43. Cybercrime Newsletter

27.08.2024

1) "Perfide Masche" – Verbraucherschützer warnen vor Telekom-Konkurrent

Wegen der Namensähnlichkeit mit der Telekom schließen Kunden bei 1N Telecom immer wieder ungewollt Verträge ab – mit ungeahnten Folgen.

Verbraucherschützer warnen vor dem DSL-Anbieter 1N Telecom: Der Anbieter werde immer wieder mit der Deutschen Telekom verwechselt und nutze das mit einer "perfiden Masche" aus, erklärte der Verbraucherzentrale Bundesverband (vzbv). Seit Anfang 2023 seien mehr als 11.000 Beschwerden darüber eingegangen, der vzbv habe nun eine Unterlassungsklage erhoben.

1N Telecom schreibe Verbraucher an und biete ihnen 24-Monats-DSL-Verträge an, erklärten die Verbraucherschützer. Nehmen Interessenten das Angebot an, beantrage 1N Telecom die Portierung der Rufnummer.

Im Glauben, einen Vertrag mit der Telekom geschlossen zu haben, widersprächen viele daraufhin der Portierung, erklärte der vzbv. Anschließend fordere 1N Telecom "Schadenersatz in Höhe von 419,88 Euro und lässt das Geld auch von einer Inkassofirma eintreiben".

Vor allem ältere Personen betroffen

"Vor allem ältere Menschen sind betroffen, wie zahlreiche Verbraucherbeschwerden zeigen", erklärte Sebastian Reiling vom vzbv. "Wir halten die hohen Schadensersatzforderungen des Unternehmens gegenüber Verbrauchern für vollkommen unberechtigt."

Rechtlich angreifbar macht sich der Anbieter laut vzbv dadurch, dass er ausschließlich 24-Monats-Verträge anbietet. "Es müsste zugleich ein Vertrag mit einer Laufzeit von maximal zwölf Monaten angeboten werden." Der Verband prüfe auch eine Sammelklage, betroffene Verbraucher sollen sich dafür melden.

Der Telekom-Konkurrent macht immer wieder mit dubiosen Werbebriefen auf sich aufmerksam. Im vergangenen Jahr hatte das Unternehmen unter anderem irritierende Werbepost an Telekom-Kunden verschickt, die daraufhin ungewollt Verträge mit dem DSL-Anbieter abschlossen.

Ungewollte Vertragsabschlüsse widerrufen

Weil die Schreiben des Anbieters persönliche Daten wie Adresse und Telefonnummer der Empfänger enthalten hatten, zeigten sich diese überrascht, woher das Unternehmen diese Informationen habe.

"Viele denken, dass es sich um ein Schreiben der Telekom handele, was nicht der Fall ist, und unterschreiben daher das Angebot", sagt Felix Flosbach damals. Flosbach ist Jurist

bei der Verbraucherzentrale Nordrhein-Westfalen.

Die Verbraucherschützer raten, ungewollte Vertragsabschlüsse zu widerrufen. Das sei bis zu 14 Tage nach Abschluss möglich. "Dafür kann das Widerrufsformular verwendet werden, das Anbieter wie die 1N Telecom GmbH ihrem Werbebrief beigelegt haben."

Quelle: https://www.t-online.de/digital/aktuelles/id_100475264/1n-telecom-telekom-konkurrent-lockt-kunden-in-kostenfalle.html

2) Stuttgart Hauptbahnhof: Wie eine junge Frau eine Betrugsmasche aufdeckte

Immer wieder sieht unsere Reporterin denselben Betrüger am Stuttgarter Bahnhof. Dann spricht sie ihn an. Doch tun kann sie gegen seine Masche wenig.

Ein Mann spricht am Gleis eine Freundin an, während ich telefoniere. Als ich auflege, überweist sie ihm über Paypal fünf Euro. Das Geld sieht sie nie wieder. Den Mann hingegen sehe ich seitdem jedes Mal am Stuttgarter Hauptbahnhof.

