42. Cybercrime Newsletter

26.06.2024

1) Cyberkriminalität – Hackerangriff auf Bank: Viele Anleger betroffen

Hacker haben einen Angriff auf eine Fondstochter der DZ-Bank verübt. Zehntausende Anleger könnten betroffen sein. Es geht um hochsensible Daten.

Eine Immobilientochter der DZ-Bank ist Opfer einer schweren Cyberattacke geworden. Mehrere Zehntausend Kunden der DG Immobilien Management (DGIM) seien betroffen, sagte eine Sprecherin der DZ-Bank in Frankfurt am Main. Die genaue Zahl der Betroffenen sei noch unklar. Betroffen sind hauptsächlich die Anleger von geschlossenen Immobilienfonds, darunter auch Kunden der Volks- und Raiffeisenbanken. Daten von Kunden der DZ-Bank seien nicht betroffen, sagte sie. Zuvor hatte die "Rheinische Post" darüber berichtet.

Hochsensible Kundendaten möglicherweise gestohlen

Die DZ-Bank und ihre Fondstochter hätten eine Task-Force gebildet. "Wir sind gerade dabei, das alles aufzuarbeiten", sagte die Sprecherin. Die DZ-Bank und ihre Fondstochter hätten die Polizei, die Staatsanwaltschaft und das Bundesamt für die Sicherheit in der Informationstechnik (BSI) eingeschaltet. Auch die zuständige Datenschutzaufsicht wurde informiert.

Zudem habe die DGIM ihre Kunden in einem Schreiben gewarnt, dass "personenbezogene Daten von Anlegern abgeflossen sein könnten". Die Rede ist von Zehntausenden von Anlegern bundesweit, die über die Volksbanken Produkte der DGIM erworben haben.

Laut Bericht könnten nicht nur Adressdaten, sondern auch Geburtsdaten, Anlagebeträge, Kontendaten, Steuernummern, Mitteilungen der Finanzämter und auch diverse Schriftwechsel sowie Nachweisdokumente abgeflossen sein. Die Fondstochter warnt demnach die betroffenen Anleger vor Betrugsversuchen mit diesen Daten.

Die Angreifer könnten mithilfe der Dokumente beispielsweise an die Zugangsdaten der Anleger gelangen. Denkbar ist auch, dass sich die Datendiebe gegenüber Dritten als Vertreter der Anleger ausgeben, um Geschäfte zu deren Nachteil abzuschließen, so die "Rheinische Post" weiter. Sollten Kunden verdächtige Mails und Briefe erhalten, sollten sie sofort ihre zuständige Bank oder die DGIM informieren.

Die DGIM gehört zum DZ-Bank-Konzern, der das Spitzeninstitut der Volks- und Raiffeisenbanken ist. Die Anleger haben laut Bericht über die Volks- und Raiffeisenbanken Produkte der DGIM erworben. Hacker haben einen Angriff auf eine Fondstochter der DZ-Bank verübt. Zehntausende Anleger könnten betroffen sein. Es geht um hochsensible Daten.

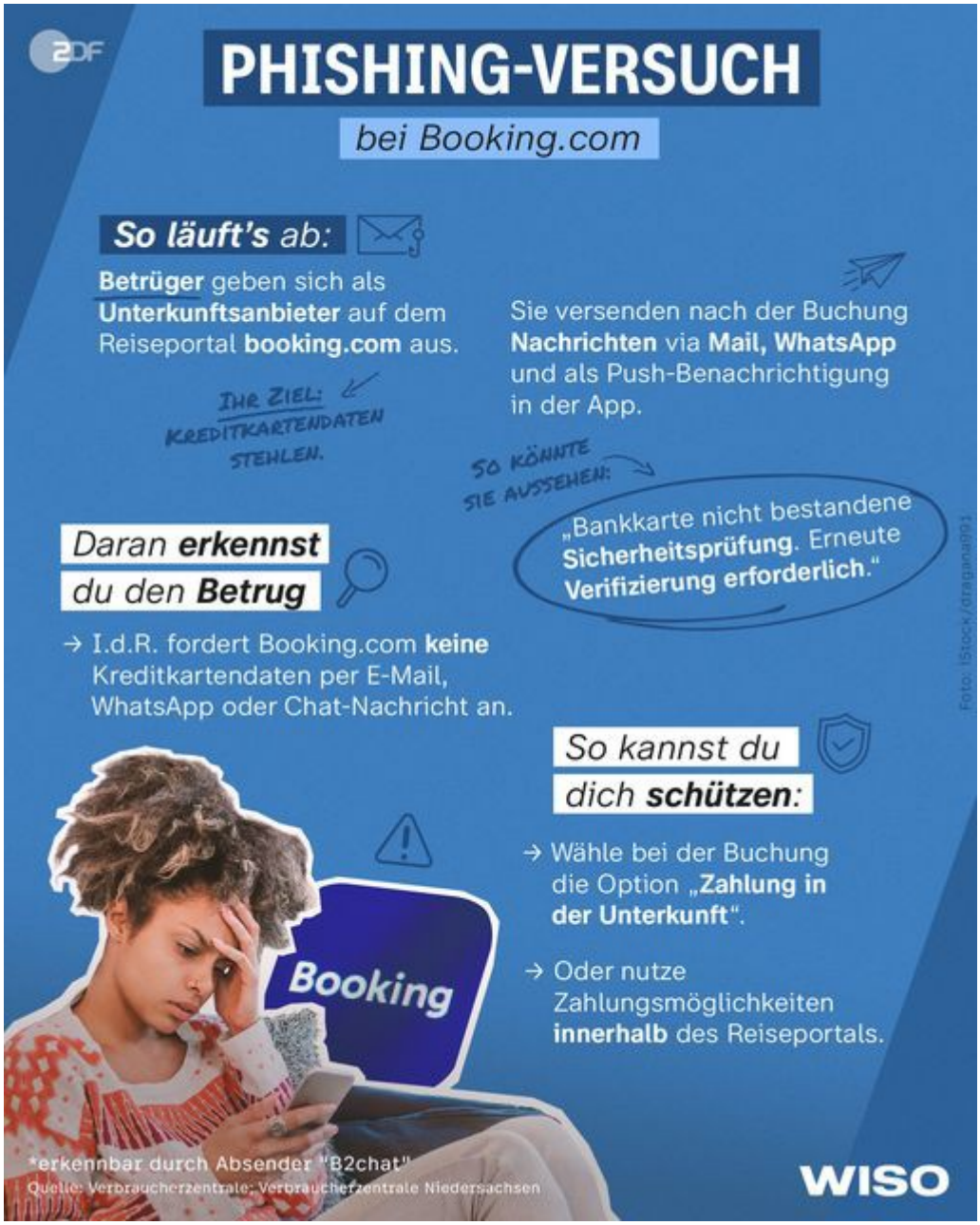
Quelle:https://www.t-online.de/digital/aktuelles/id_100432532/hacker-angriff-auf-tochter-der-dz-bank-kunden-daten-betroffen.html

2) Betrugsmasche mit booking.com – Ärger bei der Hotelbuchung vermeiden

Bei dieser Betrugsmasche kapern Hacker Hotel-Accounts und kontaktieren Hotelgäste, um an deren Geld zu kommen. Kümmert sich Booking.com ausreichend um die Sicherheit der Kunden?

Bitte über den unten genannten Link den Filmbeitrag anschauen, eine reine Textversion ist nicht vorhanden.

https://www.zdf.de/verbraucher/wiso/betrugsmasche-mit-booking-com-100.html



Quelle: ZDF WISO

Quelle: https://www.zdf.de/verbraucher/wiso/phishing-gestohlene-kontodaten-100.html?at_medium=Social%20Media&at_campaign=Facebook&at_specific=WISO

3) Panne bei beliebtem Broker – Ist Ihr Geld in sicheren Händen? Na hoffentlich

Die Geldanlage der Deutschen hat sich in den letzten Jahren deutlich verändert. Viele, insbesondere junge Anleger setzen auf Neo-Broker. Jetzt gibt es Ärger.

Als ich Mitte der 90er-Jahre mit aktivem Aktienhandel begann, war der Dreiklang aus teuren Ordergebühren, mittelgutem Service und ausschließlich telefonischer Erreichbarkeit normal. Die Sparkassen oder Volksbanken verdienten sich eine goldene Nase, aber immerhin konnte man bei Beschwerden persönlich in der Filiale vorstellig werden.

In der Brunnenstraße in Berlin-Mitte dürfte man bei Trade Republic wohl primär auf IT-Experten und Marketing-Menschen treffen, denn persönliche Kundenbetreuung ist bei dem Neo-Broker nicht vorgesehen. Kunden setzen sich also besser mit Laptop oder Smartphone in den nahe gelegenen Weinbergspark und adressieren ihre Probleme digital.

Kunden verärgert

Allerdings: Beim Alles-Digital-Modell ruckelte es zuletzt mehrfach. Das Versprechen der Marketingmaschine Trade Republic bedeutete bisher, dass man Kunden mit geringen Gebühren, hohen Zinsen und einfachem Handling der App glücklicher machen würde. Ein erstes Rauschen gab es, als 2023 die App einen Relaunch erfuhr und Kunden wenig erfreut waren – unter anderem litt nun die Übersichtlichkeit.

Dazu stellte man als aktiver Kunde an Handelstagen mit hohen Kursschwankungen – etwa am 14. Juni, als der Dax seinen schlechtesten Tag seit Monaten verzeichnete – fest, dass die Geschwindigkeit der App mitunter an ein 56k-Modem erinnert. Wer an solchen Tagen Hebelpapiere oder Aktien handeln möchte, trifft mitunter auf mangelhafte Ordergeschwindigkeit.

Auch die Vermarktung einer Debitkarte als Kreditkarte kam bei manchen Anlegern keinesfalls gut an, da es sich in gewisser Weise um Etikettenschwindel handelt. Wer schon einmal an einem Flughafen versucht hat, mit einer Debitkarte einen Mietwagen zu erhalten, weiß davon ein Lied zu singen. Lesen Sie hier mehr zu den Unterschieden von Debitkarte und Kreditkarte.

Verbesserungen dringend nötig

Obendrauf kommen nun Abrechnungsprobleme bei Dividenden und der Umgang mit den Beschwerden. Trade Republic verweist durch seinen Pressesprecher darauf, dass "wenige Dividenden nicht in Echtzeit, sondern, wie bei anderen Brokern üblich, erst wenige Bankarbeitstage nach dem Zahltag an den Kunden gebucht wurden". Im aktuellen Quartal habe dies unter anderem DWS und Porsche betroffen.

In zahlreichen Foren sieht man jedoch, dass nicht die verspätete Zahlung per se die Kunden verärgert hat, sondern primär eine mangelhafte Kommunikation des Brokers. Der äußerte und erklärte sich nämlich erst, als die Medien anfingen, über die Dividendenpanne zu berichten. Nicht wenige Kunden von Trade Republic könnten sich nun emanzipieren.

Die Konkurrenz holt auf

Unbestritten haben die Berliner, seit sie 2015 an den Start gingen, den Markt verändert. Die Haptik der App gehört zum Besten, was man am Markt finden kann. Daran arbeiten jedoch auch Konkurrenten wie Smartbroker, ebenfalls aus Berlin. Erfahrene Trader wissen zudem die Verlässlichkeit einer Consorsbank zu schätzen.

Auch hohe Zinsen für Neukunden gibt es auch bei der Konkurrenz, echte Kreditkarten haben einige Mitbewerber im Angebot und vor allem stimmt die Ausführungsqualität gerade bei Hebelprodukten an volatilen Handelstagen. Konkurrenten wie Smartbroker, Flatex oder Consorsbank bieten zudem bei Hebelpapieren alle Emittenten als Auswahlpartner an.

Vertrauen schlägt Marketing

Ohne Zweifel hat Trade Republic gerade bei jungen Leuten ein hervorragendes Marketing an den Tag gelegt. Am Ende geht es bei Geldanlage aber um Ertrag und Vertrauen. Genau an diesem Punkt können auch die jungen Kunden unangenehm werden. Ein scheinbar vertrautes und hippes per-Du in der Ansprache ist dann cool und frisch, wenn alles funktioniert.

Treten Probleme auf, möchte der Kunde dann doch den langweiligen Kundenbetreuer, der in klassischer Ansprache das Problem vom Tisch räumt. Überraschend sind Probleme bei schnell wachsenden, jungen Unternehmen keineswegs. Trade Republic wird seine Kunden-Kommunikation hoffentlich verbessern, denn für eine gute Aktienkultur sind Börsen und Broker unerlässlich – ganz egal ob in der Neo- oder der etablierten Variante.

Quelle: https://www.t-online.de/finanzen/die-anleger/id_100431160/panne-bei-broker-trade-republic-kunden-frustriert-ueber-service.html

4) Vorsicht bei Nachricht vom „Finanzamt“ - „Ignorieren und löschen Sie die SMS“

In gefälschten SMS geben sich Betrüger als das Finanzamt aus. Die Empfänger sollen Geld bezahlen. Die Polizei gibt jetzt wichtige Verhaltenstipps.

Hagen - Vermeintliche SMS vom Finanzamt wurden in Hagen verschickt. Betrüger haben inzwischen schon mehrfach versucht, von ihren Opfern mit den gefälschten Nachrichten Geld zu erbeuten. Wie sollte man handeln, wenn man eine solche SMS erhält?

„Ignorieren und löschen Sie die SMS“: Vorsicht bei Nachricht vom „Finanzamt“

Bei den Betrugsversuchen wurden die Empfänger der SMS aufgefordert, einen bestimmten Geldbetrag zu überweisen, teilt die Polizei Hagen mit. Die Nachricht beinhaltete zudem einen Link. Die Polizei und das Finanzamt warnen darüber hinaus vor ähnlichen Betrugsversuchen über verschiedene Kanäle wie E-Mail und Telefon, wie come-on.de berichtet.

Die gefälschten SMS können durch verschiedene Faktoren identifiziert werden. Zum einen teilt die Polizei Hagen mit, dass die Finanzverwaltung NRW niemals Zahlungsaufforderungen per SMS versenden würde. Die Zahlungsbescheide würden ausschließlich schriftlich versendet. Zum anderen könne die Uhrzeit der SMS einen Hinweis auf einen Betrug liefern. Viele Empfänger erhielten die gefälschte SMS in den Abendstunden, also erst nach Ende der Arbeitszeit des Finanzamtes. Ein weiteres Indiz für eine gefälschte SMS sei eine ausländische IBAN als Zielkonto, so die Hagener Polizei.

Betrugsmasche „Smishing“

Das sogenannte „Smishing“ ist eine Betrugsmasche, die immer häufiger von Betrügern angewendet wird. Hierbei benutzen die Kriminellen SMS-Nachrichten, um an Zugangsdaten von Online-Konten zu kommen oder, wie im aktuellen Fall in Hagen, die Empfänger zu einer Überweisung zu bewegen. Deshalb gibt die Polizei Verhaltens-Tipps für den richtigen Umgang mit gefälschten SMS:

- „Ignorieren und löschen Sie die SMS und folgen Sie in keinem Fall den Anweisungen der Textnachricht!“, so die Polizei.
- Links in der SMS sollten nicht angeklickt werden.
- Angegebene Telefonnummern in der SMS sollten nicht angerufen werden.
- Falls vorhanden: Benutzen Sie den Spam-Filter Ihres Smartphones.
- Empfänger von Betrugs-SMS sollten nicht auf diese antworten.
- Es empfiehlt sich, Updates auf dem Smartphone regelmäßig zu installieren und einen Virenschutz zu nutzen.
- Weiterhin rät die Polizei: „Sofern Sie Ihre Handynummer in ein öffentliches Telefonbuch eingetragen haben, lassen Sie diese entweder wieder löschen oder verzichten Sie auf die Angabe Ihres Vornamens.“
- SMS-Empfänger sollten eine Anzeige bei der Polizei erstatten.

Wie kann ich mich vor „Smishing“ schützen?

Hat man bereits eine Betrugs-SMS erhalten, kann man sich laut *Verbraucherzentrale* mit wenigen Schritten vor weiteren gefälschten SMS schützen. In den Einstellungen vieler Nachrichten-Apps können Betroffene festlegen, dass sie nur Nachrichten von Rufnummern erhalten wollen, die sie eingespeichert haben. Außerdem soll man die eigene Handynummer immer nur dann angeben, wenn es zwingend nötig ist, so die *Verbraucherzentrale*. Hilft beides nicht, sollten Betroffene über den Wechsel der Rufnummer nachdenken.

Quelle: https://www.hna.de/verbraucher/nrw-betrug-ignorieren-loeschen-sms-vorsicht-nachricht-finanzamt-hagen-93132829.html

5) Perfide Betrugsmasche auf Kleinanzeigen: Polizei warnt Käufer und Verkäufer eindringlich

Auf Verkaufsportalen wie Amazon und Kleinanzeigen lauern immer wieder Betrüger. Mit einer perfiden Masche werden gleich zwei Personen betrogen.

München – Auf der Suche nach einem neuen Smartphone, Möbeln oder anderen Haushaltsgegenständen landen Käufer oftmals auf Portalen wie Kleinanzeigen. Wird dort nicht aufgepasst, können Unwissende schnell um ihr Geld gebracht werden.

Dreiecksbetrug auf Kleinanzeigen: Polizei warnt Nutzer

Die Polizei warnt bereits seit längerem vor dem sogenannten Dreiecksbetrug. Beschrieben wird die Masche dort folgendermaßen: Ein Verkäufer A bietet sein Smartphone auf Kleinanzeigen oder ähnlichen Portalen an. Ein Interessent B bietet an, das Gerät über PayPal zu zahlen und danach die Ware zu bekommen. Zeitgleich inseriert der Interessent B das Smartphone aber ebenfalls und verkauft es an einen anderen Nutzer C. Dann gibt B als Zahlungsadresse den PayPal-Account von A an, wovon C nicht in Kenntnis gesetzt wird.

B möchte das Smartphone zudem nicht geschickt bekommen, sondern es von einem Freund abholen lassen. In der Folge erhält A das Geld von C und B bekommt das Smartphone von A durch besagten Freund. Kurz gesagt: B ist um ein Smartphone reicher, während A und C der Betrugsmasche zum Opfer gefallen sind. Der mit dem größten Nachteil ist in diesem Falle der ursprüngliche Verkäufer A, da er das Smartphone nicht mehr hat und das erhaltene Geld an C zurückschicken muss. A kann nicht einmal den Käuferschutz geltend machen, weil er das Gerät nicht verschickt, sondern es an der Haustür übergeben hat.

Verbraucherzentrale warnt vor teurer Betrugsmasche im Onlineshop

Die Verbraucherzentrale Niedersachsen warnte ebenfalls bereits vor der Dreiecksmasche. Dort heißt es, dass auch Käufer schnell Opfer dieser Betrugsmasche werden können. Wird ein Produkt auf eBay oder Kleinanzeigen von einem Privatverkäufer gekauft, kann dieses unwissentlich von einem Shop geschickt werden – doch wie ist das möglich? Der vermeintliche Verkäufer hat die Daten des Interessenten an den Shop weitergegeben.

