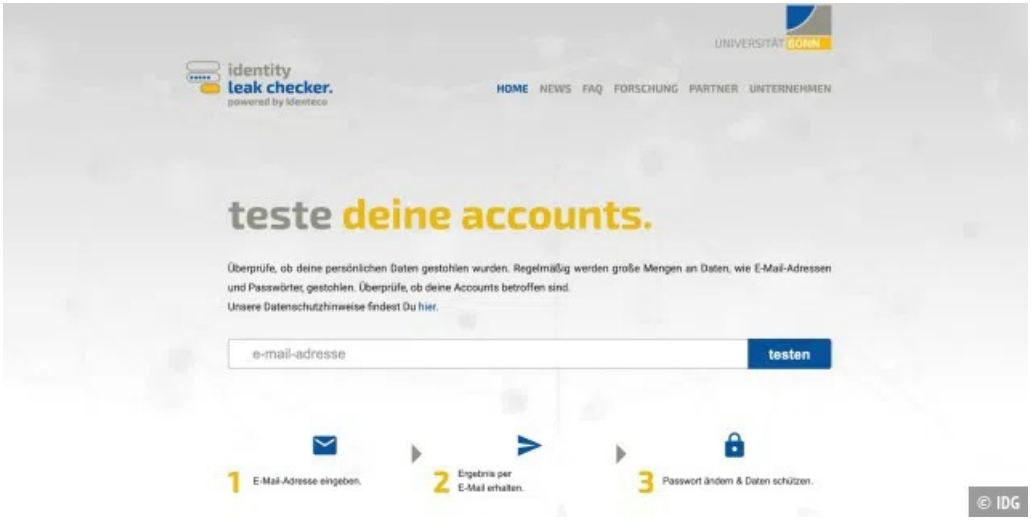
Somit ist über den HPI Identity Leak Checker kein Stalking wie bei haveibeenpwned möglich.

Betreiber ist hier das Hasso-Plattner-Institut (HPI) der Universität Potsdam. In der FAQ erfahren Sie Details zur Funktionsweise. Wichtig: "Der Identity Leak Checker gibt lediglich Auskunft dazu, ob Ihr Kennwort in einem Leak gefunden wurde. Der Leak Checker sagt nichts darüber

aus, ob dieses Kennwort für das betroffene Benutzerkonto noch funktioniert. Da Ihr Kennwort weiterhin in dem entsprechenden Leak zu finden ist, gibt die Webseite weiterhin eine Warnung aus."

Identity Leak Checker der Universität Bonn

Die Universität Bonn bietet ebenfalls einen Leak-Checker an. Er funktioniert genauso wie der des HPI: Sie geben die zu überprüfende Mailadresse ein und die Auswertung erhalten Sie dann an die eingegebene Mailadresse. Das verhindert also ebenfalls Stalking- beziehungsweise Ausspähversuche, wie es theoretisch bei haveibeenpwned möglich ist.



Der Leakchecker der Universität Bonn.

Der Bonner Leak-Checker entstand aus dem mit Bundesmitteln geförderten Projekt EIDI .

So reagieren Sie richtig

Falls Ihnen die oben genannten Tools anzeigen, dass Ihre Mailadresse in Datenleaks/Breaches auftaucht, dann sollten Sie sofort das Passwort dazu ändern. Haben Sie das gleiche Passwort, das Sie für Ihr Mailkonto verwenden, auch bei anderen Diensten verwendet, so sollten Sie dieses Passwort auch dort ändern.

Experten: So finden Sie ein wirklich sicheres Passwort

Ganz wichtig: Installieren Sie die Zweifaktor-Authentifizierung, sofern diese für Ihr Mailkonto unterstützt wird.

Gegebenenfalls nutzen Sie einen Passwortmanager wie Lastpass, um ein möglichst sicheres Passwort erstellen und speichern zu lassen.

Woher stammen die gestohlenen Mailadressen?