Die Betrugsmasche

Die Betrugsmasche ist simpel und immer die gleiche: Der Betrüger spricht Menschen an und tischt ihnen eine Geschichte auf - der Geldbeutel wurde geklaut oder seine Karte wurde am Automat eingezogen. Er erzählt, dass er nur nachhause möchte. Für ein Online-Ticket benötige er etwas Geld, das er natürlich zurückzahlen werde - schließlich habe man ja seine Daten. Also überweisen ihm einige Leute Geld auf sein Paypal-Konto. Seine Masche ist dreist, aber effektiv.

Meist spricht der Mann Englisch. Er sieht aus wie jede andere reisende Person am Bahnhof: ordentliche Kleidung, gekämmte Haare und Reisegepäck.

Wenn man ablehnt, ihm Geld zu geben, wird er nicht aufdringlich und verabschiedet sich freundlich - dann geht er zu seinem nächsten Opfer über.

Betrug erfolgreich vereitelt

Als ich den Mann das nächste Mal wiedersehe, denke ich zuerst an einen Zufall. Vielleicht sieht er dem Mann, der eine Freundin um Geld betrogen hat, nur sehr ähnlich. Doch auch diese Person sehe ich aus der Ferne mit einem Fremden sprechen. Ich werde aufmerksam. Ein paar Tage später sehe ich den Mann wieder - und jedes Mal scheint er nach Geld zu fragen.

Als ich das nächste Mal am Gleis warte, sitzt eine Frau neben mir. Ihr Gepäck steht zwischen ihren Beinen und sie schaut auf ihr Handy, als sie angesprochen wird. Aus den Augenwinkeln beobachte ich die Situation und bin bereit, einzuschreiten. Denn der Mann hat seinen Vertrauensvorschuss verloren.

Als ich ihn mit den Worten „Habe ich Sie neulich nicht schon mal gesehen?“ verschwindet er in der Menschenmenge der Reisenden. Ich erkläre der Frau neben mir die Situation. „Ich dachte zuerst, dass er Hilfe braucht, seine Verbindung zu finden“, sagt sie kopfschüttelnd. Als er Geld wollte - auch wenn es nur zwei Euro waren - wurde sie stutzig.

Wiederkehrende Begegnungen

Wenige Tage später stehe ich erneut an den Gleisen. Der Stuttgarter Hauptbahnhof ist ein zentraler Knotenpunkt für Reisende aus aller Welt. Täglich passieren tausende Menschen die Hallen. Es ist spät und trotzdem ist der Bahnhof noch voller geschäftiger Menschen, die zu ihren Zügen hetzen.

Quelle:https://www.schwaebische.de/regional/baden-wuerttemberg/stuttgart-hauptbahnhof-wie-eine-junge-frau-eine-betrugsmasche-aufdeckte-reporterin-2798493

3) Betrugs-Ticker – E-Mail-Betrugsmasche droht mit hoher Geldstrafe

Betrüger sind einfallsreich, wenn es darum geht, Menschen um ihr Geld zu bringen. Wir zeigen Ihnen, welche Maschen derzeit im Umlauf sind.

Kriminelle versuchen ständig, an sensible Daten von Konten und Kreditkarten sowie persönliche Informationen von Verbrauchern zu kommen. Dafür nutzen sie vor allem digitale Kanäle. Welche Maschen sie dabei verwenden, erfahren Sie hier.

++ Aktuelle Phishing-E-Mails drohen mit hoher Geldstrafe (26.8.2024) ++

Die Verbraucherzentrale warnt vor neuen Betrugsmaschen in Form von Phishing-Mails an die Kundschaft der Sparkasse. In den E-Mails mit dem Betreff "Sicherheitsmeldung" geben die Betrüger vor, wegen einer vermeintlich ungültigen Geräte-Registrierung den Kunden mehrfach kontaktiert zu haben. Die Empfänger werden aufgefordert, umgehend ihre Registrierungsdaten über einen Link in der Mail zu korrigieren – sonst droht ihnen eine Strafe von 5.200 Euro.