Auffällig wird das erst, wenn der Shop eine Zahlungserinnerung an den Käufer schickt, obwohl dieser bereits auf dem Shopping-Portal überwiesen hat. „Hier handelt es sich ganz klar um Identitätsmissbrauch“, sagte Kathrin Bartsch von der Verbraucherzentrale Niedersachsen. „Mit der Bestellung über den Online-Shop gehen Betrüger einen perfiden Weg – schließlich könnten sie auch nur das Geld kassieren, ohne die Ware zu bestellen.“ Die Betrüger könnten sogar planen, das Paket abzufangen. Eine andere Betrugsmasche betrifft die ING.

Quelle: https://www.merkur.de/verbraucher/warnt-kaeufer-verkaeufer-betrugsmasche-amazon-kleinanzeigen-polizei-zr-93097976.html

6) Datenklau bei WhatsApp-Alternative: Ihr Konto könnte auch dabei sein

Der Messenger Telegram wurde durch Hacker angegriffen, die sensible Informationen von 361 Millionen Konten erbeuten konnten. Das sind rund 122 Gigabyte an vertraulichen Daten.

Der kostenlose Internet-Dienst Have I Been Pwned lässt Sie schnell prüfen, ob Ihre Konten von Leaks wie diesem betroffen sind. Durch Eingabe ihrer E-Mail-Adresse können Benutzer überprüfen, ob ihre Informationen bei diesem Datenleak ebenfalls kompromittiert wurden und im Internet durchgesickert sind. Dafür greift der Anbieter auf einen riesigen Datensatz bereits gehackter Konten zurück – insgesamt umfasst die Liste aktuell über 11 Milliarden Einträge.

Alternativ können Sie über Pwned Passwords diesen Datensatz nicht nur nach E-Mail-Adressen, sondern auch direkt nach Passwörtern durchsuchen. Damit lassen sich einige neue Erkenntnisse gewinnen, die Ihnen dabei helfen sollen, sicherer im Netz unterwegs zu sein. Wir erklären, wann und wie "Pwned Passwords" sinnvoll einzusetzen ist.

Cyber-Kriminelle nutzen oftmals die Brute-Force-Methode, um ein Passwort zu knacken. Dabei werden so lange Buchstaben-, Zahlen- oder Wörterkombinationen ausprobiert, bis das richtige Kennwort "erraten" wurde. Das kann allerdings sehr zeitaufwändig sein und führt eigentlich nur bei simplen Passwörtern zum Ziel. Deshalb kommen alternativ auch oft Wörterbuchlisten zum Einsatz, mit denen feststehende Begriffe priorisiert durchprobiert werden können.

Oft werden diese Listen allerdings umfangreich ergänzt, etwa um Buchstabenkombinationen, die bereits einmal als Passwort verwendet und erbeutet wurden. Dann werden auch komplizierte Phrasen mit in die Liste aufgenommen. Die Folge: Selbst bei eigentlich sehr komplexen Passwörtern besteht die Gefahr, dass diese so geknackt werden können.

Via Pwned Passwords können Sie nun überprüfen, ob ein Passwort in dem Datensatz von über 11 Milliarden geklauten Login-Daten auftaucht. Dies bedeutet, dass es eventuell in eine Wörterbuchliste aufgenommen wurde und trotz aller Komplexität leicht zu knacken sein könnte. Schlägt die Anzeige in der Web-App also rot an, sollten Sie lieber ein anderes Passwort verwenden.

Haben Sie in Pwned Passwords ein Kennwort eingegeben, erhalten Sie als Rückmeldung entweder eine grüne oder eine rote Meldung. Grün bedeutet: Das Passwort ist noch in keinem der durchsuchten Datensätze zu finden gewesen.

Springt die Anzeige auf Rot, ist das Kennwort Bestandteil erbeuteter Daten – und damit nicht mehr sicher. Sollte das Passwort in irgendeiner Weise von Ihnen aktiv genutzt werden, sollten Sie Ihr Kennwort sofort ändern.

Übrigens: In unserem umfangreichen Passwort-Tutorial erklären wir auch, wie Sie schnell und unkompliziert bei verschiedenen Anbietern (Amazon, Gmail, GMX etc.) Ihr Kennwort ändern können.

Wenn Sie nicht gerade Gedächtnisweltmeister sind, wird es Ihnen recht schwer fallen, sichere Passwörter für jedes Ihrer Benutzerkonten im Kopf zu behalten. Einen Ausweg bieten Passwort-Manager.

Die speichern sämtliche Zugangsdaten in einer verschlüsselten Datenbank ab, die Sie per Master-Passwort öffnen können. Sie müssen sich also nur noch ein starkes Passwort merken, den Rest übernehmen die Passwort-Manager.

Mehr oder weniger zum Standard ist es in den letzten Jahren geworden, dass Passwort-Manager die Passwort-Leaks von Have I Been Pwned zur Überprüfung der Passwort-Sicherheit einbinden. Wenn Sie zum Beispiel den beliebten Passwort-Manager KeePass nutzen, können Sie mit einem Plugin einen Passwort-Check realisieren. Bei KeePassXC ist der HIBP-Check sogar schon integriert.

Auch einige andere Passwort-Manager integrieren mittlerweile den Passwort-Sicherheitstest. HIBP arbeitet zum Beispiel eng mit dem Passwort-Manager 1Password zusammen, der im letzten CHIP-Test unser Testsieger war.

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

Quelle:https://www.chip.de/news/Datenklau-bei-WhatsApp-Alternative-Ihr-Konto-koennte-auch-dabei-sein_120125147.html?utm_source=flipboard&utm_content=topic%2Fde-digital

7) Vorsicht vor neuer Telefon-Abzocke: So locken Betrüger Sie in teure Abofallen

Erneut macht eine Telefon-Abzocke die Runde. Wie die Betrüger vorgehen und wie Sie sich vor der Abo-Falle schützen können, erklären wir hier.

Die "Apotheken Umschau", ein renommiertes Gesundheitsmagazin, dient aktuellen Berichten zufolge als Köder für eine raffinierte Betrugsmasche wie die "Deutsche Apotheker Zeitung" berichtet. Telefonbetrüger missbrauchen den guten Ruf der Zeitschrift, um arglose Bürgerinnen und Bürger hereinzulegen. Sie täuschen Gewinne aus Preisausschreiben vor und drängen den Angerufenen Zeitschriften-Abonnements auf.

Laut einer Mitteilung des Wort & Bild Verlags vom vergangenen Freitag, der das Magazin herausgibt, werden Gewinner von Preisausschreiben niemals telefonisch kontaktiert. Der Verlag distanziert sich zudem klar von der Weitergabe von Daten an Dritte.

Neuer Telefon-Betrug: Apotheken als Vertrauensfaktor missbraucht

Insbesondere ältere Menschen geraten häufig ins Visier von Telefonbetrügern, die sich das Vertrauen in lokale Apotheken zunutze machen. Ein Apothekeninhaber aus Unna berichtete dem "Hellweger Anzeiger" von einer Betrugsserie, bei der unter dem Vorwand einer Umfrage persönliche Daten und Kontaktdaten erfragt wurden. In vielen Fällen endete das Gespräch mit dem Abschluss eines unerwünschten Abonnements.

Um sich vor derartigen Betrugsversuchen zu schützen, ist es wichtig, wachsam zu bleiben und keine persönlichen Informationen am Telefon preiszugeben, insbesondere wenn man selbst keinen Kontakt initiiert hat.

Quelle: https://www.chip.de/news/Vorsicht-teure-Abo-Falle-Betrueger-nutzen-fiese-Telefon-Abzocke_185303907.html

8) Ticketmaster – Bericht: Hacker stellen angeblich Millionen Nutzerdaten ins Netz

Ticketmaster verkauft Eintrittskarten für große Konzerte und Festivals. Millionen Kundendaten des Anbieters stehen jetzt angeblich im Internet zum Verkauf.

Cyberkriminelle verkaufen laut eigenen Angaben 560 Millionen Kundendaten des Konzertkartenanbieters Ticketmaster im Internet. Das berichtet das Online-Magazin "Hackread". Unter den angebotenen Daten sollen Kreditkarteninformationen, Klarnamen, Adressen und E-Mail-Adressen sein. Ticketmaster hat sich bisher nicht zu dem Fall geäußert.

In dem 1,3 Terabyte großen Datenpaket, das die Hackergruppe "ShinyHunters" angeblich in ihrem Forum anbietet, könnten sich auch Millionen private Informationen deutscher Kunden befinden. Ticketmaster verkauft Eintrittskarten für Konzerte und Festivals auch hierzulande. Die Daten werden laut "Hackread" für 500.000 US-Dollar angeboten.

Jake Moore vom Sicherheitsunternehmen Eset stuft den Fall – sollte er sich wirklich so zugetragen haben – als besonders kritisch ein. "Die Menge an persönlichen Daten, die bei dieser Sicherheitsverletzung möglicherweise betroffen waren, macht diesen Vorfall für alle Beteiligten besonders besorgniserregend", sagt er.

Ticketmaster-Kunden sollten unbedingt ihre Zugangsdaten ändern

Moore rät Kunden von Ticketmaster, Passwörter zu ändern und Spam-Anrufe und Spam-Nachrichten zu ignorieren. "Vorfälle wie diese können verheerende Auswirkungen auf Nutzer haben, einschließlich Identitätsdiebstahl und Finanzbetrug", sagt Moore.

Laut "Hackread" wäre der Fall nicht der erste bei Ticketmaster. Bereits im vergangenen Jahr sei es zu einer Cyberattacke auf den Ticketverkauf für Konzerte der bekannten Sängerin Taylor Swift gekommen.

Ticketmaster selbst soll sich 2021 in die Infrastruktur des Konkurrenten Songkick gehackt haben, um vertrauliche Informationen zu erhalten. Dafür soll Ticketmaster die Passwörter ehemaliger Angestellten von Songkick genutzt haben. Das Unternehmen wurde damals zu einer Entschädigungszahlung in Höhe von zehn Millionen US-Dollar verurteilt.

Quelle: https://www.t-online.de/digital/aktuelles/id_100416236/ticketmaster-hacker-stellen-angeblich-millionen-nutzerdaten-ins-netz.html

9) „Nicht auf das Gespräch einlassen“: Vorsicht bei WhatsApp-Anruf

Digitale Kommunikationswege eröffnen Betrügern neue Möglichkeiten. Betrüger rufen derzeit über WhatsApp an. Sie täuschen vor, ihren Opfern helfen zu wollen.

Hamm - Betrüger lassen sich immer wieder neue Maschen einfallen, um Geld von ihren Opfern zu erbeuten. Zum Beispiel versprechen sie eine schnelle Kapitalanlage in Kryptowährung mit hoher Rendite oder falsche Medikamenten-Rezepte. Bei aktuellen Betrugsversuchen bieten Unbekannte nun ihren Opfern Hilfe bei der Suche nach verlorenem Geld an – und geben sich als seriöses Verbraucherzentrum aus.

Vorsicht bei WhatsApp-Anruf – „nicht auf das Gespräch einzulassen“

Die Betrüger verwenden verbotenerweise den Namen des Europäischen Verbraucherzentrums Deutschland (EVZ), teilt das EVZ selbst mit. Hinzu kommt, dass die Unbekannten das Logo des Netzwerks der europäischen Verbraucherzentren verwenden. Damit wollen die Betrüger vertrauenswürdig wirken. Erst kürzlich habe ein Verbraucher das EVZ darauf aufmerksam gemacht, dass Name und Logo des Zentrums für Betrugsanrufe verwendet wurden, erzählt Pressesprecherin und Co-Leiterin Karolina Wojtal im Gespräch mit *wa.de*. Es sei immer wieder der Fall, dass sich jemand als EVZ ausgebe.

„Die betroffenen Verbraucher haben eine Vorgeschichte. Das sind Verbraucher, die schon einmal betrogen wurden und ein vermeintliches Investment getätigt haben und so viel Geld verloren haben“, erklärt Karolina Wojtal weiter. Von den Betrügern werden sie daher als naiv eingestuft. Wer einen Anruf der Betrüger erhält, sollte „sich nicht auf das Gespräch einlassen“.

Behörden melden sich per Post

Zwischen dem ersten Betrugsfall und dem Anruf befindet sich ein zeitlicher Abstand. Dann werden die Verbraucher „aus heiterem Himmel kontaktiert und die Betrüger wollen helfen. Wir gehen davon aus, dass das dieselben Täter sind, die die Verbraucher bereits vorher betrogen haben. Oder es handelt sich um ein Netzwerk, das die Daten untereinander weitergibt“, erzählt Karolina Wojtal. Besonders perfide: Die Betrüger kontaktieren auch Menschen, die wegen des ersten Betrugsfalls gar keine Anzeige erstattet haben.

Die Gespräche laufen häufig so ab: Die Betrüger wollen erst Nachweise über den ersten Verlustfall. Erst verlangen sie harmlose Dokumente wie Überweisungsnachweise. Wenn durch erste Gespräche schon Vertrauensverhältnisse aufgebaut wurden, wird eine Kaution oder Gebühr verlangt. Denn die Betrüger geben gegenüber den Verbrauchern an, dass sie das verlorene Geld zurückverfolgen und bald auszahlen können. „Das ist alles erfunden“, so Karolina Wojtal. Die Täter kassieren dann das Geld und wenn sie merken, dass da kein Geld mehr zu holen ist oder das Betrugsopfer Verdacht schöpft, brechen sie den Kontakt ab.

Karolina Wojtal gibt einen wichtigen Hinweis an die Verbraucher: „Über die Handynummer werden die Menschen nicht kontaktiert.“ Wenn es neue Entwicklungen in Betrugsfällen gibt, erhalten die Verbraucher stattdessen Post vom Staatsanwalt. Und auch da sollte man laut Karolina Wojtal die Richtigkeit des Dokuments prüfen und notfalls bei der Staatsanwaltschaft anrufen.

Eine weitere fiese Betrugsmasche: Ein vermeintlicher Vertreter Ihres Stromanbieters will Ihre Zähler ablesen. Daraufhin ist ein neuer Stromvertrag in der Post.

Quelle: https://www.wa.de/verbraucher/whatsapp-betrug-anruf-vorsicht-warnung-achtung-masche-93093355.html

10) Banking-Trojaner bedroht Ihre Kontodaten: Android Nutzer müssen aufpassen

Android-Nutzer aufgepasst: Ein gefährlicher Banking-Trojaner hat es auf Ihre Kontodaten abgesehen. Was Sie beachten müssen, lesen Sie hier.

Cyber-Sicherheitsexperten stehen vor einer wachsenden Herausforderung: Der Banking-Trojaner "Grandoreiro" hat in einer ausgeklügelten Phishing-Kampagne die Kundendaten von ungefähr 1.500 Banken ins Visier genommen und breitet sich rasant aus. Einem neuen Bericht der IBM X-Force zufolge wurden diese Malware-Aktivitäten inzwischen schon in mehr als 60 Ländern festgestellt, darunter Regionen in Mittel- und Südamerika, Afrika, Europa und im Indopazifik.

Schon im Januar 2024 hatte eine gemeinsame Aktion von brasilianischen, spanischen Behörden, Interpol, der Sicherheitsfirma ESET und der Caixa Bank zu einer vorübergehenden Unterbrechung der Malware-Operation geführt, die seit 2017 besonders spanischsprachige Länder ins Visier nahm und Verluste von etwa 120 Millionen Dollar verursacht hat.

Banking-Trojaner Grandoreiro schlägt wieder zu: Trotz Razzia bleibt die Bedrohung bestehen

Obwohl im Rahmen der Operation fünf Personen in Brasilien festgenommen und dreizehn Durchsuchungen durchgeführt wurden, bleibt unklar, welche Rolle die Verhafteten in dem Malware-Netzwerk spielten. Der IBM X-Force-Bericht deutet darauf hin, dass Grandoreiro seit März 2024 mit neuer Kraft zurück ist, möglicherweise durch ein Malware-as-a-Service-Modell an Cyberkriminelle vermietet wird und nun auch englischsprachige Länder angreift.

Zusätzlich hat der Trojaner technische Verbesserungen und neue leistungsfähige Funktionen erhalten, was darauf hindeutet, dass seine Schöpfer einer Festnahme entkommen sind und sich von der Razzia nicht abschrecken ließen.

Phishing-E-Mails, die von IBM beobachtet wurden, geben sich als Mitteilungen von Regierungseinrichtungen in Mexiko, Argentinien und Südafrika aus und zielen vornehmlich auf Steuerbehörden, Finanzdienstleister und Elektrizitätskommissionen ab. Diese E-Mails nutzen das jeweilige Muttersprachniveau der Empfänger, beinhalten offizielle Logos und Formate und locken mit Handlungsaufforderungen wie Links zum Betrachten von Rechnungen, Kontoauszügen oder Steuerdokumenten. Ein Klick darauf leitet den Empfänger zu einem PDF-Bild, das den Download einer ZIP-Datei auslöst – darin enthalten ist eine aufgeblähte (100 MB) ausführbare Datei, mit der die Grandoreiro-Malware ausgeführt wird.

Quelle: https://www.chip.de/news/Banking-Trojaner-bedroht-Kontodaten-Android-Nutzer-muessen-aufpassen_185283627.html

11) Dubiose Mails – Phishing-Offensive mit Gebühren-Androhung: Kunden zahlreicher Banken betroffen

Betroffen sind Kunden von Targobank, Commerzbank, Deutscher Bank und DKB. Phisher wollen mit angedrohten Gebühren an Kundendaten gelangen.

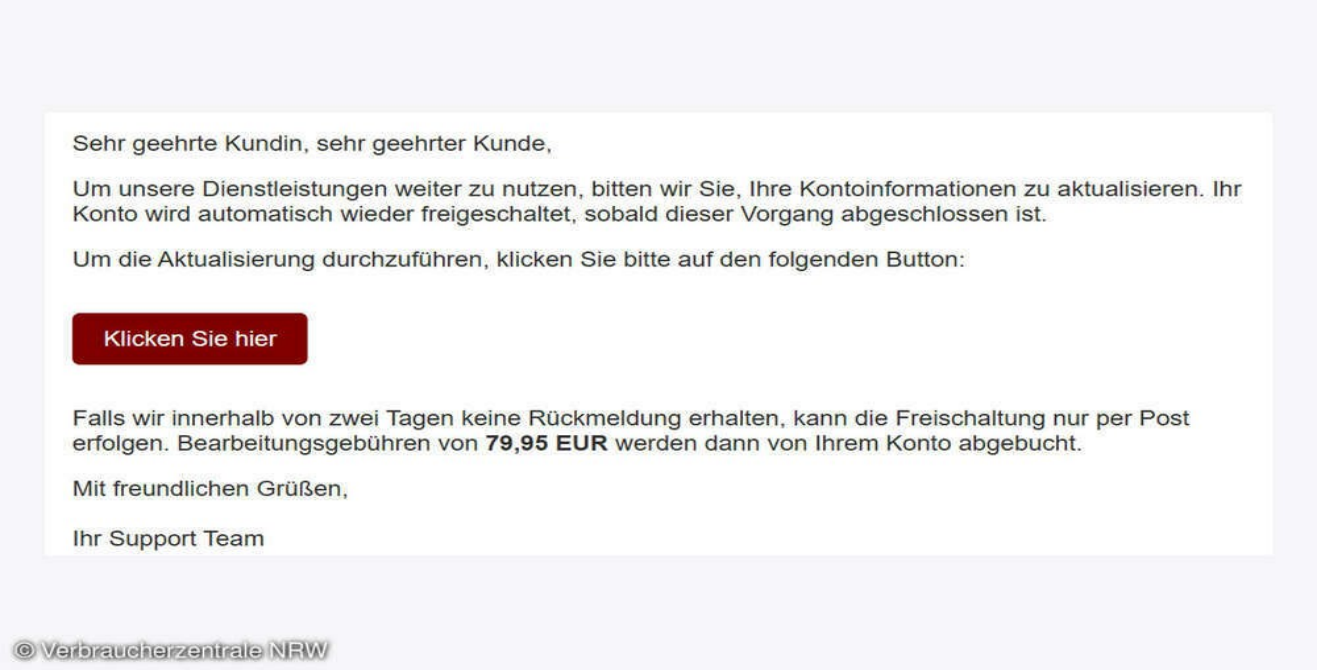
Phishing-Mails gehören mittlerweile zur Normalität. Das bedeutet auch, dass von den Nutzern erhöhte Aufmerksamkeit gefordert ist. Denn die gefälschten Mails werden immer

besser – und fallen immer dreister aus. Derzeit machen Phishing-Versuche bei der Targobank, der Deutschen Bank, der Commerzbank und der DKB die Runde, wovor die Verbraucherzentralen eindringlich warnen.