Die meisten geklauten Mailadressen stammen aus Angriffen auf Unternehmensserver, auf denen Dienste laufen, bei denen Sie sich mit Ihrer Mailadresse registriert haben. Beispielsweise stahlen Cybergangster die Daten von mehreren Hunderttausend Kunden des hessischen Energieversorgers Entega, wie im Juli 2022 bekannt wurde. Diese Datenschätze werden von den Dieben dann in Internetforen beziehungsweise im Darknet zum Kauf angeboten. Weitere große Datendiebstähle auf Unternehmensebene waren zum Beispiel:

Facebook-Daten gestohlen: Hier sehen Sie, ob Sie betroffen sind

Ein schon länger zurückliegender, aber damals sehr spektakulärer Datendiebstahl: Im Jahr

2011 stahlen Cybergangster die Daten von rund 160 Millionen Sony-Kunden.

Gegen solche Datenleaks, die durch das Stehlen von Serverdaten verursacht werden, sind Sie machtlos, diese können Sie nicht verhindern.

Quelle: https://www.pcwelt.de/article/1206465/so-pruefen-sie-ob-ihre-mailadresse-missbraucht-wird-und-so-schuetzen-sie-sich.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20So%20pr%C3%BCfen%20Sie%2C%20ob%20Ihre%20Mailadresse%20missbraucht%20wird%20und%20so%20sch%C3%BCtzen%20Sie%20sich&utm_campaign=Security&utm_term=PC-WELT%20Newsletters&utm_date=20221026132830&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

19) Nutzerkonten in Gefahr – Hunderte Smartphone-Apps mit Malware verseucht

Facebook warnt vor Hunderten potentiell gefährlicher Smartphone-Apps. Diese sind mit Schadsoftware verseucht, die private Nutzerkonten kompromittieren können.

Der Facebook-Mutterkonzern Meta warnt auf seinem Blog vor mit Schadsoftware verseuchten Apps. Sicherheitsforscher des Unternehmens hätten Hunderte Anwendungen entdeckt, die darauf ausgerichtet seien, private Kontoinformationen abzugreifen und Nutzerkonten zu kompromittieren.

Bei den über 400 Apps, unter denen sich lediglich 47 iPhone-Anwendungen befinden, handelt es sich zum Großteil um Software zur Bildbearbeitung oder Taskmanager, die das Arbeiten erleichtern oder dabei helfen sollen, das Handy aufzuräumen.

Beim ersten Start der jeweiligen Anwendung erbittet diese weitreichenden Zugriff auf das Smartphone – erteilen Nutzer diesen, beginnt die versteckte Malware damit, Accountinformationen zu stehlen und sich unrechtmäßig in betroffene Nutzerkonten einzuloggen. Betroffen hiervon seien vor allem Login-Daten für Metas eigenes soziales Netzwerk Facebook.

Liste der schädlichen Apps

iOS-Apps:

- Ad Optimization Meta
- Ads & Business Suite
- Ads & Pages
- Ads Analytics
- Ads Business Advance
- Ads Business Knowledge
- Ads Business Manager
- Ads Business Suite
- Ads Manager Suite
- Adverts Ai Optimize
- Adverts Bussiness Suite
- Adverts Manager
- Business & Ads
- Business Ads
- Business Ads Clock
- Business ADS Manager
- Business Adverts Manager
- Business Manager Overview
- Business Manager Pages (iOS App ID: 1597553589)

- Business Manager Pages (iOS App ID: 1635301567)
- Business Manager Pages (iOS App ID: 1636825108)
- Business Manager Suite
- Business Meta Pages
- Business Meta Support
- Business Suite
- Business Suite Ads (iOS App ID: 1613983385)
- Business Suite Ads (iOS App ID: 1626632781)
- Business Suite Manager
- Business Suite Managers
- Business Suite Optimize
- Fb Ads
- FB Ads Cost
- FB Advertising Optimization
- FB Adverts Community
- FB Adverts Optimization
- FB Analytic
- FB Business Support
- FB Pages Manager
- Meta Adverts Manager
- Meta Business
- Meta Optimizer
- Page Suite Manager
- Page Suite Managers
- Pages Manager Suite (iOS App ID: 1623362126)
- Pages Manager Suite (iOS App ID: 1632606219)
- Pages Managers Suite
- Very Business Manager

Android-Apps:

In Metas offiziellem Beitrag findet sich unter der Überschrift "Threat Indicators" eine vollständige Liste der betroffenen Android-Apps. Da es sich um mehrere Hundert Anwendungen handelt, haben wir auf eine vollständige Aufzählung in diesem Artikel verzichtet.