Dass es sich dabei um eine Betrugsmasche handelt, ist auf den ersten Blick gar nicht so leicht zu erkennen. Die Absenderadresse ist laut Verbraucherzentrale nicht immer eindeutig als Phishing-Versuch zu enttarnen. Typisch sind allerdings der unprofessionelle Wortlaut, die unpersönliche Anrede und Verlinkungen innerhalb der Mail.

Auch Kundinnen und Kunden der ING und Targobank sollten aktuell achtsam in ihrem E-Mail-Postfach sein. Unter dem Vorwand "Wichtige Information zur Kontosicherheit" oder ähnlichen Betreffzeilen sind Empfänger dazu aufgefordert, ihre Kontaktdaten zu aktualisieren. Die Betrüger geben sogar vor, sie damit vor kriminellen Aktivitäten zu schützen. Mit diesen perfiden Tricks versuchen solche Phishing-Versuche an persönliche Daten zu gelangen.

Wichtig: Eine seriöse Bank würde Ihre Daten niemals über einen Link abfragen. Wenn eine der Betrugsmaschen bei Ihnen im Postfach landet, sollten Sie unter keinen Umständen auf die enthaltenen Links klicken. Verschieben Sie die E-Mail einfach in den Spam-Ordner.

++ Vorsicht vor gefälschten E-Mails der Steuerverwaltung (23.8.2024) ++

Eine E-Mail von der Steuerverwaltung im Posteingang – da wird man schnell aufmerksam. Doch Vorsicht: Wer aktuell eine solche E-Mail erhält, sollte besonders wachsam sein. In letzter Zeit häufen sich betrügerische Nachrichten, die den Anschein erwecken, von Elster, dem Finanzamt oder dem Bundeszentralamt für Steuern (BZSt) zu stammen.

Diese E-Mails enthalten oft die Aufforderung, eine angehängte Datei zu öffnen, die als Steuerbescheid oder Rechnung ausgegeben wird, so der Hinweis auf der Website der elektronischen Steuererklärung (Elster). Das Ziel: An persönliche Daten wie Log-in-Informationen sowie Bank- oder Kreditkartendaten zu gelangen.

Empfängerinnen und Empfänger solcher E-Mail sollten daher keine Anhänge öffnen, wenn sie sich nicht sicher über die Herkunft der Nachricht sind, so Elster. Auch bei eingebetteten Links in solchen E-Mails ist Vorsicht geboten – sie sollten nur dann angeklickt werden, wenn die Echtheit der Nachricht zweifelsfrei feststeht.

Zudem gilt: Steuerverwaltungen fragen niemals per E-Mail nach sensiblen Daten wie Steuernummern, Bankverbindungen oder PINs. Bei Unsicherheiten kann die Rücksprache mit dem zuständigen Finanzamt Klarheit bringen.

++ Angeblicher Gewinn ist Betrugsmasche (19.8.2024) ++

Wer freut sich nicht, wenn man unerwartet Geld erhält? Wenn Sie eine SMS von "SofortInfo" erhalten, sollten Sie sich allerdings nicht zu früh freuen. Wie das Faktencheck-Portal "Mimikama" berichtet, versuchen Cyberkriminelle derzeit, vermeintliche Opfer mit einem Geldversprechen in die Falle zu locken. In der SMS heißt es, es sei ein Geldbetrag auf das eigene Konto eingegangen.

Um das Geld zu erhalten, soll man auf einen Link klicken – und seine persönlichen Daten eingegeben. Hier schnappt die Falle zu, denn es handelt sich dabei um eine Betrugsmasche, um private Informationen abzugreifen. Wenn Sie diese SMS erhalten, sollten Sie sie umgehend löschen und keinesfalls dem Link folgen.

++ DRSF warnt vor Betrugs-SMS (14.8.2024) ++

Der Deutsche Reisesicherungsfonds warnt vor Betrügern, die versuchen, über Phishing-SMS an die Bankdaten von Reisenden zu kommen. Laut DRSF erhielten mehrere Verbraucher verdächtige Kurznachrichten, die eine Rückerstattung in Aussicht stellten. Allerdings führt der dort enthaltene Link auf eine gefälschte Webseite.