Die Mails gehen mit dem Betreff „Dringende Kontoaktualisierung erforderlich“ bei Kunden ein. Hier sollen die bei der Bank hinterlegten persönlichen Informationen aktualisiert werden. Dazu sollen Kunden auf einen Button in der E-Mail klicken. Nur dann könne die „Dienstleistung“ weiter aufrechterhalten werden. Derlei Herangehensweise kennt man bereits.

Neu ist, dass jetzt auch mit einer Gebühr gedroht wird. Denn sollte die Bank innerhalb von zwei Tagen keine Rückmeldung erhalten, müsse man auf eine Freischaltung per Post umstellen, was eine Bearbeitungsgebühr in Höhe von 79,95 Euro zur Folge hätte. Dieser Betrag würde einfach vom Konto abgebucht.

Die Phishing-Mail kann als solche allerdings leicht identifiziert werden. Es gibt keine persönliche Anrede, es gibt keine Hinweise auf ein bestehendes Geschäftsverhältnis, es ist kein Logo enthalten und es wird ein nicht adäquater Zeitdruck für eine Reaktion, verbunden mit der Androhung einer Gebühr, aufgebaut. Die einzig richtige Reaktion ist: Verschieben Sie die Mail in den Spam-Ordner!



So sieht die aktuelle Phishing-Mail aus, die Kunden diverser deutscher Banken derzeit erhalten. © Verbraucherzentrale NRW

Quelle: https://www.connect.de/news/phishing-warnung-targobank-commerzbank-deutsche-bank-dkb-kontoaktualisierung-erforderlich-3205952.html?utm_source=connect-NL&utm_medium=newsletter

12) Sicherheit – Neue Phishing-Taktik: Gefälschte Amazon-Mails zielen auf ahnungslose Kundschaft

Derzeit häufen sich Berichte über Phishing-Versuche, die sich gegen die Amazon-Kundschaft richten. Eine neue Betrugsmasche fordert Nutzer unter dem Vorwand angeblicher Abrechnungsprobleme auf, ihre Zahlungsinformationen zu aktualisieren.

Erst vor nicht einmal zwei Monaten berichteten wir über einen Phishing-Angriff auf Amazon-Kunden. Doch die Phishing-Mafia lässt nicht locker und denkt sich immer neue Betrugsmaschen aus.

Diesmal soll das Amazon-Konto wegen angeblicher **Abrechnungsprobleme in der Warteschleife** hängen. Wir zeigen Ihnen, wie Sie sich vor diesem Betrugsversuch schützen können.

Erkennungsmerkmale der Phishing-Mails

Diese Phishing-E-Mails beginnen typischerweise mit einer alarmierenden Nachricht über Probleme bei der Kontenabrechnung, gefolgt von einem auffälligen Button, der die Nutzer dazu auffordert, ihre **Zahlungsdetails zu aktualisieren**. Die Gestaltung dieser Nachrichten ist oft mangelhaft, erkennbar an fehlenden offiziellen Logos und unprofessioneller Ansprache.

Technik der Täuschung

Die Betrüger nutzen die persönliche Anrede der Empfänger, um Vertrauen zu schaffen und Dringlichkeit zu suggerieren. Die Fristsetzung von **24 Stunden** soll die Empfänger zu einer überstürzten Handlung bewegen. Hierbei handelt es sich um eine klassische Technik, um Unsicherheit und Eile zu erzeugen.

Zielgruppe und Warnungen

In erster Linie wird **Stammkundschaft von Amazon** angesprochen, insbesondere solche, die mit den typischen Kommunikationskanälen des Unternehmens nicht vertraut sind. Es ist wichtig, solche E-Mails kritisch zu betrachten und für Zahlungsangelegenheiten auf die offiziellen Kanäle zurückzugreifen.

Die jüngsten Phishing-Versuche zeigen, dass Cyberkriminelle ständig neue Methoden entwickeln, um Nutzer zu täuschen. Die **gefälschten E-Mails**, die sich auf angebliche Abrechnungsprobleme bei Amazon beziehen, sind ein aktuelles Beispiel für die Notwendigkeit, wachsam zu bleiben und offizielle Kommunikationswege zu nutzen, um persönliche Informationen sicher zu halten.

5 Schritte zum Schutz vor Phishing

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

FAQ - Häufig gestellte Fragen zum Thema Phishing

- **Was ist Phishing und wie gehen die Betrüger vor?** Beim Phishing versuchen Betrüger, mit gefälschten E-Mails an persönliche Daten zu gelangen. Bei dieser Phishing-Welle erhalten Klarna-Kunden gefälschte E-Mails, in denen sie aufgefordert

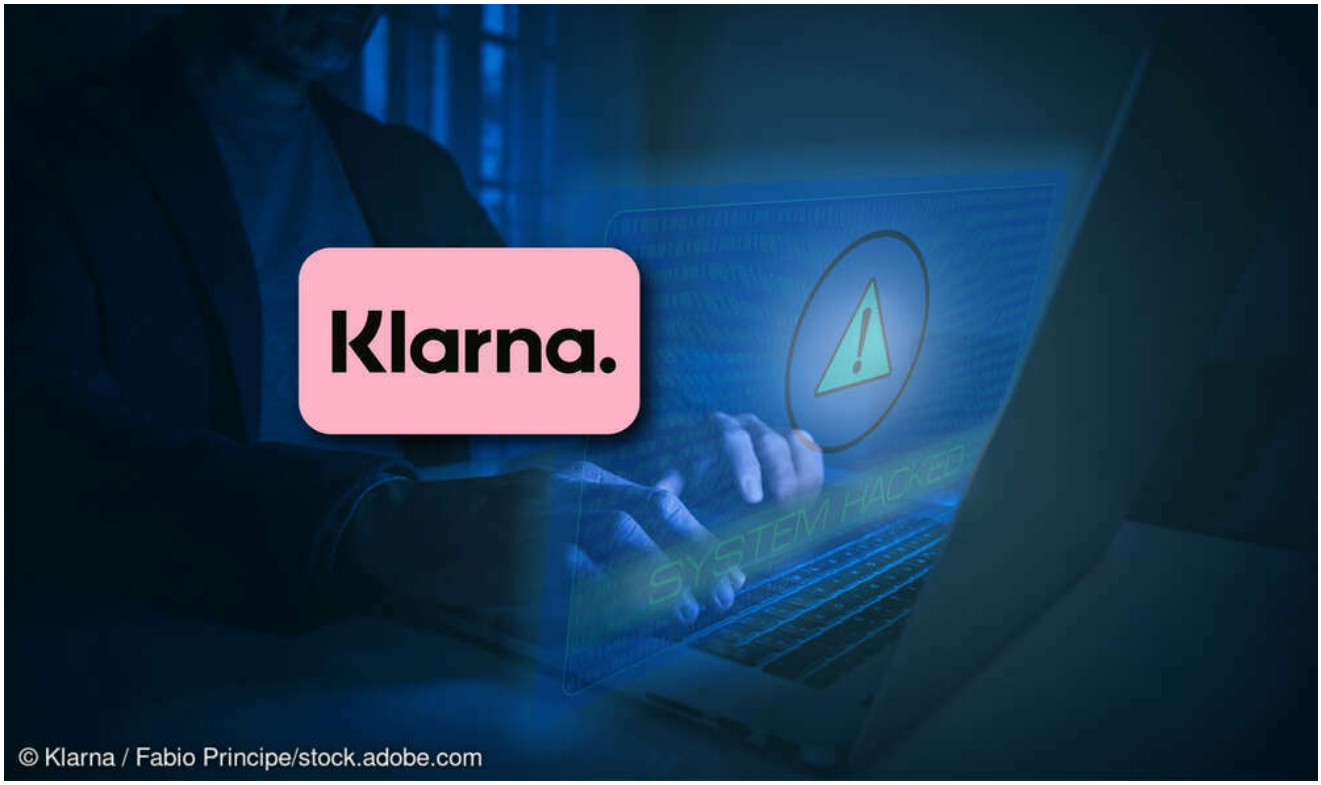
werden, ihre Einzugsermächtigung zu erneuern. Die Betrüger verwenden personalisierte Anreden, sehr eindringliche Aufforderungen und gefälschte Logos, um ihre Opfer dazu zu bringen, auf Links in der E-Mail zu klicken und ihre Daten preiszugeben.

- **Wie erkenne ich eine betrügerische E-Mail?** Achten Sie auf verdächtige Absenderadressen, Rechtschreib- oder Grammatikfehler, hohe Dringlichkeit und unerwartete Forderungen nach persönlichen Daten. E-Mails, die angeblich von Klarna stammen, haben eine unseriöse Absenderadresse und drängen zum sofortigen Handeln.
- **Was soll ich tun, wenn ich eine solche E-Mail erhalte?** Verschieben Sie die E-Mail sofort in den Spam-Ordner und kontaktieren Sie das Unternehmen direkt, anstatt auf Links in der E-Mail zu klicken.
- **Wie kann ich mich vor Phishing schützen?** Geben Sie niemals persönliche Daten preis, überprüfen Sie die Absenderadresse, klicken Sie nicht blind auf Links in E-Mails, verwenden Sie Spam-Filter und installieren Sie Antiviren-Software.
- **Sind alle Aufforderungen zum Handeln betrügerisch?** Nicht immer, aber seien Sie wachsam und wenden Sie sich im Zweifelsfall direkt an das Unternehmen.

Quelle: https://www.connect.de/news/neue-phishing-taktik-gefaelschte-amazon-mails-zielen-auf-ahnungslose-kundschaft-3206000.html?utm_source=nachrichten-NL&utm_medium=newsletter

13) Sicherheit – Betrugswarnung: Neue Phishing-Welle zielt auf Klarna-Kunden ab

Mit einer neuen Masche versuchen Kriminelle, über gefälschte E-Mails an Kontodaten zu gelangen. Wir erklären, wie die Betrüger vorgehen und wie Sie sich schützen können.



Die Phishing-Mafia ist nach wie vor aktiv und auf der Suche nach neuen Opfern. Aktuell sind Klarna-Kunden im Visier.

In der vergangenen Woche haben viele Klarna-Kunden E-Mails erhalten, in denen sie aufgefordert wurden, ihr Lastschriftmandat zu erneuern. Unter dem Vorwand, weiterhin bequem mit Klarna bezahlen zu können, fordern die scheinbar offiziellen Nachrichten zum sofortigen Handeln auf. **Doch Vorsicht ist geboten!**

Die Täuschung entlarvt

Die E-Mail beginnt mit einer persönlichen Anrede und informiert den Empfänger, dass die Einzugsermächtigung zu einem bestimmten Datum (in diesem Fall der 11.04.2024) abläuft. Der Druck wird erhöht, indem der Empfänger aufgefordert wird, das Mandat **innerhalb von 48 Stunde**n zu erneuern.

Ein auffälliger Button mit der Aufforderung „Erneuern“ soll den Empfänger dazu verleiten, auf den Link zu klicken, um die vermeintlich nächsten Schritte einzusehen.

Das **Klarna-Logo** und die persönliche Ansprache sollen Sicherheit suggerieren. Hinter dieser Fassade verbirgt sich jedoch ein klares Ziel: **sensible Daten auszuspähen**.

Ein weiteres **Warnsignal** ist die unseriöse Absenderadresse der E-Mail. Es handelt sich mit hoher Wahrscheinlichkeit um einen betrügerischen Phishing-Versuch. Es wird dringend davon abgeraten, den Anweisungen in dieser E-Mail zu folgen. Alle ähnlichen Nachrichten sollten sofort in den **Spam-Ordner** verschoben werden.

Vorsicht ist geboten!

Es ist wichtig, immer aufmerksam und wachsam zu sein, insbesondere bei E-Mails, die zum sofortigen Handeln auffordern. Klarna oder andere seriöse Unternehmen würden **niemals so dringend nach sensiblen Daten fragen**. Im Zweifelsfall ist es ratsam, das Unternehmen direkt zu kontaktieren, anstatt unbekannten Links in E-Mails zu folgen.

Sicherheit sollte immer an erster Stelle stehen. Bleibt wachsam und schützt eure persönlichen Daten!

Quelle: https://www.connect.de/news/phishing-warnung-klarna-betrug-kontodaten-sicherheit-schutz-lastschriftmandat-3205175.html

Anwenderinformationen:

1) Sicherheitsrisiko durch Russland – US-Regierung verbietet Kaspersky-Software

Die US-Regierung hat den Verkauf der Antivirensoftware Kaspersky in den Vereinigten Staaten verboten. Grund dafür sind mögliche Verbindungen zum Kreml.

Kaspersky Lab ist ein weltweit bekannter Anbieter von Cybersicherheitslösungen, dessen Produkte auch in Deutschland weit verbreitet sind. Wie die Nachrichtenagentur Reuters berichtet, habe die US-Regierung nun entschieden, dass der Einfluss Russlands auf das Unternehmen ein erhebliches Risiko darstelle.

"Russland hat gezeigt, dass es in der Lage ist und die Absicht hat, russische Unternehmen wie Kaspersky auszunutzen, um die persönlichen Daten von Amerikanern zu sammeln und als Waffe einzusetzen", erklärte Handelsministerin Gina Raimondo.

Konkrete Gefahren durch privilegierten Zugriff

Der privilegierte Zugang der Kaspersky-Software zu Computersystemen könnte es ermöglichen, vertrauliche Informationen zu stehlen oder Schadsoftware zu installieren und wichtige Updates zurückzuhalten. Besonders brisant sei dies, da laut einer nicht näher genannten Quelle auch Anbieter kritischer Infrastrukturen sowie staatliche und lokale Behörden zu den Kunden von Kaspersky zählen würden.

Der demokratische Senator Mark Warner betonte: "Wir würden niemals einer gegnerischen Nation die Schlüssel zu unseren Netzwerken oder Geräten geben. Es ist also verrückt zu glauben, dass wir weiterhin zulassen würden, dass russische Software mit dem tiefstmöglichen Gerätezugang an Amerikaner verkauft wird."

Konsequenzen für Nutzer und Unternehmen

Der Verkauf der Software soll ab dem 20. Juli 2024 verboten werden. Ab dem 29. September 2024 solle es für Nutzer dann auch keine Updates mehr geben. Dadurch hätten Unternehmen noch eine gewisse Zeit, um Alternativen zu finden.

Verkäufer und Wiederverkäufer, die gegen diese Beschränkungen verstoßen, müssen mit Geldstrafen rechnen. Vorsätzliche Verstöße könnten sogar strafrechtlich verfolgt werden. Nutzer der Software selbst müssen zwar keine rechtlichen Sanktionen befürchten, werden aber dringend aufgefordert, auf andere Lösungen umzusteigen.

Reaktionen aus Russland

Kaspersky selbst wies darauf hin, dass die Entscheidung auf "dem gegenwärtigen geopolitischen Klima und theoretischen Bedenken" basiere und nicht auf einer umfassenden Bewertung ihrer Produkte und Dienstleistungen. In einer Erklärung betonte das Unternehmen, es habe "mit seinen Reports und seinem Schutz vor einer Vielzahl von Bedrohungsakteuren, die es auf die Interessen der USA und ihren Verbündeten abgesehen haben, tatsächlich sogar einen wichtigen Beitrag geleistet." Zudem kündigte Kaspersky an, alle rechtlichen Mittel auszuschöpfen, um das Verbot anzufechten.

Schon seit Jahren stehen Kasperskys Aktivitäten unter Beobachtung. Bereits 2017 hatte das US-Heimatschutzministerium (Department of Homeland Security) den Einsatz von Kasperskys Antivirenprodukten in Bundesbehörden verboten – wegen angeblicher

Verbindungen zu russischen Geheimdiensten.

Nun zeigt sich erneut wachsender Druck auf das Unternehmen aufgrund Moskaus Kriegshandlungen in der Ukraine. Durch das neue Verkaufsverbot wolle die USA jegliche Risiken durch mögliche russische Cyberangriffe ausschließen – insbesondere in Zeiten erhöhter geopolitischer Spannungen.

Auswirkungen auf Deutschland?

Inwieweit die Entscheidung der US-Regierung auch Auswirkungen auf deutsche Nutzer haben könnte, bleibt abzuwarten. Während bisher keine konkreten Maßnahmen gegen Kaspersky in Deutschland bekannt sind, könnte dieser Schritt der USA durchaus Diskussionen über Cybersicherheitsrisiken auch bei uns anstoßen.

Bereits im März 2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Warnung vor dem Einsatz von Kaspersky ausgesprochen. Hintergrund ist ein Gesetz, das es der russischen Regierung ermöglicht, auf Daten von Unternehmen zuzugreifen.

Tipp der Reaktion: "Ein Muss für jeden Rechner": Stiftung Warentest prüft Antivirenprogramme

Quelle: https://www.t-online.de/digital/aktuelles/id_100431864/kaspersky-verbot-usa-stoppen-russische-software-wegen-sicherheitsrisiko.html

2) Datenrettung – Android: Gelöschte Kontakte wiederherstellen – so klappt's

Die Kontakte-App von Android erlaubt es Ihnen, gelöschte Kontakte wiederherzustellen. Das klappt jedoch nur unter bestimmten Bedingungen. Eine Anleitung.

Auf vielen Smartphones häufen sich im Laufe der Zeit allerhand Kontaktdaten an. Manchmal lohnt es sich, die Kontaktliste auszumisten und ein paar nicht mehr benötigte Einträge zu löschen. Wie Sie gelöschte Kontakte unter Android wiederherstellen, wenn Sie beim Aufräumen etwas übereifrig waren, erfahren Sie hier.

Kurz zusammengefasst:

- Gelöschte Kontakte können unter Android oft wiederhergestellt werden.
- Voraussetzung ist eine aktive Kontaktsynchronisation mit Google.
- Die Wiederherstellung ist über den Papierkorb der Kontakte-App möglich.