- Trojaner-Gefahr: Vorsicht vor diesem Android-Trojaner
- Über drei Millionen Downloads: Gefährliche Malware in Apps entdeckt
- Android-Nutzer aufgepasst: Diese Apps sind mit Malware verseucht

Was sollten betroffene Nutzer tun?

Falls Sie eine der betroffenen Apps auf dem Smartphone installiert und dort Anmeldeinformationen oder persönliche Daten hinterlegt haben, sollten Sie wie folgt vorgehen:

- Die entsprechende App sofort vom Telefon löschen.
- Passwörter der hinterlegten Nutzerkonten erneuern.
- Sollte das Passwort auch bei anderen Webseiten verwendet worden sein: Ebenfalls ein neues Passwort vergeben (Empfehlung: Kein Passwort auf mehreren Webseiten gleichzeitig benutzen).

Quelle: https://www.t-online.de/digital/handy/id_100063868/ios-und-android-hunderte-smartphone-apps-mit-schadsoftware-verseucht.html

20) Neue Funktion: Pandemieradar – Corona-Warn-App: Aktuelle Version 2.28 veröffentlicht

Für die Corona-Warn-App ist ein neues Update veröffentlicht worden. Dieses bringt mit dem "Pandemieradar" eine brandneue Funktion mit sich.

Für die offizielle Corona-Warn-App (CWA) des Bundes ist ein neues Update veröffentlicht worden. Das Projektteam rund um das Robert Koch-Institut, die Deutsche Telekom und SAP hat die neue Version mit der Nummer 2.28 veröffentlicht.

Wie auf dem offiziellen Blog der CWA berichtet wird, bringt die aktuelle Version neben einigen Verbesserungen auch eine neue Funktion mit, der "Pandemieradar".

Darüber hinaus wird jetzt auch in der Detail-Ansicht zum Impfstatus ein kurzer Text eingeblendet, der Aufschluss über den Impfstatus für Kinder unter 12 Jahren gibt (beruhend auf Informationen aus dem aktuellen Infektionsschutzgesetz).

Das steckt hinter dem "Pandemieradar"

Über die neue Kachel des "Pandemieradar" werden Nutzer der Corona-Warn-App auf eine Internetseite des Robert Koch-Instituts weitergeleitet. Auf dieser finden sich viele Informationen und Statistiken sowie alle relevanten Kennzahlen zur Corona-Pandemie. Aus diesem Grunde wurde die Kachel in der App auch entsprechend prominent platziert.

Unter anderem befinden sich in der Übersicht neben der 7-Tage-Inzidenz auch die Viruslast im Abwasser, die COVID-Auslastung der Intensivstationen oder die belegten Krankenhausbetten. Die dort vorliegenden Informationen werden laut CWA-Blog werktäglich aktualisiert.

Die Version 2.28 der Corona-Warn-App wird ab sofort schrittweise in den nächsten 48 Stunden an alle Anwender ausgerollt. iOS-Nutzer können über den App-Store bereits jetzt ein Update anstoßen, für Nutzer der Android-App gibt es diese Funktion nicht. Hier geschieht das Update der CWA innerhalb der nächsten 1 bis 2 Tage automatisch.

Quelle: https://www.t-online.de/digital/handy/id_100071360/corona-warn-app-aktuelle-version-2-28-veroeffentlicht.html

21) Passkey-Einführung – Paypal: Passwörter sollen abgeschafft werden

Der Zahlungsdienstleister Paypal will künftig anstelle des klassischen Log-ins via Passwort auf ein Passkey-Verfahren setzen. 2023 soll die Umstellung auch in Deutschland erfolgen.