Dort sollten die Empfänger ihre Bankdaten eingeben, um das erhoffte Geld zu erhalten. Der DRSF betont jedoch, dass diese Nachrichten nicht von ihm stammen und warnt eindringlich davor, auf den Link zu klicken oder persönliche Daten preiszugeben; stattdessen solle die SMS sofort gelöscht werden. Wer unsicher ist, kann sich an die DRSF-Hotline wenden.

Der Zeitpunkt für diesen Betrugsversuch erscheint als nicht zufällig gewählt. Erst kürzlich startete der DRSF nach der Pleite des Reiseanbieters FTI den bisher größten Rückerstattungsprozess seit der Reform des Kundengeldschutzes. Die Betrüger versuchen offenbar, die Situation auszunutzen, um an sensible Daten von Reisenden zu gelangen.

++ Das sind die effektivsten Phishing-Betreffzeilen (14.8.2024) ++

Eine Studie des Sicherheitsunternehmens KnowBe4 zeigt, dass Hacker bei ihren Phishing-Attacken besonders oft auf E-Mails setzen, die angeblich von der Personal- oder IT-Abteilung stammen. Besonders beliebt sind Betreffzeilen wie "Möglicher Tippfehler" oder "Wichtige Änderungen am Dresscode". Auch vermeintliche Aufforderungen, Formulare zu aktualisieren oder an Schulungen teilzunehmen, verleiten viele zum Klicken.

Die Experten warnen, dass solche E-Mails besonders gefährlich seien, da HR-Abteilungen oft viel Entscheidungsgewalt hätten und sofort die Aufmerksamkeit der Mitarbeiter wecken. Ähnliches gilt für Nachrichten, die angeblich von der IT stammen. Auch hier fallen Nutzer leicht auf Meldungen über gesperrte Konten oder fehlgeschlagene Back-ups herein.

KnowBe4-Chef Stu Sjouwerman betont, dass sich die Taktiken der Cyberkriminellen ständig weiterentwickeln und dadurch eine große Gefahr für Unternehmen weltweit darstellen würden. Laut dem Bericht setzen Kriminelle in ihren Phishing-Versuchen auch verstärkt auf QR-Codes, da die Angriffe dadurch noch schwerer zu durchschauen sind.

Laut dem Lagebericht der IT-Sicherheit 2023 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Bedrohung im Cyberraum "so hoch wie nie zuvor". Gerade für Unternehmen sind die Folgen eines Cyberangriffs oft fatal. Aber auch Privatpersonen können nach einem erfolgreichen Angriff viel Geld verlieren und jede Menge Ärger bekommen.

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

Quelle: https://www.t-online.de/digital/aktuelles/id_100468380/e-mail-betrugsmasche-droht-sparkassen-kunden-mit-geldstrafe.html

4) Kleinunternehmen im Visier – Ransomware-Attacken: Die digitale Erpressung boomt

Cyberkriminelle setzen verstärkt auf Erpressungssoftware, um an Geld zu kommen. Ein aktueller Bericht zeigt besorgniserregende Entwicklungen in Bezug auf Ransomware.

Der WithSecure-Report "Ransomware Landscape 2024" offenbart einen beunruhigenden Trend: Auch wenn die Produktivität der Ransomware-Branche nach ihrem Höhepunkt Ende 2023 nicht mehr ansteigt, sind sowohl die Häufigkeit der Angriffe als auch die Höhe der eingenommenen Lösegeldzahlungen in der ersten Hälfte des Jahres 2024 im Vergleich zu den Vorjahren weiter gestiegen.

"Es gibt eine deutliche Verlagerung hin zu kleinen und mittleren Unternehmen, die nun einen größeren Anteil der Ransomware-Opfer ausmachen", sagt Tim West, Direktor für Bedrohungsanalyse bei WithSecure. Der Anteil dieser Firmen an den Ransomware-Opfern stieg von 50 Prozent im Jahr 2022 auf fast 61 Prozent in der ersten Hälfte 2024. Die Experten des finnischen IT-Sicherheitsunternehmens vermuten, dass Kriminelle hier auf schnellere und häufigere Lösegeldzahlungen setzen.