So lassen sich gelöschte Kontakte unter Android wiederherstellen

In den Werkseinstellungen synchronisiert Android Ihre Kontaktliste automatisch mit den Servern von Google. Wenn Sie diese Android-Funktion nicht explizit deaktiviert haben und der Löschvorgang nicht mehr als 30 Tage in der Vergangenheit liegt, lassen sich gelöschte Kontaktdaten über den Papierkorb der Kontakte-App wiederherstellen. Gehen Sie dafür wie folgt vor:

1. Öffnen Sie auf Ihrem Android-Smartphone die (Google-)Kontakte-App.
2. Stellen Sie sicher, dass oben rechts das Google-Konto ausgewählt ist, in dem die Kontaktdaten gespeichert waren.
3. Wechseln Sie unten auf den Tab "Verwalten" und tippen Sie dann auf "Papierkorb".
4. Wenn Sie nur einen der von Ihrem Android-Gerät gelöschten Kontakte wiederherstellen möchten, tippen Sie diesen an und wählen Sie "Wiederherstellen".

Wollen Sie mehrere Kontakte auf einmal wiederherstellen, so halten Sie zunächst auf einen der Kontakte gedrückt und tippen Sie danach weitere Kontakteinträge an, um sie zu markieren. Öffnen Sie anschließend oben rechts das Dreipunkt-Menü und wählen Sie "Wiederherstellen".

Tipp: Möchten Sie ausnahmslos alle im Papierkorb befindlichen Kontakte auf einmal wiederherstellen, so öffnen Sie in Schritt 4 einfach direkt das Dreipunkt-Menü und tippen Sie auf "Alle auswählen". Dies erspart Ihnen die manuelle Auswahl der einzelnen Listeneinträge.

Darum lassen sich Ihre Android-Kontakte nicht wiederherstellen

Wenn das Wiederherstellen der Kontakte auf Ihrem Android-Smartphone nicht möglich ist, kann das verschiedene Ursachen haben.

Stellen Sie zunächst sicher, dass die Kontaktsynchronisation aktiv ist. Öffnen Sie dafür die Systemeinstellungen von Android und navigieren Sie zu "Google > Alle Dienste > Einstellungen für Google-Apps > Google Kontakte synchronisieren > Synchronisierungsstatus". War der Status bisher nicht aktiv, so ist eine Wiederherstellung Ihrer gelöschten Kontakte nicht möglich.

Darüber hinaus ist der Papierkorb der Kontakte-App nur verfügbar, wenn Ihr Mobiltelefon mit dem Internet verbunden ist. Gelöschte Kontakte liegen auf den Servern von Google und lassen sich nur wiederherstellen, wenn Ihr Android-Gerät diese erreichen kann.

Kontaktdaten, die nur lokal auf Ihrer SIM-Karte gespeichert sind, werden nicht automatisch mit Ihrem Google-Konto synchronisiert. Auch in diesem Fall ist eine Wiederherstellung ausgeschlossen. Übertragen Sie die Kontakte auf Ihr Google-Konto, um künftig von der Papierkorb-Funktion zu profitieren.

Quelle: https://www.t-online.de/digital/smartphone/id_100424080/android-geloeschte-kontakte-wiederherstellen-so-klappt-s.html

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

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

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

Sind iPhones vor Viren sicher?

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

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

So erkennen Sie Viren

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

- Ungewöhnlich hoher Akkuverbrauch
- Plötzlich langsame Leistung
- Unautorisierte App-Installationen

- Unerwartete Pop-ups oder Anzeigen
- Anstieg des mobilen Datenvolumens

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

Scannen Sie Ihr iPhone

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

Entfernung von iPhone-Viren

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

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

Sicherheitstipps

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

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

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

Web-Sicherheit

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

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

Was ist ein Jailbreak?

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

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

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

4) Gefahr für's Smartphone: 92 Prozent aller Urlauber machen auf Reisen denselben Fehler

Auch im Urlaub ist das Smartphone für die meisten Menschen ein steter Begleiter. Viele sind sich den Gefahren dabei nicht bewusst.

Wer im Urlaub ist, möchte entspannen und sich keine Gedanken um Datensicherheit machen. Doch eine aktuelle Studie des IT-Security-Spezialisten G Data unter 1.000 Internetnutzern aus Deutschland warnt: 92 Prozent der Reisenden nehmen ihre mobilen Geräte mit und nutzen achtlos öffentliche WLAN-Netze – eine Einladung für Cyberkriminelle.

Beliebte Anlaufpunkte wie Flughäfen, Hotels und Bahnhöfe bieten oft unsichere Netzwerke, in denen Datendiebe leichtes Spiel haben, um sensible Informationen wie Passwörter oder Kreditkartendaten zu stehlen. Die Folgen: Identitätsdiebstahl oder finanzielle Betrügereien. G DATA-Experte Tim Berghoff mahnt zur Vorsicht und empfiehlt wichtige Sicherheitsvorkehrungen.

Prävention vor der Abreise: Sicherheitslösungen und VPNs schützen ihr Smartphone

Um sich vor den Gefahren unsicherer Netzwerke zu schützen, sollten Urlauber vor Reiseantritt handeln. Eine umfassende Sicherheitslösung auf allen mobilen Geräten ist ebenso ratsam wie die Nutzung eines VPNs. Dieses bietet durch die verschlüsselte Übertragung einen effektiven Schutz der Privatsphäre, indem es die Daten von außen unsichtbar macht.

Zusätzlich rät G Data zur Durchführung von Updates, um Sicherheitslücken in Betriebssystemen und Apps zu schließen. Eine Datensicherung auf einem externen Medium ist ebenfalls empfehlenswert. Für das Aufladen der Geräte an öffentlichen USB-Ladestationen sollte ein USB-Kondom verwendet werden, um das Gerät vor Datenableitung zu schützen – ein kleines Gadget, das große Wirkung zeigt.

Quelle: https://www.chip.de/news/Fast-jeder-Deutsche-macht-im-Urlaub-diesen-Smartphone-Fehler_185336092.html

5) Besonders perfider Anruf-Betrug: Bei dieser Nummer sollten Sie direkt auflegen

Aktuell mehren sich die Berichte über eine neue Art von Telefonbetrug. Wir erklären, bei welcher Nummer Sie am besser direkt auflegen.

In den letzten Tagen häufen sich die Meldungen über verdächtige Anrufe unter der Nummer 015214662659, warnt "tellows". Offenbar handelt es sich dabei um eine neue Form des Telefonbetrugs, bei dem Kriminelle an persönliche Daten der Empfänger gelangen wollen.

Wenn man den Anruf annimmt, wird man von einer Computerstimme begrüßt und bekommt ein Angebot zur Kostenersparnis bei der Krankenversicherung. Wer auf die Aufforderung reagiert und die "1" drückt, landet bei einem Callcenter-Mitarbeiter, der persönliche Daten abfragt und zum Wechsel der Krankenkasse drängt. Wer skeptisch bleibt und nicht reagiert, wird teilweise immer wieder kontaktiert, manchmal auch unter wechselnden Nummern.

Das Prinzip hinter der Betrügerei ist einfach: Die Callcenter verwenden Wählcomputer mit raffinierten Programmen, die nicht nur Nummern fälschen, sondern auch potenzielle Opfer identifizieren. Die Technik heißt Call-ID-Spoofing und erleichtert Betrügern das Leben.

So erkennen Sie betrügerische Anrufe und wehren Sie richtig ab

Es handelt sich dabei um sogenannte Ping-Anrufe, die die Existenz und Reaktion der Angerufenen testen. Das Ziel von den Betrüger ist es, unter Druck Geschäfte anzubahnen oder persönliche Daten zu erlangen. Bei Rückrufen kann auch die Weiterleitung nach Drücken der Taste "1" schon zu hohen Zusatzkosten für den Anrufer führen.

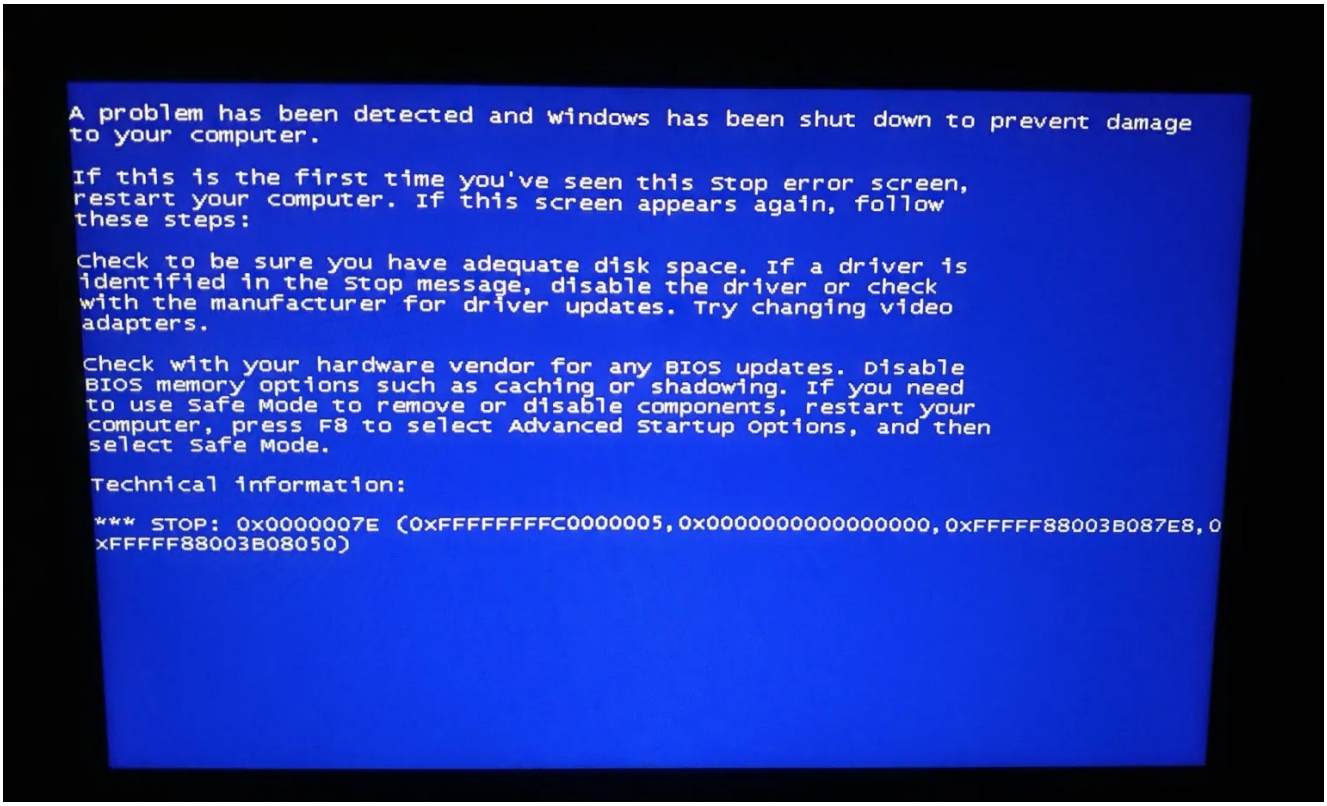
Diese Form des Betrugs stellt eine Herausforderung für Verbraucher und Gesundheitsdienstleister dar. Sie erfordert eine stärkere Sensibilisierung und geeignete Maßnahmen zum Schutz vor finanziellen und persönlichen Schäden. Das Problem ist nicht zu unterschätzen: Laut "tellows" sind 75% aller Anrufe von angeblichen Krankenkassen als Spam oder Phishing einzustufen.

Anmerkung der Redaktion: unter dem u.g. Link kann noch ein entsprechender Filmbeitrag abgerufen werden.

Quelle: https://www.chip.de/news/Neuer-Telefonbetrug-Bei-Anrufen-dieser-Nummer-besser-auflegen_185258909.html

6) Computer: Vorsicht vor dieser Fehlermeldung – nicht klicken

Kriminelle locken ihre Opfer inzwischen mit gefälschten Popup-Fenstern in die Falle. Dabei verwenden sie verschiedene Tarnungen.



Windows 11: Welche Systemanforderungen dein PC erfüllen muss

Windows 11 bietet gegenüber seinem Vorgänger eine Vielzahl neuer Funktionen.Willst du jede von ihnen problemlos nutzen, musst du allerdings einige Voraussetzungen erfüllen. Quelle: u00a9 HaileyFaith - stock.adobe.com

Wer am **Computer** eine Fehlermeldung erhält, denkt sich in der Regel nichts Schlimmes dabei. Und genau das wissen auch Hackerinnen und Hacker, die aktuell mit einer neuen Malware sowohl gefälschte Chrome-, OneDrive- als auch Microsoft Word-Benachrichtigungen erstellen.

Computer: Vor dieser Malware warnen Forschende

Sicherheitsforschende des Cybersicherheitsunternehmens Proofpoint haben eine neue Masche von Kriminellen gemeldet, mit der sie Nutzer*innen dazu verleiten, eine Malware namens ClickFix zu installieren. Dazu bieten man ihnen gefälschten Lösungen für häufige Fehler am Computer in den beliebten Diensten wie den oben genannten an.

In der Chrome-Version besagt das sich öffnende Popup beispielsweise „Etwas ist schief gelaufen mit der Darstellung dieser Webseite“. Das wird begründet mit einem fehlenden Update des Browsers, das sich über die angezeigte Schaltfläche „Korrektur kopieren“ (engl.: Copy fix) aber nachholen ließe.

Sobald Betroffene das entsprechende Feld anklicken, die vermeintlichen „Korrekturen“ herunterladen und ausführen, führen sie allerdings statt der Fehlerbehebung unwissentlich einen PowerShell- oder Windows-Ausführungsdialogbefehl aus, der ihre Systeme kompromittiert.

Dabei handelt es sich im Detail um ein Computer-Kommando, das direkt in die PowerShell-Konsole oder in den Ausführen-Dialog von Windows eingegeben wird, um eine Vielzahl von Aufgaben zu erledigen, die von der Ausführung von Programmen über das Öffnen von Systemwerkzeugen bis hin zur Durchführung von Systemadministrationsaufgaben reichen. Fremde erlangen damit also ganz unbemerkt weitreichende Systemzugriffe.

Wer am **Computer** eine Fehlermeldung erhält, denkt sich in der Regel nichts Schlimmes dabei. Und genau das wissen auch Hackerinnen und Hacker, die aktuell mit einer neuen Malware sowohl gefälschte Chrome-, OneDrive- als auch Microsoft Word-Benachrichtigungen erstellen.

Computer: Vor dieser Malware warnen Forschende

Sicherheitsforschende des Cybersicherheitsunternehmens Proofpoint haben eine neue Masche von Kriminellen gemeldet, mit der sie Nutzer*innen dazu verleiten, eine Malware namens ClickFix zu installieren. Dazu bieten man ihnen gefälschten Lösungen für häufige Fehler am Computer in den beliebten Diensten wie den oben genannten an.

In der Chrome-Version besagt das sich öffnende Popup beispielsweise „Etwas ist schief gelaufen mit der Darstellung dieser Webseite“. Das wird begründet mit einem fehlenden Update des Browsers, das sich über die angezeigte Schaltfläche „Korrektur kopieren“ (engl.: Copy fix) aber nachholen ließe.

Sobald Betroffene das entsprechende Feld anklicken, die vermeintlichen „Korrekturen“ herunterladen und ausführen, führen sie allerdings statt der Fehlerbehebung unwissentlich einen PowerShell- oder Windows-Ausführungsdialogbefehl aus, der ihre Systeme kompromittiert.

Dabei handelt es sich im Detail um ein Computer-Kommando, das direkt in die PowerShell-Konsole oder in den Ausführen-Dialog von Windows eingegeben wird, um eine Vielzahl von Aufgaben zu erledigen, die von der Ausführung von Programmen über das Öffnen von Systemwerkzeugen bis hin zur Durchführung von Systemadministrationsaufgaben reichen. Fremde erlangen damit also ganz unbemerkt weitreichende Systemzugriffe.

Quelle: https://www.futurezone.de/digital-life/article556727/computer-fehlermeldung-nicht-klicken.html?utm_source=flipboard&utm_content=topic%2Fde-digital

7) Neue Sicherheitsfunktion – WhatsApp will Ihre E-Mail-Adresse wissen – das ist der Grund

Neben der Telefonnummer können WhatsApp-Nutzer in den Einstellungen jetzt auch ihre E-Mail-Adresse hinterlegen. Das hat einen einfachen Grund.

Kurz zusammengefasst:

- WhatsApp-Nutzer können jetzt im Messenger ihre E-Mail-Adresse hinterlegen.
- Die E-Mail-Adresse ermöglicht eine zusätzliche Verifizierung des Anwenders.
- Beim Verlust der PIN kann diese per E-Mail erneuert werden.

Der beliebte Messenger WhatsApp gibt Ihnen jetzt auch die Möglichkeit, Ihre E-Mail-Adresse zu hinterlegen. Diese Funktion dient als zusätzlicher Schutz, damit Sie sich als Inhaber des WhatsApp-Kontos identifizieren können. Bislang war das nur über die Telefonnummer möglich.

Ein Grund für die Verifizierung per E-Mail kann zum Beispiel sein, dass Sie den Messenger auf einem neuen Telefon installieren wollen. Wenn der Handyempfang schlecht sein sollte, brauchen Sie nicht auf einen Verifizierungscode per SMS zu warten, sondern können sich diesen an Ihre bei WhatsApp hinterlegte E-Mail-Adresse schicken lassen.

So können Sie bei WhatsApp eine E-Mail-Adresse hinterlegen:

- Rufen Sie die Einstellungen im Messenger auf.
- Gehen Sie auf "Konto" und dann auf "E-Mail-Adresse".
- Gehen Sie auf "E-Mail hinzufügen".
- Klicken Sie auf "Weiter".
- Geben Sie den sechsstelligen Code ein, den WhatsApp an Ihre E-Mail-Adresse geschickt hat.
- Fertig.

Sie können Ihre E-Mail-Adresse jetzt auch nutzen, wenn Sie Ihre bei WhatsApp eingerichtete PIN vergessen haben, um die Verifizierung in zwei Schritten (Zwei-Faktor-Authentifizierung) durchzuführen. Dann schickt WhatsApp Ihnen ebenfalls einen Code an die von Ihnen hinterlegte E-Mail-Adresse.

So richten Sie die Zwei-Faktor-Authentifizierung ein:

- Rufen Sie die Einstellungen im Messenger auf.
- Gehen Sie auf "Konto" und dann auf "Verifizierung in zwei Schritten".
- Gehen Sie auf "Aktivieren".
- Geben Sie eine sechsstellige PIN ein.
- Bestätigen Sie Ihre PIN.
- Fertig.

Künftig wird Sie WhatsApp regelmäßig nach Ihrer PIN fragen. Sollten Sie die sechsstellige PIN vergessen haben, können Sie den Zahlencode über Ihre bei WhatsApp hinterlegte E-Mail-Adresse zurücksetzen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100434312/whatsapp-will-ihre-e-mail-adresse-wissen-das-ist-der-grund.html

8) Jetzt deaktivieren: Experte rät von 2 beliebten iPhone-Einstellungen ab

Nicht jede iPhone-Einstellung muss dir etwas bringen. Ein Spezialist sagt sogar, dass du zwei Funktionen besser sein lässt.