Zahlungsdienstleister Paypal schraubt an der Nutzersicherheit: Wie das Unternehmen in einer Pressemitteilung bekannt gab, soll künftig statt Passwörtern ein sogenannter Passkey zum Einloggen in das jeweilige Nutzerkonto erforderlich sein. Damit verspricht Paypal eine „einfache und sichere Möglichkeit“, ohne sich lange Zahlen- und Buchstabenkombinationen als Log-in merken zu müssen.

Das Verfahren selbst basiert auf dem neuen Industriestandard, der vom World Wide Web-Konsortium und der FIDO Alliance entwickelt wurde. Die kryptografischen Schlüsselpaare seien „resistent gegen Phishing und wurden so konzipiert, dass keine Daten zwischen Plattformen ausgetauscht werden“.

In der Praxis können derzeit nur US-amerikanische iPhone-, iPad- und Mac-Nutzer auf die neue Methodik zugreifen. Für diese wird auf dem jeweiligen Apple-Gerät ein Passkey erstellt, wozu der User beim nächsten klassischen Log-in aufgefordert wird. Anschließend wird der erstellte

Schlüssel mit der iCloud-Keychain synchronisiert. Ist dies erfolgt, können sich Benutzer künftig wahlweise mit Touch ID oder Face ID authentifizieren.

Vorläufig nicht unterstützte Geräte – etwa das gesamte Android-Spektrum – bekommen beim Log-in auf der Paypal-Webseite zunächst einen QR-Code angezeigt, der mit dem entsprechenden Gerät zur Authentifizierung gescannt werden muss.

Der Support von Android-Geräten soll ebenso in naher Zukunft erfolgen wie auch die Ausweitung des Passkey-Verfahrens auf weitere Länder. In Deutschland wird der Start der Paypal-Passkey-Methode 2023 erwartet. Bis dahin gilt wie auch bei allen Log-in-Daten, ein möglichst sicheres Passwort zu erstellen – wie das geht, erfahren Sie im verlinkten Artikel bei den Kollegen von PC-Magazin.

Quelle: https://www.connect.de/news/paypal-passkey-start-login-ohne-passwort-3203045.html?utm_source=connect-NL&utm_medium=newsletter

22) News – Gute Nachricht für Samsung-Nutzer: Diese Geräte erhalten Android 13

Fast 50 Samsung-Geräte bekommen bis Februar 2023 ein Update auf Googles neues Betriebssystem Android 13.

Nach ausgiebigen Tests hat Samsung in dieser Woche das Update auf Android 13 sowie die neuste Version seiner Benutzeroberfläche One UI 5.0 für die drei Smartphones Galaxy S22, Galaxy S22+ und Galaxy S22 Ultra veröffentlicht. Weitere aktuelle Smartphone- und Tablet-Modelle von Samsung sollen im November 2022 folgen. Ältere Flaggschiffe und Mittelklasse-Galaxy-Hardware werden dann im Dezember 2022 mit dem Update bedacht. Im Januar und Februar 2023 wird die Firmware schließlich für weitere Galaxy-Tab- und Galaxy-A-Modelle veröffentlicht. Geräte, die in der Übersicht noch fehlen, sollen im ersten und zweiten Quartal 2023 folgen.

Android 13: Diese Smartphones erhalten das Update

One UI 5.0 beinhaltet unter anderem acht unterschiedliche Dynamic Themes, Hintergrundbilder für Anrufer, einen überarbeiteten Benachrichtigungsbereich, stapelbare Widgets, verbessertes Multitasking und eine neue Bedienoberfläche für die Kamera-App. In der folgenden Übersicht sehen Sie, ob auch Ihr Smartphone oder Tablet von Samsung das Update erhält:

October 2022:

- Galaxy S22
- Galaxy S22+
- Galaxy S22 Ultra
- November 2022:
- Galaxy Z Fold 4
- Galaxy Z Flip 4
- Galaxy Z Fold 3
- Galaxy Z Flip 3
- Galaxy S21
- Galaxy S21+
- Galaxy S21 Ultra
- Galaxy Note 20
- Galaxy S20
- Galaxy S20+

- Galaxy S20 Ultra
- Galaxy Tab S8
- Galaxy Tab S8+
- Galaxy Tab S8 Ultra
- Galaxy Tab S7
- Galaxy Tab S7+
- Galaxy Quantum 3
- Galaxy A53 5G
- Galaxy A33 5G