Besonders betroffen sind laut dem Bericht Branchen wie das verarbeitende Gewerbe, das Baugewerbe und das Gesundheitswesen. Diese Entwicklung könnte weitreichende Folgen für die Wirtschaft haben, da kleinere Unternehmen oft nicht über die nötigen Ressourcen verfügen, um sich effektiv gegen solche Angriffe zu schützen oder sich davon zu erholen.

Auch für Verbraucher hat diese Entwicklung konkrete Auswirkungen: Kleinere Onlineshops, lokale Dienstleister oder Arztpraxen könnten Ziel von Attacken werden und dabei sensible Kundendaten verlieren. Das bedeutet ein erhöhtes Risiko für den Missbrauch persönlicher Informationen wie Adressen, Kreditkartendaten oder sogar Gesundheitsinformationen.

Neue Tricks der Erpresser

Die Angreifer passen ihre Methoden stetig an und werden dabei immer raffinierter. Statt aufwendiger Netzwerkeinbrüche konzentrieren sie sich oft auf leicht zugängliche Daten. Dabei nutzen sie vermehrt Schwachstellen in öffentlich erreichbaren Anwendungen aus – in rund 45 Prozent der Fälle war dies der Einstiegspunkt. Auch Cloud-Dienste geraten verstärkt ins Visier der Kriminellen.

Der Bericht hebt außerdem hervor, dass Ransomware-Gruppen zunehmend auf sogenannte Dual-Use-Tools (zu Deutsch: doppelt verwendbare Werkzeuge) setzen – legitime Software für Fernzugriff und Datentransfer, die für böswillige Zwecke missbraucht wird und die Erkennung von Angriffen erschwere. Zudem beobachten die Experten einen Trend zu gezielteren Angriffen auf kritische Infrastrukturen, was potenziell schwerwiegende

gesellschaftliche Auswirkungen haben könnte.

Behörden schlagen zurück

Im Kampf gegen Ransomware zeigt sich aber auch, dass Behörden verstärkt und mit einigem Erfolg gegen kriminelle Gruppen vorgehen. Ein aktuelles Beispiel sei die Infiltration und Störung der Infrastruktur der berüchtigten Hacker-Gruppierung Lockbit durch die Ermittler. Solche Aktionen erschweren es Kriminellen, ihr Geschäftsmodell aufrechtzuerhalten, und säen Misstrauen in der Cybercrime-Szene.

Der Bericht deutet an, dass der Rückgang der Produktivität solcher Ransomware-Gruppen möglicherweise auf diese behördlichen Maßnahmen zurückzuführen sei. Allerdings warnen die Experten, dass sich die Bedrohungslandschaft ständig anpasst und weiterentwickelt.

Der Report zeige jedoch auch vermehrt Hinweise auf eine Umbauphase bei Lockbit. Daraus ziehen die Autoren den Schluss, dass Lockbit "mit großer Sicherheit beabsichtigt, mit einem robusteren Betriebsmodell in die Branche zurückzukehren".

Hinweis: Was ist eine Ransomware-Attacke?

Ransomware ist eine bestimmte Art von Software, die darauf abzielt, wichtige Daten oder Systeme eines Nutzers oder einer Organisation zu verschlüsseln, sodass sie nicht mehr zugänglich sind. Die Angreifer fordern dann von den Opfern ein Lösegeld, häufig in Form von Kryptowährungen wie Bitcoin, da diese Zahlungen schwer zurückzuverfolgen sind.

Ransomware-Angriffe können sich auf Privatpersonen, Unternehmen oder öffentliche Einrichtungen auswirken. Diese Art von Cyberangriff ist besonders problematisch, da sie kritische Daten oder Dienste lahmlegen und erhebliche finanzielle und betriebliche Schäden verursachen kann.