Läuft es mit dem Handy mal nicht ganz so flüssig wie gewohnt, muss das nicht an der Hardware liegen. In machen Fällen sind verschiedenen **iPhone-Einstellungen** Schuld, wie der Experte James Calderon des Tech-Magazins Alrigh weiß. Ihm zufolge gibt es gleich zwei überraschende Features, die in Frage kommen können und von Zeit zu Zeit deaktiviert gehören.

Ungewöhnlich träge? Achte auf 2 iPhone-Einstellungen

Die erste der beiden iPhone-Einstellungen, auf die Calderon hinweist, kann durchaus einen störenden Charakter entwickeln. Zumindest wenn Nutzer*innen der Funktion keinen großen Wert beimessen. Das andere dagegen ist auf den ersten Blick eigentlich recht nützlich.

#1 iPhone-Einstellung Autoplay bei Videos

Das Autoplay-Feature dürftest du eher selten brauchen. In Apps sozialer Medien wie Facebook, Instagram oder Twitter werden Video und GIFs damit automatisch abgespielt, ob du willst oder nicht. Das verbraucht unnötig Datenvolumen, wenn du dich nicht im WLAN befindest. Und sobald du deine Daten-Flatrate für den Monat ausgeschöpft hast, drosselt dein Anbieter die Surfgeschwindigkeit erheblich.

Calderon rät aber nicht nur deshalb von einer zu intensiven Nutzung des Features ab. Denn gerade wenn Videos zum Abspielen bereit stehen, kann das dein iPhone insgesamt in seiner Performance verlangsamen. Auch verbraucht es deutlich mehr Energie, Videos und Co. zu streamen, was wiederum deinen Akku beeinträchtigt.Willst etwas an der iPhone-Einstellung ändern, kannst du das indirekt zunächst über diesen Pfad. Er sorgt dafür, dass Videos im mobilen Netz nicht mehr automatisch abgespielt werden. Nötig ist das allerdings nur, falls du die Funktion bereits ausgestellt hattest, denn die „WLAN-Unterstützung“ ist laut Apple standardmäßig aktiviert.

Anleitung: Einstellungen > Mobiles Netz/Mobile Daten > WLAN-Unterstützung

Auf anderem Wege ist das auch in den Apps selbst möglich. So lässt sich bei Facebook und Twitter in den Einstellungen festlegen, dass Videos nur durch Antippen aktiviert werden. Bei Instagram dagegen kannst du lediglich anpassen, dass Video sich im mobilen Netz langsamer laden.

#2 iPhone-Einstellung Handoff

Diese Funktion erlaubt es dir, auf dem iPhone mit etwas zu beginnen und damit dann zu einem anderen Gerät in deiner Nähe, wie deinem MacBook, iPad oder iPod touch, zu wechseln. Wie Apple erkärt: „Du kannst z.B. auf dem iPad beginnen, eine E-Mail zu beantworten, und sie dann in Mail auf dem Mac zu Ende schreiben. Du kannst Handoff mit vielen Apple-Apps verwenden, z. B.’Kalender‘, ‚Kontakte‘ und Safari. Unter Umständen funktioniert Handoff auch mit Apps von Drittanbietern.“Laut Calderon kann das Feature zwar hilfreich sein. Dennoch „kann es dein iPhone langsamer machen, wenn du Handoff viel nutzt“, erklärt er weiter. Um es auszuschalten, kannst du folgendermaßen vorgehen:

Anleitung: Einstellungen > Allgemein > AirPlay & Handoff

Quelle: https://www.futurezone.de/digital-life/article396328/iphone-einstellungen-ratschlaege-fachmann.html

9) Samsung-Handy zu lahm? So einfach macht ihr euer Smartphone schneller

Nicht immer laufen Samsung-Handys auch wirklich flüssig. Unnötige Ruckler und Verzögerungen der Oberfläche schmälern die Freude am Smartphone etwas. Doch mit nur einer Einstellung könnt ihr die Leistung gefühlt deutlich steigern. Im Video zeigen wir euch, wie es funktioniert.

Das genannte Video ist über den u.g. Link abrufbar.

Samsung-Smartphone einfach schneller machen

Wer sich ein Samsung-Smartphone kauft, erwartet eigentlich, dass das Gerät schnell und flüssig läuft. Dabei hat man selbst bei den schnellsten Top-Smartphone gesehen, dass das nicht immer der Fall ist – obwohl die Leistung eigentlich ausreichen müsste. Wenn ihr nicht auf ein Software-Update von Samsung warten wollt, welches die Probleme mit der Performance behebt, oder ein älteres Modell besitzt, das generell nicht mehr so flott unterwegs ist, dann könnt ihr **eine Einstellung ändern** und die Leistung so erhöhen.

Das Problem bei Samsung-Smartphones sind die Animationen. Wenn die Software richtig funktioniert, dann läuft das Smartphone eigentlich flüssig. Ab und zu ist das aber nicht der Fall und dann sorgen die ruckelnden Animationen für ein unschönes Bild. Das merke ich aktuell beim Galaxy A54. Obwohl die Leistung da sein müsste, fühlt sich das Smartphone durch die unrunden Animationen beim Schließen oder Öffnen von Apps, dem Wechsel zwischen Inhalten und so weiter etwas schwach an. **Dafür gibt es eine Lösung**.

Animationen bei Samsung-Handys ausschalten

Ihr könnt die Animationen nämlich einfach ausschalten. Wenn ihr also eines der Samsung-Smartphones besitzt, bei dem die Animationen nicht flüssig laufen, dann könnt ihr die Leistung dadurch erhöhen.

Dazu müsst ihr wie folgt vorgehen:

1. Einstellungen
2. Eingabehilfe
3. Verbesserung der Sichtbarkeit
4. Animationen entfernen

Wenn ihr diese Einstellung aktiviert, dann sind die Animationen auf eurem Samsung-Handy komplett deaktiviert. Das merkt ihr dann sofort. Egal ob ihr zurück geht, eine App schließt, die Kamera öffnet oder den Auslöser beim Fotografieren drückt. Die Animationen sind weg und alles passiert sofort. Das erhöht die Leistung spürbar, **man muss sich aber auch etwas daran gewöhnen**. Denn besonders beim Auslösen in der Kamera fehlt etwas die Animation. So zackig habt ihr euer Handy aber noch nie erlebt.

Hinweis: Die Funktion ist nicht hundertprozentig fehlerfrei. Es kann vorkommen, dass es in bestimmten Apps zu Problemen kommt. Dann müsst ihr die Animationen wieder einschalten und könnt diesen Trick leider nicht verwenden.

Quuelle: https://www.giga.de/news/samsung-handy-zu-lahm-so-einfach-macht-ihr-euer-smartphone-schneller/?utm_content=topic%2Fde-technologie&utm_source=flipboard

10) Horror: Über 90 Viren-verseuchte Android-Apps auf Google Play – über 5,5 Millionen Downloads

In den letzten Monaten haben Android-Nutzer über 5,5 Millionen Mal Viren-verseuchte Android-Apps von Google Play heruntergeladen. Besonders ein Banking-Trojaner ist gefährlich. Auch deutsche Nutzer sind gefährdet.

Sicherheitsexperten haben über 90 Android-Apps auf Google Play, dem offiziellen Download-Store für Android-Apps, gefunden, die mit Malware verseucht waren. Android-Nutzer haben diese gefährlichen Apps über 5,5 Millionen Mal auf Android-Geräten installiert. Vor allem der Banking-Trojaner “Anatsa” alias “Teabot” (ein alter Bekannter, der schon länger auch Android-Nutzer in Deutschland im Visier hat) spielt dabei eine unrühmliche, wichtige Rolle.

Test: Die besten Antivirus-Programme für Android

Anatsa greift über 650 Apps von Finanzinstituten an. Dabei handelt es sich um Banken aus Europa (auch um Banken aus Deutschland), den USA und Asien. Der Trojaner versucht die Zugangsdaten für das Online-Banking zu stehlen und damit betrügerische Bank-Transaktionen vorzunehmen. Anatsa versteckt sich dabei in unterschiedlichen Apps, die sich als Produktivitätstools ausgeben. Bereits im Februar 2024 hatte Anatsa mit dieser Tarnung mindestens 150.000 Infektionen über Google Play erzielt. Eine ausführliche Analyse dieser damaligen Angriffe lesen Sie hier.

Jetzt im Mai 2024 gelang Anatsa erneut der Einbruch in Google Play, wie Sie in diesem Dokument von Zscaler nachlesen können. Cybergangster verbreiten den Banking-Trojaner, der auch auf Anwender aus Deutschland abzielt, über die harmlos und nützlich klingenden Apps “PDF Reader & File Manager” und “QR Reader & File Manager”, wie das englischsprachige IT-Sicherheitsportal Bleepingcomputer berichtet. Zu dem Zeitpunkt, an dem das Sicherheitsunternehmen Zscaler seine Untersuchung vorgenommen hat, hatten Anwender diese beiden verseuchten Apps rund 70.000 Mal auf ihren Geräten installiert.

Anatsa entgeht der Malware-Erkennung von Google, indem es seine schädlichen Bestandteile in mehreren Stufen nachlädt. Zunächst ruft die Dropper-App die Konfiguration und wichtige Zeichenfolgen von den Command-and-Control-Servern der Hacker ab. Dann lädt die App die DEX-Datei mit dem bösartigen Dropper-Code heruntergeladen und aktiviert diesen auf dem Android-Gerät. Anschließend lädt die App die Konfigurationsdatei mit der Anatsa-Payload-URL herunter. Schließlich holt und installiert die DEX-Datei die eigentliche Malware als APK-Datei und schließt damit den Infektionsvorgang ab. Die DEX-Datei prüft zudem, dass die Malware nicht in Sandboxen oder innerhalb von Emulationen ausgeführt wird, wo sie wirkungslos bleiben würde.

Sobald Anatsa auf dem neu infizierten Androiden läuft, lädt es die Bot-Konfiguration und die Ergebnisse der App-Scans auf die Server hoch und lädt dann die gezielten “Injektionen” herunter, die dem Standort und dem Profil des Opfergeräts entsprechen.

Anatsa ist wie gesagt nur eine Malware, die aktuell besonders auf Google Play aktiv ist. Insgesamt fanden die Sicherheitsexperten über 90 verseuchte Apps (deren Namen veröffentlichten die Sicherheitsforscher nicht), die Android-Nutzer über 5,5 Millionen Mal installiert haben. Diese Apps tarnen sich als Tools, Personalisierungs-Apps, Fotografie-Utilities, Produktivitäts- sowie Gesundheits- und Fitness-Apps.

Google hat die infizierten Apps mittlerweile von Google Play entfernt.

So schützen Sie sich

Grundsätzlich sollten Sie Android-Apps nur von Google Play herunterladen und andere Download-Angebote vermeiden – auch wenn in dem hier geschilderten Fall die Hacker die Sicherheitsmechanismen von Google austricksen konnten. Lesen Sie sich vor jedem Download die Berechtigungen durch, die eine App auf Ihrem Gerät beansprucht. Hinterfragen Sie kritisch, ob diese Berechtigungen Sinn ergeben oder ob sie zu weit gehen.

Sie sollten zudem einen Virenscanner auf Ihrem Android-Gerät installieren. Eine bewährte Auswahl stellen wir in Test: Die besten Antivirus-Programme für Android vor.

TiPP:

- Gefahr für Android-Nutzer: Banking-Trojaner stiehlt Zugangsdaten und trickst Google Play aus
- Banking-Trojaner stiehlt Bankdaten deutscher Nutzer

Quelle: https://www.pcwelt.de/article/2348922/malware-android-apps-google-play.html

11) Gefahr durch WhatsApp-Klon: Diese 5 Fake-App stehlen eure Passwörter

Derzeit verwenden Cyberkriminelle Imitate von populären Apps wie WhatsApp, um an eure Login-Daten zu gelangen. So erkennt ihr die gefährlichen Fälschungen rechtzeitig.

Cyberkriminelle kennen viele Wege, um an eure persönlichen Daten zu gelangen. Fast täglich müsst ihr euch mit Phishing-Mails im Namen von Banken oder lästigen Spam-Anrufen herumschlagen. Habt ihr jedoch ein Auge für die Betrugsmaschen entwickelt und wisst, welche Indizien sie entlarven, ist es relativ leicht sie zu erkennen. Bei Fake-Apps sieht das jedoch anders aus.

Mit Malware infizierte Software macht auf den ersten Blick oft einen seriösen Eindruck. Zudem schaffen es die Betrüger immer wieder, die Schadsoftware in den Google Play Store einzuschmuggeln, der eigentlich als sichere Bezugsquelle gilt. Auch machen die Cyberkriminellen den Besitzerinnen und Besitzern von Android-Geräten auf diese Weise zu schaffen.

Sicherheitsexperten von Sonicwall Capture Labs sind auf fünf gefährliche Apps gestoßen, die sich als beleibte Software ausgeben. Darunter auch der Messenger WhatsApp. Ziel der Cyberattacke sind vor allem eure Passwörter. Um an diese zu gelangen, wird ein simpler Trick angewandt.

Diese Apps sind nicht, was sie scheinen

Um euch zum Download der bösartigen Apps zu bewegen, verpassen die Kriminellen ihnen einen neuen Anstrich. Dabei greifen sie für die Icons auf die Optik von populären Anwendungen zurück. Es macht anschließend teilweise den Anschein, als handle es sich um die echte Software.

Einige Icons können jedoch sofort als Fälschung enttarnt werden, wenn das Original euch bekannt ist. Die betroffenen fünf Fake-Apps imitieren Instagram, Snapchat, WhatsApp, Google und X (ehemals Twitter).

Einige der Fake-Apps könnt ihr schon am Icon erkennen. (Quelle: Sonicwall Capture Labs)

Funktioniert die Täuschung und ihr ladet eine der Apps herunter, wird zunächst die Berechtigung "Geräteverwaltung" und "Bedienungshilfen" eingefordert. Hier sollten bereits die Alarmglocken läuten. Denn diese Herangehensweise ist nicht normal. Mit der Berechtigung können Anwendungen nämlich Einstellungen auf eurem Smartphone ohne euer Zutun verändern. Genau das ist auch der Plan der integrierten Malware.

So gelingt der Datendiebstahl

Mit eurer Zugriffsbestätigung kann die Schadsoftware die Kontrolle über euer Smartphone oder Tablet übernehmen. Dabei sammelt sie sensible Informationen über euch. Zudem baut sie über einen Server eine Verbindung zu den Cyberkriminellen und wartet auf weitere Befehle.

Auf Anweisung kann die Malware eure Chats, Anruflisten und Kontakte an die Betrüger weiterleiten. Auch das Versenden von Fake-Nachrichten und Aufrufen von Phishing-Seiten ist für die bösartige Software kein Problem. Auf diese Weise gelangen die Verbrecher auch an eure Login-Daten.

Die Malware leitet euch mithilfe falscher html-Dateien auf Seiten von Instagram, PayPal, Netflix, Facebook oder auch Microsoft. Es wird sofort ein Anmeldefenster geöffnet, in dem ihr eure Zugangsdaten eingeben sollt. In Wahrheit handelt es sich jedoch um eine Fälschung. Gebt ihr eure Daten ein, werden sie unmittelbar an die Cyberkriminellen weitergeleitet.

Die Malware leitet euch mithilfe falscher html-Dateien auf Seiten von Instagram, PayPal, Netflix, Facebook oder auch Microsoft. Es wird sofort ein Anmeldefenster geöffnet, in dem ihr eure Zugangsdaten eingeben sollt. In Wahrheit handelt es sich jedoch um eine Fälschung. Gebt ihr eure Daten ein, werden sie unmittelbar an die Cyberkriminellen weitergeleitet.

Danach ist es ein leichtes für sie eure Accounts zu übernehmen. So fallen den Betrügern hochsensible Daten in die Hände. Die Folgen können großer finanzieller Schaden und Identitätsdiebstahl sein.

So schützt ihr euch

Die Verbreitungsmethode der fünf Fake-Apps ist laut den Sicherheitsforschern bislang nicht bekannt. Gerade deswegen sind die richtigen Schutzmaßnahmen enorm wichtig. Wollt ihr eine App für euer Android-Gerät herunterladen, solltet ihr stets eine vertrauenswürdige Quelle nutzen. Bei Downloads außerhalb des offiziellen Google Plays Stores raten wir daher zu extremer Vorsicht.

Allerdings ist auch der App Store von Google kein Garant für sichere Software. Immer wieder tauchen auch dort Programme auf, die mit Malware infiziert sind. Achtet daher immer genau auf den Namen der App, den Hersteller sowie die Bewertung und Kommentare. Auch die fünf Fake-Apps könnt ihr so erkennen. Der Instagram-Klon wird beispielsweise unter dem Namen "Instagram indo" verbreitet.

Damit euer Konto nicht direkt von Cyberkriminellen übernommen werden kann, wenn ihr auf eine Phishing-Masche hereinfallt, solltet ihr zudem unbedingt die Zwei-Faktor-Authentifizierung bei allen Konto einrichten, wo es möglich ist. Da diese Malware jedoch Zugriff auf eure Nachrichten hat, könnte sie das Sicherheitssystem aushebeln.

Wir raten euch, euer mobiles Gerät nach den betroffenen Apps zu durchsuchen und sie sofort zu löschen. Ein Antivirenprogramm kann eine große Hilfe dabei sein, sie ausfindig zu machen und euch auch künftig zu schützen. Befand sich tatsächlich eine der Anwendungen auf eurem Handy, solltet ihr zudem umgehend all eure Passwörter ändern.

Quelle: https://www.netzwelt.de/news/231361-gefahr-whatsapp-klon-5--fake-apps-stehlen-passwoerter1906.html#utm_source=newsshowcase&utm_medium=gnews&utm_campaign=CDAqDggAKgYICjD0umIw_v0NMOis1gI&utm_content=bullets&gaa_at=la&gaa_n=ARTJ-U_tCtJ6YeggbiMWiZKHfThF84lVnAsTrP5o6gHjCDyET9n8ttorU9UkDbmNyTBkcAK6TosHG_dejC6t&gaa_ts=665839f6&gaa_sig=mPbAydEXwKD73jQG-K9E3_fDOaV_frNtwYtSQSIcWkHC8OgXQk_f_JtVkADXfuKox4P1JaMkg-3Uvp8ETiMB3w%3D%3D

12) WLAN-Sicherheit: 7 Tipps, um euer Heimnetzwerk vor Hackern zu schützen

Obwohl unsere heimischen Router mit Passwörtern geschützt sind, können sich Unbefugte darauf Zugriff verschaffen. Zumindest dann, wenn einige Sicherheitstipps nicht eingehalten und die Standardeinstellungen nicht geändert werden.