Dezember 2022:

- Galaxy Z Fold 2
- Galaxy Z Flip 5G
- Galaxy Z Flip
- Galaxy S20 FE
- Galaxy Tab S7 FE/S7 FE 5G
- Galaxy Tab S6 Lite
- Galaxy A Quantum
- Galaxy A Quantum 2
- Galaxy A52s 5G
- Galaxy A51
- Galaxy A51 5G
- Galaxy A42 5G
- Galaxy A32
- Galaxy Jump
- Galaxy Jump 2

Januar 2023:

- Galaxy Tab A8
- Galaxy Tab A7 Lite
- Galaxy Tab Active 3
- Galaxy Buddy 2
- Galaxy Wide 6
- Galaxy Wide 5
- Galaxy Buddy
- Galaxy A23
- Galaxy A13
- Galaxy M12
- Galaxy XCover 5

Februar 2023:

- Galaxy Tab Active 4 Pro

Quelle: https://www.pcwelt.de/article/1362354/gute-nachricht-fur-samsung-nutzer-diese-gerate-erhalten-android-13.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Gute%20Nachricht%20f%C3%BCr%20Samsung-Nutzer%3A%20Diese%20Ger%C3%A4te%20erhalten%20Android%2013&utm_campaign=Best-of%20PC-WELT&utm_term=PC-WELT%20Newsletters&utm_date=20221027102833&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

23) Tip – Amazon Prime Vorteile teilen – so geht’s

Amazon gibt Prime-Abonennten die Möglichkeit, ihre Vorteile zu teilen. Wir zeigen Ihnen, wie es geht und welchen Haken es gibt.

Als Prime-Mitglied genießen Sie bei Amazon einige Vorteile: Sie profitieren von kostenlosem und schnellerem Versand, erhalten exklusiven Zugang zu besonderen Angeboten wie an den sogenannten Prime Days und können etwa den Streaming-Dienst Amazon Prime Video nutzen.

Amazon Prime können Sie 30 Tage lang gratis nutzen. Der reguläre Preis für das Abo liegt entweder bei 8,99 Euro monatlich oder 89,99 Euro jährlich. Wer Prime-Abonnent ist, kann bestimmte seiner Vorteile teilen, ohne dass die andere Person dafür zahlen muss.

Wie Sie Ihre Prime-Vorteile teilen

Was Sie teilen können: Sie können Ihre Versandvorteile von Amazon teilen. Eine weitere Person kann demnach mit “Prime” gekennzeichnete Artikel kostenlos bestellen und vor allem schneller als regulär erhalten. Weitere Vorteile können Sie leider nicht teilen.

Der Haken: Sie können die -Prime-Versandvorteile nicht mit jeder Person teilen. Die Person muss laut Amazon zu Ihrem Haushalt gehören. Sie muss außerdem über ein Amazon-Konto verfügen.

Und So geht es:

1. Rufen Sie Ihre Prime-Mitgliedschaft im Browser Ihres Desktop-PCs auf und melden Sie sich gegebenenfalls an. Per Smartphone oder Tablet können Sie diese Seite nicht erreichen.
2. Scrollen Sie nach ganz unten und klicken Sie auf “Prime-Vorteile teilen”.
3. Geben Sie den Namen der einzuladenden Person an sowie die Mail-Adresse, mit der sie bei Amazon angemeldet ist.
4. Klicken Sie auf “Einladung verschicken”.

Die Person erhält nun eine Mail, in der Sie die Einladung annehmen muss und anschließend die Versandvorteile erhält. Sie können maximal eine Person hinzufügen. Falls Sie die Person austauschen möchten, rufen Sie erneut die Prime-Abo-Seite auf, scrollen Sie nach unten und klicken Sie bei der bestehenden Verknüpfung auf “Kündigen”. Laden Sie dann eine andere Person Ihres Haushaltes ein.

Quelle: https://www.pcwelt.de/article/1346664/amazon-prime-vorteile-teilen-so-gehts.html?tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4