Quelle: https://www.t-online.de/digital/aktuelles/id_100473554/ransomware-hacker-angriffe-auf-kleinunternehmen-nehmen-2024-laut-report-zu.html

5) Polizei warnt: 150.000 Euro nach einem einzigen Telefonanruf weg

Betrüger erbeuten mit nur einem einzigen Telefonanruf 150.000 Euro. So gingen die Gangster vor und das rät die Polizei.

Die bayerische Polizei berichtet von einem Enkeltrickbetrug, durch den eine ungewöhnlich hohe Schadenssumme entstanden ist. Die Betrüger konnten nämlich eine Seniorin dazu bringen, 150.000 Euro Bargeld zu übergeben.

Das Opfer ist laut dem Polizeipräsidium Oberbayern Süd eine Mitte 80-jährige Frau aus dem Landkreis Berchtesgadener Land (Oberbayern). Die Polizei schildert den Anruf, durch den die Frau am 16. August 2024 Opfer des Betruges wurde, folgendermaßen:

Eine unbekannte Anruferin, welche sich als Rechtsanwältin ausgab, hatte die Seniorin am Telefon in ein Gespräch verwickelt und ihr erzählt, dass deren Nichte einen tödlichen Verkehrsunfall verursacht hätte und nun eine Kaution für deren Freilassung gezahlt werden müsse. Die angebliche Rechtsanwältin fingierte die Festnahme der Nichte durch Polizei und Staatsanwaltschaft.

Die eigentliche Geldübergabe hat sich laut der Polizei so abgespielt:

Um die vermeintliche Kaution zu bezahlen, übergab die ältere Dame im Laufe des Vormittags an deren Wohnanschrift schließlich Bargeld in Höhe von 150.000 Euro an die Betrüger. Ein Abholer konnte das Bargeld und an sich nehmen und unerkannt verschwinden. Einige Zeit darauf bemerkte die ältere Dame, dass sie Opfer von Betrügern wurde und wählte den Polizeinotruf.

Die Polizei nennt keine Details dazu, wieso die 80-jährige Frau so schnell 150.000 Euro in bar zur Verfügung hatte. Laut dem Bayerischen Rundfunk hatte die Frau diese enorme Summe aber tatsächlich bei sich zu Hause – das allein ist äußerst fragwürdig und gefährlich. Hätte die Frau das Geld dagegen erst von ihrer Bank abheben müssen, hätte ein aufmerksamer Bank-Mitarbeiter eingreifen und die Polizei verständigen können.

Das rät die Polizei

- Lassen Sie sich nie unter Druck setzen, auch nicht durch angeblich dringende Ermittlungen oder eine Kaution, die angeblich unbedingt zu bezahlen ist!
- Die Polizei fordert niemals Bargeld, Überweisungen oder Wertgegenstände von Ihnen, um Ermittlungen durchzuführen! Legen Sie einfach auf!
- Geben Sie am Telefon niemals Auskünfte über Ihr Hab und Gut, Ihr Bargeld und Ihre Wertgegenstände! Legen Sie einfach auf!
- Lassen Sie niemanden in die Wohnung, der sehen will, wo Sie Geld oder Schmuck aufbewahren!
- Rufen Sie nie über die am Telefon angezeigte Nummer zurück! Drücken Sie KEINE Wahlwiederholung. Legen Sie auf und wählen Sie stattdessen den Notruf 110!
- Erstatten Sie immer, auch im Versuchsfall, Anzeige bei Ihrer Polizeiinspektion!
- Kinder und Enkel sollen ihre älteren Verwandten über diese Betrugsmasche informieren.