Wer in einem Mehrfamilienhaus wohnt, kennt die Situation: Sucht ihr mit einem Smartphone oder einem Laptop nach einer WLAN-Verbindung, gibt es viele verschiedene Treffer. Neben eurem eigenen Anschluss könnt ihr auch die Router der anderen Hausbewohner:innen sehen. Im Umkehrschluss heißt das aber auch, dass Fremde euer Wi-Fi-Signal sehen können.

Im Normalfall klickt ihr auf eure Verbindung und schenkt den anderen keine Beachtung. Was aber, wenn jemand versucht, auf euer WLAN-Signal zuzugreifen und sich so Zutritt zu eurem Netzwerk zu verschaffen? In vielen Fällen geht das schneller als gedacht, weil nur wenige die Standardeinstellungen des Routers anpassen.

Wenn jemand in euer Netzwerk gelangt, können schnell Daten abhandenkommen. Um das zu verhindern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Leitfaden für ein sicheres Heimnetzwerk herausgegeben. Die wichtigsten Tipps und was ihr sonst noch dabei beachten solltet, fassen wir hier für euch zusammen.

Passwort und Name des Routers ändern

Bekommt ihr einen neuen Router, hat dieser zunächst einen Standardnamen, über den ihr ihn im Netzwerk erkennt. Meist ist das die Modellbezeichnung des Routers sowie ein Zahlen- oder Buchstabenkürzel, um ihn von gleichen Modellen in Reichweite abzuheben. Allerdings gibt dieser Name schon Infos über euer Netzwerk preis. Hacker:innen sehen so auf Anhieb, welches Routermodell ihr nutzt und könnten etwaige Schwachstellen ausnutzen.

Auch der Login, den ihr für euren Router bekommen habt, kann eine solche Schwachstelle sein. Hier meinen wir die Daten, mit denen ihr auf Einstellungen des Routers zugreifen

könnt. In vielen Fällen ist der Nutzername standardmäßig auf „admin“ festgelegt und wird von einem unsicheren Passwort begleitet, das sich leicht knacken lässt.

Bekommen Hacker:innen also die Info, welchen Router ihr nutzt, und wissen, welche Standard-Logins dafür genutzt werden, könnten sie direkt auf das Gerät zugreifen. Ändert also Namen und Login schnellstmöglich nach Erwerb des Routers. Beides könnt ihr in den Einstellungen eures Routers anpassen. Schlagt einfach im Handbuch des Geräts nach, wo sich die entsprechende Option befindet.

WLAN-Passwort möglichst komplex halten

Damit ihr euch in euer WLAN einwählen könnt, braucht es ebenfalls ein Passwort. Das besteht meist aus einer langen Zahlenfolge, die vom Hersteller für jeden einzelnen Router generiert wurde. Auch wenn die Passwörter sich nicht mit anderen Geräten überschneiden, können sie deutlich einfacher geknackt werden als komplexe Passwörter.

Das BSI empfiehlt deshalb eine Passwortlänge von mindestens 20 Zeichen. Diese sollten zudem keinen Zusammenhang haben. Heißt: keine Wörter innerhalb des Passworts, sondern einzelne Buchstaben, Zahlen und Sonderzeichen. Wer sich diese Passwörter nicht merken kann, sollte auf einen Passwortmanager zurückgreifen, in dem der Login sicher verwahrt werden kann.

Aktuelle Verschlüsselungsstandards nutzen

In vielen Routern könnt ihr auswählen, welcher Verschlüsselungsstandard genutzt werden soll, um euer WLAN vor unbefugten Zugriffen zu bewahren. Die aktuellsten Standards sind dabei WPA2 und WPA3. Letzterer ist dabei die sicherste Netzwerkverschlüsselung und sollte immer präferiert werden.

Das sollte gerade bei neuen Routern kein Problem sein, da diese häufig WPA3 unterstützen. Solltet ihr einen älteren Router haben, stellt sicher, dass dieser wenigstens WPA2 unterstützt. Entsprechende Informationen findet ihr ebenfalls in der Benutzeroberfläche des Routers unter „WLAN“. Sucht dort nach einem Punkt namens „Sicherheit“ oder einer Option, die ähnlich benannt ist. Bietet euer Router kein WPA2 oder WPA3, solltet ihr auf ein neueres Modell umsteigen.

Die Firewall regelmäßig überprüfen

Die Firewall eures Routers schützt euer Netzwerk vor Einflüssen von außen. Heißt: Sämtlicher Traffic, der zwischen eurem Netzwerk und dem Internet entsteht, muss erst durch diese Schutzbarriere. In einigen Fällen greift die Firewall ein und blockiert den Zugang. So kann niemand einfach auf euer Netzwerk zugreifen.

Damit das so bleibt, solltet ihr regelmäßig nachschauen, ob die Firewall aktiviert ist. Ihr findet die entsprechenden Einstellungen in der Benutzeroberfläche eures Routers. Schaut zudem unter „Internet“ nach sogenannten „Freigaben“. Dabei handelt es sich um Ausnahmen, die eure Firewall nicht blockiert. Solche Freigaben braucht ihr nur in Spezialfällen. Wenn niemand Zugriff auf euer Netzwerk haben soll, dann sollten dort keine aktiven Freigaben stehen.

Den Router mit Updates aktuell halten

Die Sicherheit eures Netzwerkes ist nur so gut wie das schwächste Glied. Gelegentlich können sich Sicherheitslücken auch bei Routern einschleichen. Diese könnten Angreifer:innen dann etwa nutzen, um sich unbemerkt Zugang zu eurem WLAN zu verschaffen.

Um das zu verhindern, solltet ihr regelmäßig Updates für euren Router durchführen. Viele Geräte haben eine automatische Update-Funktion, die ihr im Reiter „System“ der Benutzeroberfläche aktivieren könnt. Wählt dafür aber einen Zeitpunkt, an dem ihr das WLAN definitiv nicht nutzt – etwa in der Nacht. Denn durch das Update könnte der Router neu starten und dadurch kurz das WLAN abreißen.

Fernzugriff deaktivieren

Über den Fernzugriff könnt ihr auch auf euer Netzwerk zugreifen, wenn ihr gerade unterwegs seid. So könnt ihr etwa noch eine wichtige Datei aufrufen, die sich auf einem USB-Stick befindet, der am Router angeschlossen ist. Das kann zwar nützlich sein, ist aber auch ein Sicherheitsrisiko.

Das BSI rät deshalb, diese Funktion nicht dauerhaft zu aktivieren. Schaltet den Fernzugriff aus, wenn ihr ihn in absehbarer Zeit nicht benötigt. Die entsprechende Einstellung findet ihr in Bereichen wie „Sicherheit“ oder „Internet“. Deaktiviert dort Optionen wie „Internetzugriff“ oder „Fernzugriff“.

Ein Gastnetzwerk für Gäste

Viele kennen die Situation: Kommt Besuch in die Wohnung, fragen einige direkt nach dem WLAN-Passwort, um nicht das mobile Datenvolumen zu verbrauchen. Zudem sind die heimischen Anschlüsse meist schneller. Wer Gästen erlaubt, sich mit dem Hauptnetzwerk zu verbinden, bringt es in Gefahr. Denn befinden sich auf den Endgeräten der Besucher:innen Viren oder andere schädliche Dateien, könnten die über das WLAN in euer Netzwerk gelangen.

Deshalb bieten zahlreiche Router einen sogenannten Gastzugang. Dieses Netzwerk ist vom Hauptnetzwerk getrennt, bietet aber dieselbe Geschwindigkeit und einfache Verbindung. Die Einstellung dazu findet ihr meist im Abschnitt „WLAN“ eures Routers. Dort könnt ihr einen Namen und ein Passwort für das Netzwerk festlegen. Manche Router können sogar einen QR-Code generieren, über den sich Gäste noch schneller im Gastnetzwerk anmelden können.

Quelle: https://t3n.de/news/wlan-sicherheit-heimnetzwerk-schuetzen-hacker-1625501/?utm_source=flipboard&utm_content=topic%2Fde-technologie

13) Achtung: Microsoft aktiviert dieses Feature in Windows 11, ohne Sie zu fragen

Offenbar möchte Microsoft, dass Sie Ihre Ordner und Dateien mit OneDrive sichern. Unbedingt. Denn die Funktion wird jetzt ohne Erlaubnis aktiviert.

Microsoft hat eine etwas fragwürdige Änderung in Windows 11 vorgenommen, die Nutzerinnen und Nutzern die Entscheidungsfreiheit in Bezug auf eine bestimmte Funktion nimmt. Ohne vorherige Ankündigung oder Erklärung wird nun die automatische Ordnersicherung mit OneDrive aktiviert, wenn Sie einen neuen Rechner einrichten. Und zwar, ohne den User um Erlaubnis zu bitten.

Wer einen neuen Windows-Computer einrichtet, während er mit dem Internet verbunden ist und ein Microsoft-Konto nutzt, findet auf seinem Desktop wie gehabt OneDrive vor. Das Programm synchronisiert Daten aus Ordnern wie Desktop-Bilder, Dokumente, Musik und Videos, was in bestimmten Fällen sehr nützlich sein kann.

Im schlimmsten Fall kann es aber passieren, dass Sie Windows neu aufsetzen oder einrichten und sofort mit einem Desktop konfrontiert werden, der mit Ordnern und Dateien zugemüllt ist. Das dürfte bei vielen für Frust sorgen.

Bisher musste man die automatische Ordnersicherung bewusst aktivieren. Zudem richtete Microsoft immer wiederkehrende Benachrichtigungen ein, um an das Feature zu erinnern. Mittlerweile scheint das Unternehmen aber einfach anzunehmen, dass jeder OneDrive standardmäßig aktiviert haben muss, um ausnahmslos alle Daten zu sichern.

Den meisten dürfte das nicht einmal auffallen, bis Sie einen neuen Rechner einrichten und plötzlich sämtliche alte Dateien wiederfinden.

So deaktivieren Sie das OneDrive-Backup

Wenn Sie nicht möchten, dass Ihr Computer mit OneDrive alles auf Ihrem Desktop oder in anderen Ordnern sichert, können Sie die Funktion wieder deaktivieren.

Klicken Sie hierfür mit der rechten Maustaste auf das OneDrive-Symbol unten rechts im Infobereich Ihrer Taskleiste. Falls Sie das Symbol nicht direkt finden, müssen Sie eventuell das Feld aufklappen. Gehen Sie dann auf das Einstellungsrädchen und wählen **Einstellungen**.

Unter dem Punkt **Synchronisierung und Sicherung** wählen Sie dann **Sicherung verwalten** aus. Deaktivieren Sie nun alle Ordner, die Sie nicht in OneDrive sichern möchten, und bestätigen Sie die Änderungen.

Falls Sie eine ältere OneDrive-Version mit der klassischen Oberfläche mit Registerkarten haben, gehen Sie zur Registerkarte **Sicherung** und klicken Sie auf **Sicherung verwalten** und schließlich **Sicherung anhalten**. Die Einstellung müssen Sie noch einmal bestätigen.

Alternativ können Sie OneDrive natürlich auch einfach deinstallieren, falls Sie die Backups gar nicht nutzen wollen. Das wäre die einfachste Lösung, dürfte Microsoft aber gar nicht schmecken.

Quelle: https://www.pcwelt.de/article/2376191/microsoft-onedrive-backup-aktiviert-ohne-erlaubnis.html?utm_date=20240626121045&utm_campaign=Best-of%20PC-WELT&utm_content=Title%20Story%3A%20Achtung%3A%20Microsoft%20aktiviert%20dieses%20Feature%20in%20Windows%2011%2C%20ohne%20Sie%20zu%20fragen&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

14) Sofort aktualisieren: Kritische Sicherheitslücke bei WLAN-Routern entdeckt

Wer einen ASUS-WLAN-Router nutzt, sollte jetzt schnell aktiv werden. Der Hersteller meldet nämlich eine kritische Sicherheitslücke, die es Fremden erlaubt, sich aus der Ferne auf den Geräten einzuloggen.

WLAN-Router sind das Herzstück für die heimische Internet-Verbindung. Gleichzeitig müssen Nutzer die Geräte aber auch optimal vor Angreifern schützen. Asus vermeldet jetzt eine kritische Sicherheitslücke, die sieben WLAN-Router-Modelle betrifft.

Gebündelt sind die Erkenntnisse zum Problem unter CVE-2024-3080. Auf den unten genannten WLAN-Router-Modellen von Asus lässt sich die Authentifizierung umgehen, sodass sich unter Umständen auch Fremde auf den Geräten anmelden können.

Besonders brisant ist das deshalb, weil Angreifer nicht in WLAN-Reichweite sein müssen. Die Angriffe funktionieren auch aus dem Internet, wenn der WLAN-Router von außen erreichbar ist.

Die gute Nachricht: Asus hält für das Problem Sicherheitsupdates bereit, die Nutzer möglichst schnell einspielen sollten. Außerdem gibt der Hersteller noch weitere Empfehlungen für betroffene Nutzer.

Diese Asus-Router sollten Sie schnell updaten

Asus erklärt, dass sieben Router-Modelle von der Schwachstelle betroffen sind. Nutzer sollten schnellstmöglich ein Firmware-Update einspielen:

- **ZenWiFi XT8:** anfällig sind Version 3.0.0.4.388_24609 und älter
- **ZenWiFi XT8 v2:** anfällig sind Version 3.0.0.4.388_24609 und älter
- **RT-AX88U:** anfällig sind Version 3.0.0.4.388_24198 und älter
- **RT-AX58U:** anfällig sind Version 3.0.0.4.388_23925 und älter
- **RT-AX57:** anfällig sind Version 3.0.0.4.386_52294 und älter
- **RT-AC86U:** anfällig sind Version 3.0.0.4.386_51915 und älter
- **RT-AC68U:** anfällig sind Version 3.0.0.4.386_51668 und älter

Was Asus-Nutzer noch beachten sollten

Am wichtigsten ist das Einspielen der Software-Updates. Asus rät betroffenen Nutzern aber auch noch zu diesen Schritten:

- **Verschiedene Passwörter:** Nutzer sollten verschiedene Passwörter für WLAN und Router-Oberfläche einstellen.
- **Mindestlänge:** Passwörter sollten laut Asus mindestens 10 Zeichen umfassen und ein Mix aus Großbuchstaben, Nummern und Sonderzeichen sind. Außerdem sollten Nutzer das gleiche Passwort nicht für mehrere Geräte oder Dienste nutzen.
- **Abschotten:** Sollte sich die Firmware nicht aktualisieren lassen, rät Asus dazu, alle aus dem Internet erreichbaren Dienste auf dem WLAN-Router abzuschalten, gemeint sind Einstellungen rund um Port-Forwarding oder VPN-Server.

Anmerkung der Redaktion: Die Up-Date-Möglichkeit besteht unter dem u.g. Link

Quelle: https://www.chip.de/news/Sofort-aktualisieren-Kritische-Sicherheitsluecke-bei-WLAN-Routern-entdeckt_185324857.html?utm_source=chip_1001311&utm_medium=email&utm_campaign=1013991&utm_content=26.06.2024

15) So einfach und schnell laden Sie YouTube-Videos kostenlos herunter

Bei YouTube gibt es Millionen Videos – von kurzen Clips bis zu Spielfilmen ist alles dabei. Schnell und einfach laden Sie die Videos mit dem Programm 4K Video Downloader+ auf ihren PC.

YouTube ist die größte und beliebteste Video-Plattform im Internet. Schätzungen zufolge soll es hier mehr als 800 Millionen Videos geben und täglich kommen Tausende hinzu. Hier finden Sie Videos zu allen erdenklichen Themen, von Musik über Gaming bis hin zu Wissenschaft und Bildung. Sogar ganze Spielfilme lassen sich abrufen. Es gibt viele gute Gründe, täglich die YouTube-Webseite zu besuchen oder die YouTube-App auf dem Smartphone oder Tablet zu starten.

Sie werden garantiert Inhalte finden, die Sie dauerhaft auf Ihrem PC, einem NAS oder in der Cloud speichern wollen, um sie jederzeit mit einem Videoplayer anzusehen – auch ohne Internetverbindung im Urlaub oder auf Reise. YouTube selbst bietet keine passende Download-Funktion. Gut, dass es mit dem 4K Video Downloader+ eine entsprechende

Software gibt, die schnell und zuverlässig arbeitet.

Mit der kostenlosen Desktop-Software für Windows, Mac-OS und Linux laden Sie schnell und einfach Videos von Streaming-Seiten herunter. Unterstützt werden neben YouTube auch TikTok, Vimeo, Facebook, Twitch und einige andere mehr.

Das Beste daran: Die Nutzung der deutschsprachigen Software ist völlig kostenfrei. Sie müssen nur das Programm herunterladen und auf Ihrem Windows-PC installieren. Anschließend lassen sich Videos im MP4- oder MKV-Format mit einer Auflösung von bis zu 8K herunterladen. Dabei können Sie die Qualität und Extras der Videos auch individuell festlegen – also etwa Codec, Bildrate und Untertitel auswählen.

Videos mit 4K Video Downloader+ herunterladen

Im Programmfenster der Software gibt es mehrere Optionen, um ein gewünschtes Video zu laden. Wahrscheinlich werden Sie aus Gewohnheit die folgende Vorgehensweise bevorzugen:

Sie haben die YouTube-Webseite im Browser geöffnet und spielen etwa ein Musikvideo ab. Markieren Sie mit der Maus die vollständige Webadresse (URL) und übernehmen Sie sie mit der Tastenkombination Strg-C in die Zwischenablage von Windows. Wechseln Sie zum aktiven 4K Video Downloader+ und klicken Sie hier auf den grünen Button „Link einfügen“. Die URL wird direkt übernommen und Sie haben mehrere Auswahlmöglichkeiten: Mit einem Klick auf „Das Video herunterladen“ starten Sie den direkten Download in das Verzeichnis „C:\Users\[Nutzer]Videos\4K Video Downloader+“.

Mehr Optionen haben Sie im „Erweiterten Modus“, den Sie auf Mausklick aktivieren. Dann startet der Download nicht automatisch: In einem neuen Fenster wählen Sie – sofern von YouTube unterstützt – die Qualität, den Codec, die Bildfrequenz und das Containerformat (MKV oder MP4) aus und gegebenenfalls noch Untertitel. Abweichend vom Standardausgabeverzeichnis stellen Sie mit einem Klick auf das Ordner-Symbol ein anderes Ziel ein.

Ein Klick auf die Schaltfläche „Herunterladen“ startet den Download. In echter Hochgeschwindigkeit wird das Video vom YouTube-Server geladen und ist oft schon Sekunden später lokal bei Ihnen verfügbar. Klicken Sie in der Liste auf den neuen Eintrag, um die Wiedergabe zu starten.

Von nützliche Extras profitieren

Ohne Umweg über den Webbrowser und die YouTube-Webseite lässt sich der 4K Video Downloader+ ebenfalls nutzen. Die Software besitzt nämlich praktischerweise einen eigenen Browser, mit dem Sie die gewünschten Inhalte bei YouTube und anderen Videoportalen finden können, ohne die App verlassen zu müssen. Laden Sie einfach alle gewünschten Inhalte herunter. Dazu wird im unteren Fensterbereich die grüne Schaltfläche „Herunterladen“ eingeblendet.

Doch der 4K Video Downloader+ kann tatsächlich noch einiges mehr und unterscheidet sich dadurch von vielen anderen Download-Tools. Sie können in den Programmeinstellungen (Klick auf das Zahnrad-Symbol) ein YouTube-Konto hinterlegen und auch das YouTube-Premium-Abo, um Videos mit Altersbeschränkung, Videos aus Ihrem persönlichen Bereich und HQ-Audio herunterladen. Dazu gehen Sie zu „Autorisierung“ und klicken auf „Anmelden“. Bestätigen Sie mit Ihrem Google-Konto und dem dazugehörigen Passwort und – falls eingerichtet – auch noch per Zwei-Faktor-Authentifizierung (2FA).

Dank dem intelligenten Modus, den Sie am oberen Bildschirmrand einschalten, werden die Downloads noch smarter. Alles, was Sie machen müssen: Legen Sie die Ihre persönlichen Qualitätseinstellungen einmal fest und der 4K Video Downloader+ wendet sie dann automatisch auf alle zukünftigen Downloads an.

Sie wollen Videos von bestimmten Anbietern oder Kanälen automatisch lassen? Auch dafür hat 4K Video Downloader+ eine passende Funktion an Bord: Sie wählen in Download-Fenster den Menüeintrag „Neue Videos abonnieren“. Fertig!

Das bietet die Premium-Version von 4K Video Downloader+

Sie können die Standardversion von 4K Video Downloader+ kostenlos nutzen, und das ohne Zeitbeschränkung. Allerdings ist die Gratisversion auf maximal 30 Downloads pro Tag, 10 Videos pro Playliste und fünf Videos pro Kanal beschränkt. Zudem ist es zwar möglich, Videos nacheinander, aber nicht parallel herunterzuladen.

Für die meisten Anwender sind die genannten Einschränkungen nicht hinderlich und auch so bietet der 4K Video Downloader+ schon mehr als andere kostenlose Download-Tools.

Stoßen Sie allerdings mit Ihrem Nutzungsverhalten an die Grenzen der Gratis-Version von 4K Video Downloader+, dann sollten Sie über den Kauf der Premium-Version nachdenken. Zur Auswahl stehen drei Stufen: Lite (17,85 Euro), Persönlich (29,75 Euro) und Pro (47,60 Euro).

Eine umfangreiche Übersicht über die angebotenen Funktionen und Hinweise zum Abonnement finden Sie hier.

Die Lizenzen „Lite“ (1-Jahres-Abo) und „Persönlich“ (Einmalkauf) bieten beide die gleichen Vorteile wie unbegrenzte Downloads in allen Kategorien und parallele Downloads von bis zu drei Videos.

Die Pro-Lizenz schaltet alle Funktionen dauerhaft frei und bietet zusätzlich zur „Persönlich“-Lizenz bis zu sieben parallele Downloads sowie weitere Extras: Sie können YouTube-Kanäle innerhalb der App abonnieren, so dass zukünftige Videos automatisch heruntergeladen werden. Unterstützt wird auch YouTube Premium HQ Audio.

Falls Sie die erweiterten Funktionen nicht benötigen, funktioniert die kostenlose Version großartig und zuverlässig – ganz ohne Wasserzeichen oder versteckten Einschränkungen.

Hier: 4K Video Downloader+ kostenlos downloaden

Quelle: https://www.pcwelt.de/article/2332674/so-einfach-und-schnell-laden-sie-youtube-videos-kostenlos-herunter.html?utm_date=20240626124458&utm_campaign=Best-of%20PC-WELT&utm_content=Position%20Two%20Title%3ASchneller%20geht%20es%20nicht%3A%204K%20Video%20Downloader%2B%20I%C3%A4dt%20YouTube-Videos%20herunterOrderNo%3A75522&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

16) Youtube bestätigt Zwangs-Kündigung von zu günstigen Premium-Abos

Jetzt ist es offiziell: Youtube wirft Premium-Nutzer raus, die sich ein günstiges Premium-Abo erschlichen haben. Die Kündigungswelle habe bereits begonnen.

Vor wenigen Tagen haben wir berichtet, dass Youtube gegen Nutzer vorgeht, die sich günstige Premium-Abonnements erschlichen haben, indem sie diese unter Benutzung von

VPN in Ländern abgeschlossen haben, in denen sie für das Premium-Abonnement viel weniger bezahlen müssen als in ihrem Heimatland. Mehr zu diesem neuen, harten Vorgehen von Youtube lesen Sie in Youtube kündigt Premium-Nutzern, die sich günstiges Abo erschlichen haben.

Das bedeutet, dass der folgende Trick vermutlich bald nicht mehr funktionieren dürfte: Youtube Premium für nur 1,47 statt 13,99 Euro monatlich mit diesem Trick – Sie sparen fast 90 Prozent. Doch bisher fehlte noch eine offizielle Bestätigung von Youtube zu der neuen, harten Vorgehensweise; die Berichterstattung darüber beruhte auf Informationen von betroffenen Nutzern, beispielsweise via Reddit. Doch jetzt liegt endlich eine offizielle Aussage von Youtube vor.

Denn die US-amerikanische Technik-Webseite Techcrunch zitiert einen Sprecher von Youtube zu dem neuen Kurs mit folgenden Worten:

> Um die genauesten Pläne und Angebote anbieten zu können, haben wir Systeme eingerichtet, um das Land unserer Nutzer zu ermitteln, sagte uns ein YouTube-Sprecher. In Fällen, in denen das Land der Anmeldung nicht mit dem Land übereinstimmt, in dem der Nutzer auf YouTube zugreift, bitten wir unsere Mitglieder, ihre Rechnungsdaten auf das Land ihres aktuellen Wohnsitzes zu aktualisieren.

Der Youtube-Sprecher vermeidet in diesem Zusammenhang zwar die Verwendung von Formulierungen, die man als Kündigung der betroffenen Youtube-Premium-Abonnements verstehen könnte. Ein anderer Google-Mitarbeiter dagegen soll gegenüber dem PCMag ausdrücklich von der “Stornierung von Premium-Mitgliedschaften für Konten” gesprochen haben”, bei denen gefälschte Länderangaben bei der Anmeldung festgestellt wurden”. Diesem Google-Mitarbeiter zufolge habe Youtube bereits mit der Kündigungswelle begonnen. Diese erfolge via Mail und über Informationen innerhalb der Youtube-App.

Quelle: https://www.pcwelt.de/article/2373823/youtube-bestaetigt-kuendigung-zu-guenstiger-premium-abonnements.html?utm_date=20240626130001&utm_campaign=Best-of%20PC-WELT&utm_content=Title%20Story%3A%20Youtube%20best%C3%A4tigt%20Zwangs-K%C3%BCndigung%20von%20zu%20g%C3%BCnstigen%20Premium-Abos&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

17) Die neuesten Sicherheits-Updates

Hier finden Sie aktuelle Sicherheits-Updates für die gängigsten Programme. Die Update-Tabelle wird regelmäßig aktualisiert und bei Bedarf erweitert.

Online-Kriminelle nutzen verstärkt Sicherheitslücken in beliebten Programmen aus, um auf diese Weise Schädlinge aller Art einzuschleusen. Die Software-Hersteller stellen Sicherheits-Updates bereit, um bekannt gewordene Lücken zu schließen. Überprüfen Sie daher regelmäßig, ob Ihre installierten Programme auf dem neuesten Stand sind. Die nachstehende Tabelle führt die jeweils neuesten Versionen derjenigen Programme auf, für die in letzter Zeit Sicherheits-Updates erschienen sind.

Die angegebene Risikostufe bezieht sich auf die Schwachstellen der jeweiligen Vorversion, die mit dem aktuellen Update beseitigt worden sind. Wenn Sie eine ältere Version dieser Software installiert haben, kann es durchaus sein, dass deren Risiko höher ist als hier angegeben. Wie Sie die Pflege Ihres Software-Bestands organisieren können, haben wir für Sie in unseren Ratgeber „Die besten Update-Manager“ untersucht.

Die neuesten Updates:
Brave, Chrome, Firefox, FritzOS, Opera, Vivaldi

Software	Version	Datum	Risiko	Download
7-Zip	24.07	19.06.2024	kein	PC-Welt
Acrobat Reader DC	24.002.20759 »Info	14.05.2024	hoch	PC-Welt
Android	Security Bulletin Juni 2024 für Android 12 bis 14	03.06.2024	hoch	Google
Brave Browser	1.67.123 »Info	25.06.2024	hoch	PC-Welt
Chrome	126.0.6478.126/127 »Info	24.06.2024	hoch	PC-Welt
Edge	126.0.2592.68 »Info	20.06.2024	hoch	Microsoft
FileZilla	3.67.0	15.04.2023	niedrig	PC-Welt
Firefox	127.0.2	25.06.2024	kein	PC-Welt
Foxit PDF Reader	2024.2.2	24.05.2024	hoch	PC-Welt
FritzOS (für FritzBox)	7.81 / 7.63 / 7.59 (div. Modelle: »Übersicht)	25.06.2024	kein	AVM
GIMP	2.10.38	05.05.2024	kein	PC-Welt
iCloud für Windows (UWP-App)	14.2.122.0	30.10.2023	kein	Microsoft Store
iOS / iPadOS 17	17.5.1	20.05.2024	kein	Apple
iOS / iPadOS 16	16.7.8	13.05.2024	**kritisch**	Apple
iOS / iPadOS 15	15.8.2	05.03.2024	kein	Apple
IrfanView	4.67	05.04.2024	kein	PC-Welt
iTunes	12.13.2	08.05.2024	hoch	PC-Welt
Java 8 Runtime (JRE)	Java 8 Update 411 (8u411) »Info	16.04.2024	hoch	PC-Welt
LibreOffice	24.2.4	06.06.2024	niedrig	PC-Welt
Microsoft Office	Patch Day Juni 2024 »Info	11.06.2024	hoch	Microsoft
mIRC	7.77	11.06.2024	niedrig	PC-Welt
OpenOffice	4.1.15	22.12.2023	hoch	PC-Welt

Software	Version	Datum	Risiko	Download
Opera One	111.0.5168.43	25.06.2024	kein	PC-Welt
Pegasus Mail	4.80	14.02.2022	niedrig	PC-Welt
PHP	8.3.8 / 8.2.20	06.06.2024	mittel	Hersteller
Seamonkey	2.53.18.2	28.03.2024	hoch	PC-Welt
Thunderbird	115.12.2	22.06.2024	kein	PC-Welt
Tor Browser	13.5	21.06.2024	kein	PC-Welt
VirtualBox	7.0.18 »Info	03.05.2024	kein	PC-Welt
Vivaldi	6.8.3381.46 »Info	25.06.2024	hoch	PC-Welt
VLC Media Player	3.0.21	10.06.2024	hoch	PC-Welt
VMware Workstation Pro/Player	17.5.2	14.05.2024	hoch	PC-Welt
Windows	Patch Day Juni 2024 »Info	11.06.2024	hoch	Microsoft
WinRAR	7.01	15.05.2024	kein	PC-Welt
WinSCP	6.3.4	17.06.2024	niedrig	PC-Welt
Wireshark	4.2.5	15.05.2024	mittel	PC-Welt
XnView	2.51.6	20.02.2024	hoch	PC-Welt
Zoom Client	6.1.0	17.06.2024	k. A.	Hersteller

Die neuesten Sicherheits-Updates für gängige Software

Risikostufen:

kritisch – Fernzugriff, Einschleusen und Ausführen von Code möglich; Exploit-Code ist öffentlich verfügbar und/oder Schwachstelle wird für Angriffe ausgenutzt („0-Day-Lücke“)

hoch – Fernzugriff, Einschleusen und Ausführen von Code möglich; keine Exploits oder Angriffe bekannt

mittel – Fernzugriff, Datenlecks, Absturz/DoS möglich, Krypto-Lücke

niedrig – lokale Rechteausweitung, Datenlecks möglich; oder neue Sicherheitsfunktion(en) eingebaut

kein – normale Fehlerbeseitigungen, kein Sicherheits-Update

k. A. – (noch) keine Angaben seitens des Herstellers

Die Einstufung kann von den Herstellerangaben abweichen. Ist Exploit-Code öffentlich verfügbar oder werden Schwachstellen aktiv ausgenutzt, erhöht sich die Einstufung des Risikos um eine Stufe (z. B.: aus *hoch* wird *kritisch*).

Quelle: https://www.pcwelt.de/article/1197811/die-neuesten-sicherheits-updates.html?utm_date=20240626130453&utm_campaign=Security&utm_content=First%20Description%20Story%3A%20Hacker%20aussperren%2C%20Luken%20dichtmachen%3A%20diese%20wichtigen%20Sicherheits-Updates%20sollten%20Sie%20auf%20keinen%20Fall%20verpassen%21&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

18) Warnung: BIOS-Update macht HP-Laptops unbrauchbar – Hersteller arbeitet an Lösung

In einem Forum des Notebook-Herstellers HP berichten zahlreiche Nutzer über BIOS-Probleme, die ihre Laptops seit Wochen unbenutzbar machen. Bisher gibt es keine Lösung.

Um Notebooks auf dem neuesten Stand zu halten, bringen Hersteller bekanntlich Treiber-Updates und neue BIOS-Versionen heraus, die Fehler korrigieren und Funktionen verbessern. So kann dafür gesorgt werden, dass Geräte länger nutzbar und optimal geschützt sind.

Bisweilen berichten Nutzerinnen und Nutzer allerdings über den gegenteiligen Effekt solcher Updates. So ist es aktuell auch beim Notebook-Hersteller HP der Fall. In dessen Forum häufen sich derzeit Berichte zu Laptops, die seit dem letzten BIOS-Update 1.17 im Mai nicht mehr nutzbar sind.

Betroffen sind wohl vor allem Business-Laptops wie HP-Probooks, doch auch die Elitebook-Serie und weitere Systeme kämpfen mit Abstürzen, Blackscreens und Freezes. Das sorgt für Frust bei vielen HP-Kunden, zumal der Hersteller das Problem bisher nicht lösen konnte.

Laptops sind seit Wochen unbenutzbar

Der erste Eintrag zu diesem Problem stammt vom 26. Mai 2024, ist also Stand heute über zwei Wochen alt. Weitere Postings von Betroffenen kamen immer wieder hinzu, wodurch die Zahl bekannter kaputter Systeme immer weiter ansteigt. Bisher gab es keine Antwort durch das Support-Team von HP in besagtem Forum, und das fehlerhafte BIOS-Update ist nach wie vor in Umlauf.

Gegenüber Windowsarea gab HP aber zumindest an, an einer Lösung zu arbeiten und in Kontakt mit Betroffenen zu stehen. Wer Probleme hat, soll sich an den Support von HP wenden.

Einige User erhielten das Update über den HP Support Assistant im Mai, bei anderen wurde die BIOS erst später per Windows Update aktualisiert.

Aktuell wird darüber gemutmaßt, warum das BIOS-Update bei so vielen Nutzern für Probleme sorgte. Vermutlich liegt es daran, dass HP hierbei keine Standard-UEFI-Datei lieferte, die vom System nicht verwendet werden kann. Zudem scheint die BIOS-Datei für die verbauten Chips zu groß zu sein.

Was können Sie tun?

Falls Sie einen HP-Laptop besitzen und das letzte BIOS-Update noch nicht erhalten haben, sollten Sie zum aktuellen Zeitpunkt darauf verzichten, es zu installieren. Ansonsten bleibt nicht viel übrig, als auf eine Antwort des Herstellers zu warten, damit das Problem gelöst werden kann.

Zwar könnten Programme wie NeoProgrammer dabei helfen, die UEFI-Datei korrekt auszulesen, wie etwa der Nutzer “ProBookUser61” im HP-Forum beschreibt. Doch aktuell ist nicht absehbar, ob das Problem dadurch komplett behoben werden kann.

Quelle: https://www.pcwelt.de/article/2364675/warnung-hp-bios-update-crashed-laptops.html?utm_date=20240626132952&utm_campaign=Best-of%20PC-WELT&utm_content=Title%20Story%3A%20Warnung%3A%20BIOS-Update%20macht%20HP-Laptops%20unbrauchbar%20%E2%80%93%20Hersteller%20arbeitet%20an%20L%C3%B6sung&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

19) Speichermedien – USB-Stick reparieren: So einfach geht's

Ist Ihr USB-Stick kaputt und enthält wichtige Dateien? Dann sollten Sie versuchen, den Datenträger zu reparieren. So kann es gelingen.

Zeigt Ihnen das Betriebssystem eine Fehlermeldung an, wenn Sie ihren mobilen Speicher nutzen wollen? Wenn Sie auf Ihre Daten nicht mehr zugreifen können, kann die Dateistruktur auf dem Laufwerk beschädigt sein.

Keine Panik, womöglich können Sie einen Datenverlust vermeiden. Denn in einigen Fällen lässt sich der beschädigte USB-Stick mithilfe von Software-Tools oder Windows-eigenen Lösungen reparieren und eine Datenrettung vornehmen.

Schließen Sie den defekten Stick an Ihren Windows-PC an und überprüfen Sie, ob dieser ihn erkennt. Öffnen Sie den Explorer, klicken Sie mit der rechten Maustaste auf "Wechseldatenträger", "Eigenschaften", "Tools" und "Prüfen". Wählen Sie nun "Systemfehler automatisch reparieren" und "Fehlerhafte Sektoren suchen/wiederherstellen".

Reparatur auch mit kostenloser Software möglich

Wählen Sie nun "Systemfehler automatisch reparieren" und "Fehlerhafte Sektoren suchen/wiederherstellen" aus. War die Überprüfung erfolgreich, wurden die beschädigten Daten wiederhergestellt. Hat das nicht geholfen, können Sie eine Reparatur auch mit einer kostenlosen Software vornehmen.

Dafür bietet sich beispielsweise das Programm "PC Inspector File Recovery" an, das vom Computer-Portal "Chip.de" gut bewertet wurde. Führen Sie damit eine Datenrettung durch, sichern Sie die Daten anschließend extern auf einer Festplatte und formatieren Sie Ihren USB-Stick, um erneuten Fehlermeldungen vorzubeugen.

USB-Stick reparieren: Alternativen

Wird Ihr USB-Stick nicht erkannt, kann das Fehlen eines passenden Treibers die Ursache sein. Im Normalfall wird der richtige Treiber sofort nach dem Einstecken des USB-Sticks installiert und gestartet.

Funktioniert das nicht, entfernen Sie den Stick und schließen Sie ihn an eine andere USB-Buchse an. Hilft das nicht, starten Sie Ihren Computer neu und versuchen es nochmal.

Sind Sie mit diesen Maßnahmen nicht erfolgreich, suchen Sie im Internet einen passenden Treiber für Ihr Gerät und installieren Sie ihn manuell. Möglicherweise behebt eine aktuellere Treiber-Version die Fehlfunktion.

Liegt ein Problem mit den mechanischen Komponenten Ihres USB-Sticks vor, können kaputte Lötstellen, Leiterbahnen oder elektronische Teile die Ursache sein. Sind Sie kein Hobby-Bastler, ziehen Sie unbedingt einen Fachmann hinzu, um die Schäden zu beheben.

So vermeiden Sie typische Fehler

Haben Sie es geschafft, Ihren USB-Stick zu reparieren, beugen Sie Fehlfunktionen in Zukunft vor. Verschließen Sie nach jeder Nutzung Ihren Stick mit der dafür vorgesehen Kappe, so schützen Sie ihn vor Staub, Nässe und direktem Sonnenlicht, die ihm schaden können.

Achten Sie darauf, dass der Stick weder beim Transport noch bei der Lagerung gequetscht wird. Vermeiden Sie außerdem Gewalteinwirkung beim Anstecken und Abziehen des Geräts.

Entfernen Sie Ihren USB-Stick immer erst dann von der USB-Buchse, nachdem Sie "Hardware sicher entfernen und Medium auswerfen" ausgewählt haben.

Sichern Sie wichtige Dateien regelmäßig und verwenden Sie Ihren USB-Stick lediglich zum Transport Ihrer Daten zwischen verschiedenen Endgeräten.

Quelle: https://www.t-online.de/digital/hardware/id_67094642/usb-stick-reparieren-so-geht-s.html

20) Daten im Netz – Inkognito-Modus: So surfen Sie mit Firefox anonym

Der Browser Mozilla Firefox hat einen Inkognito-Modus. Ist er aktiviert, werden keine Tracking-Cookies gespeichert. Was das bedeutet, erfahren Sie hier.

Sie wollen im Internet surfen, ohne dass die aufgerufenen Websites im Verlauf gespeichert werden? Dann ist der Inkognito-Modus von Firefox genau das Richtige für Sie. Sobald Sie diesen aktiviert haben, werden in Ihrem Browser keine Suchbegriffe und Zugangsdaten gespeichert. Außerdem verhindert Firefox, dass Webseiten ihre Cookies auf der Festplatte speichern.

So aktivieren Sie den Inkognito-Modus in Firefox

In Firefox öffnen Sie den Inkognito-Modus am einfachsten mit der Tastenkombination "Strg + Umschalttaste + P". Alternativ können Sie ihn über das Anwendungsmenü aktivieren. Danach öffnet sich ein neues Fenster, das mit mehreren Eigenschaften vom üblichen Firefox-Modus abweicht.

In der Taskleiste ist ein anderes Symbol zu sehen, das neben dem Firefox-Logo auch eine Maske darstellt. Diese steht für Anonymität. Das dunkle Farbschema des neuen Fensters stellt einen großen Unterschied dar.

Sie brauchen beim anonymen Surfen nichts weiter zu beachten, da dies genauso funktioniert wie im Standard-Modus. Wichtig für Sie ist, dass der Browser nicht auf bereits vorhandene Cookies zugreift. Bei sozialen Netzwerken, beim E-Mail-Provider und bei anderen Anwendungen sind Sie dadurch nicht automatisch eingeloggt.

So anonym ist der Inkognito-Modus wirklich

Der Inkognito-Modus verhindert, dass auf Ihrem eigenen Computer Ihr Suchverlauf nachverfolgbar ist. Anonymität bietet er Ihnen allerdings nicht. Denn Daten, wie etwa die IP-Adresse, der verwendete Browser und das Betriebssystem Ihres Rechners, können ausgelesen werden. Da sich die IP-Adresse in der Regel nur nach größeren Zeitabständen ändert, kann sie auch mit Ihrem nicht privaten Surfverhalten verbunden werden.

Alternative zum Inkognito-Modus

Wenn Sie wirklich anonym surfen möchten, müssen Sie auf eine VPN-Verbindung ausweichen. Dabei surfen Sie durch eine Art Tunnel, der Ihre Herkunft verschleiert. Ihnen stehen dann jedoch unter Umständen auf Websites und Streaming-Plattformen andere Inhalte zur Verfügung.

Den Inkognito-Modus können Sie übrigens auch auf mobilen Geräten verwenden. Auch bei anderen PC-Browsern wie Edge und Chrome ist er verfügbar. Die Bezeichnungen weichen ab und heißen beispielsweise privates Surfen oder privates Fenster.

Quelle: https://www.t-online.de/digital/internet/id_100425214/inkognito-modus-wie-sie-mit-firefox-anonym-surfen.html

21) Neuer Email Betrug - wie man einfach SCAM Emails erkennt

Hier ist noch ein Tipp vom ehemaligen Kollegen und Leser Dirk K. aus der Quelle:

Tuhl Teim DE**, welcher sehr interessant ist.**

https://www.youtube.com/watch?v=5O5zhJsfEQk

Allgemeines:

1) Ist Ihrer auch betroffen? – Mit diesen Tricks erkennen Sie einen Tachobetrug

Jeder dritte Gebrauchtwagen wird mit manipuliertem Tacho verkauft. Der Schaden: durchschnittlich 3.000 Euro. Mit diesen Tricks entlarven Sie den Schwindel.

Kurz zusammengefasst:

- Jeder dritte Gebrauchtwagen hat einen manipulierten Tacho.
- Unstimmige Dokumente und Abnutzungen können Hinweise sein.
- Diagnose-Software und Fachwerkstatt helfen bei der Überprüfung.

Laut ADAC und Polizei stimmt bei jedem dritten in Deutschland verkauften Gebrauchtwagen der Kilometerstand nicht. Aber worauf können Käufer achten, um der Abzocke zu entgehen?

Durch diese Tachomanipulation steigt der Preis eines Gebrauchtwagens im Durchschnitt um 3.000 Euro, so der ADAC. Der Gesamtschaden: sechs Milliarden Euro pro Jahr.

Für Käufer eines manipulierten Gebrauchtwagens kann Tachobetrug schwerwiegende Folgen haben. Zum einen zahlen sie einen überhöhten Preis für ein Auto, das tatsächlich mehr Kilometer gefahren ist als vom Verkäufer angegeben. Zum anderen kann es auch gefährlich werden, wenn ein erforderlicher Teilwechsel aufgrund des manipulierten Kilometerstands nicht durchgeführt wird. Wird beispielsweise der Zahnriemen nicht im vorgesehenen Intervall ausgetauscht, kann ein Motorschaden die Folge sein. Deshalb ist Tachomanipulation eine strafbare Handlung.

Anhaltspunkte für einen Betrug

Obwohl man sich niemals zu 100 Prozent vor Betrug schützen kann, gibt es einige Anhaltspunkte, die auf eine Manipulation hinweisen können. Eine niedrige Laufleistung und ein vergleichsweise günstiger Preis können erste Hinweise sein. Wenn Innenräume abgenutzt erscheinen, obwohl die Laufleistung angeblich gering ist, sollte man ebenfalls skeptisch sein.

Auch Unstimmigkeiten in der Dokumentation deuten auf Manipulationen des Kilometerstands hin. Reparaturrechnungen und das Serviceheft sollte man gründlich prüfen. Dort finden sich die Wartungsintervalle, die Kilometerstände und das Datum der durchgeführten Arbeiten. Auch Haupt- und Abgasuntersuchungsprotokolle sowie Ölwechselaufkleber oder -anhänger am Fahrzeug enthalten Kilometerstand und Laufleistung. Wenn jedoch alle Einträge im alten Serviceheft gleich neu aussehen, ist Vorsicht geboten.

Fragen Sie den Vorbesitzer

Klarheit über den tatsächlichen Tachostand bringt daher nur eine gründliche Recherche. Dazu gehört die Kontrolle der Belege oder Ölkarten im Motorraum oder des kleinen Aufklebers an der A-Säule. Steht dort, dass der nächste Wechsel erst nach mehr als 50.000 Kilometern fällig ist, kann etwas nicht stimmen. Denn in der Regel ist ein Ölwechsel spätestens nach 30.000 Kilometern, in seltenen Fällen nach 40.000 Kilometern fällig. Ein Anruf beim Vorbesitzer des Verkäufers gibt Auskunft darüber, mit welchem Kilometerstand er sein Auto verkauft hat. Der Name steht in der Zulassungsbescheinigung Teil II.

Eine Diagnose-Software kann helfen

Digitale Hilfsmittel wie spezielle Adapter für die Fahrzeugdiagnoseschnittstelle können ebenfalls weiterhelfen. Diese Schnittstelle befindet sich meist in der A-Säule auf der Fahrerseite und ermöglicht einen direkten Zugriff auf die Bordelektronik. Mit speziellen Apps kann überprüft werden, ob die Airbags bei einem Unfall ausgelöst wurden. Einige Apps können auch Daten zu Kilometerständen, Wegstrecken und Fehlerspeichern auslesen. Allerdings sind diese Ergebnisse nur so gut wie die hinterlegten Daten in den Steuerungsmodulen. Wenn diese zuvor manipuliert wurden, stimmen die Angaben nicht mehr.

Eine Fachwerkstatt kann eine Manipulation eventuell durch Auslesen des Fehler- und Wartungsintervallspeichers erkennen. So können die teilweise gespeicherten Kilometerstände mit dem Tachostand verglichen werden. Die Werkstatt kann auch das Produktionsdatum des Tachos und der Steuergeräte ermitteln. Sind sie jünger als das Produktionsdatum des Fahrzeugs (nicht Erstzulassung)? Dann wurde manipuliert.

Quelle: https://www.t-online.de/mobilitaet/autos/id_85239336/unbedingt-mal-pruefen-mit-diesen-tricks-erkennen-sie-einen-tachobetrug.html

2) Sparkassen-Karte verloren? Sperren lassen reicht noch lange nicht

Verliert ihr euer Portemonnaie oder stellt fest, dass eure Bankkarte fehlt, gilt es trotz Schock schnell zu handeln: Die Karte von Sparkasse, Volksbank, Deutsche Bank und Co. muss deaktiviert werden. Doch gesperrt ist nicht gleich gesperrt. Mit KUNO stellt ihr sicher, dass euer Konto, wenn es darauf ankommt, wirklich gut geschützt ist.

Wenn die Bankkarte weg ist: Diesen Schritt dürft ihr nicht vergessen

Zumindest die Schrecksekunde kennt jeder: Wenn auf einmal das **Portemonnaie oder die EC-Karte fehlen** und man sich einfach nicht erklären kann, wohin sie verschwunden sind. Manchmal fällt der Groschen schnell, die Erinnerung kehrt zurück. Aber wenn Girokarte oder Geldbeutel dann einmal tatsächlich nicht mehr aufzufinden sind, ist schnelles Handeln gefragt.

Es gilt, die Karte sofort sperren zu lassen. Dafür könnt ihr den deutschlandweiten Sperrservice nutzen, telefonisch zu erreichen unter **116 116.** Es gibt aber noch weitere Möglichkeiten, die wir hier für euch zusammengefasst haben. Doch auch wer sein Konto über den Sperrnotruf, im Online-Banking per App oder über den Kundenservice der betreffenden Bank hat sperren lassen, ist **noch nicht ganz auf der sicheren Seite**.

KUNO-Sperrdienst verhindert Lastschrift-Käufe auf euren Namen

Denn über die normale Sperrfunktion werden nur Transaktionen verhindert, die per PIN bestätigt werden müssen. Ist eure EC-Karte also in falsche Hände geraten, kann somit niemand mehr Bargeld am Automaten abheben. Doch **SEPA-Lastschriftzahlungen mit Unterschrift sind weiter möglich.** Um das zu verhindern, könnt ihr eure Girokarte zusätzlich über den KUNO-Service sperren lassen.

Das Kürzel KUNO steht für „Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen“. Der gemeinsame Sperrdienst von Handelsunternehmen und Polizei ist letztlich eine Datenbank. Hinterlegt ihr dort die Daten der vermissten Girokarte oder **meldet den Verlust direkt bei einer lokalen Polizeistation**, ergeht eine Meldung an angeschlossene Handelsunternehmen, „sodass diese Zahlungen mit den gemeldeten Karten anschließend abgelehnt werden können“, heißt es auf der Webseite von KUNO.

Wer die Bankkarte vermisst, sollte immer auch an diese Möglichkeit denken. Denn ohne die Sperrung für Lastschriften seid ihr zwar davor geschützt, dass euer Konto direkt leergeräumt wird. Trotzdem könnte ein Dieb **auf eure Rechnung noch ziemlich ungestört Großeinkäufe tätigen**

KUNO Karten-Sperrdienst für SEPA-Lastschriftzahlungen

Ihnen wurde die girocard gestohlen oder Sie haben ihr Portemonnaie samt allen wichtigen Karten verloren? Handeln Sie nun schnell und lassen Sie Ihre girocard für das elektronische Lastschriftverfahren bei der Polizei sperren. Mit dem Einrichten einer KUNO-Sperre sind Sie auf der sicheren Seite.

Bitte beachten Sie, dass eine KUNO-Sperrung ausschließlich bei der Polizei vorgenommen werden kann. Online oder telefonisch ist eine KUNO-Kartensperre leider aus sicherheitstechnischen Gründen nicht möglich.

Was muss ich tun?

Um eine sichere und vor allem vollständige Kartensperrung durchzuführen, ist es wichtig alle Schritte der folgenden Checkliste durchzuführen. Bitte halten Sie stets Ihre Kontonummer, Bankleitzahl und Kartenfolgenummer bereit.

1.

Anzeige bei der Polizei aufgeben

- Um den Verlust Ihrer Karte anzuzeigen, wenden Sie sich an Ihre nächstgelegene Polizeidienststelle.
- Erbitten Sie dort zudem eine KUNO-Meldung und lassen Sie sich eine Sperrbestätigungsnummer und ein KUNO-Merkblatt aushändigen.

2.

KUNO-Sperrbestätigungs-nummer anfragen

- Je nach Bundesland erhalten Sie bei der Aktivierung einer KUNO-Sperre eine Sperrbestätigungsnummer von der Polizei ausgehändigt.
- Mit dieser Nummer können Sie online Ihre Kartenfolgenummer nachmelden oder Ihre KUNO-Sperre löschen.

3.

Kartenfolgenummer nachmelden

- Bitte füllen Sie das nachstehende Formular mit Ihren persönlichen Kontodaten sowie der individuellen Sperrbestätigungsnummer, welche Ihnen im Rahmen Ihrer Kartensperrung von der Polizei übergeben wurde aus.

Zum persönlichen Login

Melden Sie sich an um Ihre Kartenfolgenummer nachzumelden, den Status Ihrer Sperrung einzusehen oder die Sperrung aufzuheben.

Kontonr./BLZ
IBAN

Bankleitzahl:

Kontonummer:

Sperrbestätigungsnummer (5-stellig):

Quelle: https://www.giga.de/news/sparkassen-karte-verloren-sperren-lassen-reicht-noch-lange-nicht/?utm_source=flipboard&utm_content=topic%2Fde-digital

3) 16 Modelle im Test – ADAC warnt vor diesen Ganzjahresreifen

Der Wechsel von Sommer- auf Winterreifen kostet Zeit, Geld und Nerven. Eine günstige Alternative sind Ganzjahresreifen. Aber sind sie auch sicher? 16 Modelle im großen ADAC-Test.

Sie sind wahre Allroundtalente: Ganzjahresreifen werden auch Allwetterreifen genannt und können im Winter und auch im Sommer eingesetzt werden. Viele von ihnen sind aber keine optimale Lösung für alle Wetterbedingungen, sondern stellen einen Kompromiss zwischen Sommer- und Winterreifen dar. Ganzjahresreifen sind vor allem für bestimmte Autofahrer geeignet:

- Sie fahren vor allem in schneearmen Gebieten.
- Sie können bei extremem Wintereinbruch das Fahrzeug stehen lassen.
- Sie sind eher in der Stadt unterwegs und fahren nicht jeden Tag lange Strecken.

Allerdings wurden Ganzjahresreifen in den vergangenen Jahren immer besser. Welche aktuellen Modelle sind eine gute Wahl? Und von welchen lässt man lieber die Finger? Das hat der ADAC getestet.

So testete der ADAC

Im ADAC-Test mussten sich 16 aktuelle Modelle verschiedenen Sicherheits- und Umweltprüfungen unterziehen. Die Anforderungen waren genauso hoch wie bei den bekannten Sommer- und Winterreifentests des Clubs.

Bei sommerlichen Asphalttemperaturen von 50 Grad Celsius sollten die Ganzjahresreifen genauso gut bremsen und haften wie reine Sommerreifen. Gleichzeitig wurde ihr Verhalten bei winterlichen Minusgraden und auf schneebedeckter Fahrbahn getestet, wo sie sich wie ein Winterreifen verhalten mussten.

Neben diesen Sicherheitsaspekten legte der ADAC großen Wert auf die Umwelteigenschaften (Laufleistung, Kraftstoffverbrauch und Abrieb) der Reifen.

Das sind die Testergebnisse

16 Ganzjahresreifen im Test Das sind die Ergebnisse des ADAC

Hersteller	Modell	Preis	Sicherheit	Umwelt	Note
Goodyear	Vector 4Seasons Gen-3	120	2,70	1,80	2,40
Pirelli	Cinturato All Season SF2	114	2,30	3,30	2,60
Hankook	Kinergy 4V	98	2,90	2,20	2,70
Michelin	CrossClimate 2	131	2,90	1,00	2,70
Kumho	Solus 4S HA32+	89	3,00	2,30	2,80
Vredesteln	quatrac	105	3,10	2,20	2,80
Falken	EuroAll Season AS210	96	3,20	2,70	3,10
Firestone	Multiseasona	97	3,60	3,10	3,60
Sava	All heather	93	3,70	2,30	3,70
Nankang	Cross Seasons AW-6	79	3,70	2,90	3,70
TOTO	Celsius AS2	96	3,80	2,30	3,80
Semperit	AllSeason-Grip	99	3,90	2,90	3,90
Uniroyal	AllSeasonExpert 2	98	4,00	2,20	4,00
Yokohama	BluEarth-45	98	4,00	3,30	4,00
Kenda	Kenetica 4s	78	5,10	2,80	5,10
Infinity	Ecofour	81	5,40	2,40	5,40

Tabelle: mab/t-onlineQuelle: ADACDaten herunterladenErstellt mit Datawrapper

- Der Goodyear Vector 4Seasons Gen-3 erreicht das beste Gesamtergebnis und erhält als erster Ganzjahresreifen die Note "gut" (2,4). Er überzeugt vor allem auf nasser und winterlicher Fahrbahn, zeigt aber leichte Schwächen auf trockener Fahrbahn. Seine sehr guten Umwelteigenschaften haben hohen Anteil an der Bestnote.
- Für Wenigfahrer empfiehlt sich der Pirelli Cinturato All Season SF2. Er bietet viel Fahrsicherheit und erhält die zweitbeste Gesamtnote (2,6). Allerdings ist seine Laufleistung geringer.
- Beim Vergleich der Bremswege zeigen sich deutliche Unterschiede: Während der Michelin CrossClimate 2 auf trockener Fahrbahn aus 100 km/h nach rund 39 Metern zum Stehen kommt, benötigt der Uniroyal AllSeasonExpert 2 knapp 47 Meter – ein Unterschied, der im Ernstfall entscheidend sein kann.
- Nicht alle getesteten Modelle können überzeugen: Die Reifen Kenda Kenetica 4S und Infinity Ecofour fallen durch deutliche Mängel bei den Sicherheitsanforderungen auf, obwohl sie im Umweltverhalten gute bis befriedigende Ergebnisse erzielen. Gesamtnote: mangelhaft.