So einfach schützen Sie sich

- Telefonbetrug: Dieses zwei einfachen Tricks schützen Sie
- Telefonbetrug und Enkeltrickbetrug: So schützen Sie sich

Mehr zum Thema Enkeltrickbetrug

- Bundesnetzagentur warnt vor Enkeltrick und sperrt tausende Rufnummern
- Dreist: Whatsapp-Betrüger melden sich ein zweites Mal bei ihren Opfern – der Grund

Quelle: https://www.pcwelt.de/article/2431373/enkeltrick-150-000-euro-nach-einem-einzigen-telefonanruf-weg.html?utm_date=20240826140901&utm_campaign=Security&utm_content=Title%20Story%3A%20Polizei%20warnt%3A%20150.000%20Euro%20nach%20einem%20einzigen%20Telefonanruf%20weg&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) NFC-Malware leert Bankkonten

Phishing und Malware kombiniert ein Angreifer, um Geldautomaten Bankkarten vorzuspielen und per NFC Geld abzuheben. Beobachtet wurde das in Tschechien.

Android-Malware, die Daten von NFC-Karten kopiert und übermittelt, hat das slowakische IT-Sicherheitsunternehmen ESET in freier Wildbahn gefunden. Über mehrere Monate hinweg wurden damit fremde Konten bei drei tschechischen Banken geleert. Seit März ist ein Verdächtiger in Haft, doch sind Nachahmer wohl nur eine Frage der Zeit. Die Malware

namens NGate soll auf Software beruhen, die Studenten der Technischen Universität Darmstadt geschrieben und für Forschungszwecke veröffentlicht haben.

Diese Software heißt nfcgate und erfasst, analysiert und modifiziert Daten, die über NFC-Verbindungen übertragen werden. Zweck ist, das Verständnis von Übertragungsprotokolle zu vertiefen und deren Sicherheit zu bestimmen. Laut ESET haben sich Unbekannte an dem Darmstädter Code bedient, um die NFC-Malware NGate für illegale Zwecke zu programmieren.

NFC steht für Near Field Communication; das ist ein mehr als 20 Jahre altes Verfahren zur kontaktlosen Übertragung von Daten über wenige Zentimeter Distanz. Eingesetzt werden NFC-Chips beispielsweise in Mobiltelefonen, Zutrittskarten, Fahrausweisen und Bankkarten. Die Mehrheit der deutschen Verbraucher zahlt inzwischen kontaktlos, dank NFC. Auch in Tschechien sind Bankkarten mit NFC längst Standard. Das haben der oder die Täter ausgenutzt.

Mehrstufiger Angriff

Die Angriffe begannen mit SMS, wahrscheinlich an wahllose tschechische Handynummern verschickt. Darin wurde die Auszahlung eines Steuerguthabens versprochen, wozu die Installation einer verlinkten App erforderlich sei, die direkt im Browser läuft (Progressive Web App, PWA). Nein, das war noch nicht die NFC-Malware. Wer die App installierte und seine Bankdaten eingab, verschaffte den Tätern Zugriff auf das eigene Bankkonto. Es folgte der Anruf einer Person, die einen "hilfreichen Bankmitarbeiter" spielte. Diese Person informierte das Opfer (faktisch korrekt) darüber, dass er Opfer eines IT-Angriffs geworden sei.

Die "notwendige Abhilfe" bestand laut der Erzählung darin, eine weitere App zu installieren, um schnell die PIN für die eigene Bankkarte ändern zu können. Dazu wurde das Opfer auf den Google Play Store nachahmende Webseiten geschickt, um die Malware NGate herunterzuladen und zu installieren. Das war dann die NFC-Malware. (Im echten Google Play Store hat ESET sie nicht gefunden.) Die Software ahmt das Interface echter Bank-Apps nach und fragt Kundennummer, Geburtsdatum und PIN ab. Außerdem leitet sie den Nutzer dazu an, die passende Bankkarte ans Gerät zu halten. Falls notwendig, wird auch das Einschalten von NFC am Handy gefordert.

Tatsächlich dient das alles nicht der Absicherung des Bankkontos; vielmehr schickt die Malware PIN und NFC-Daten an das gerootete Android-Handy eines Täters. In Tschechien ist dann ein Maskierter mit so einem Handy zu NFC-fähigen Geldautomaten gegangen und hat sich von dem fremden Konto Geld auszahlen lassen. Dank des durch die erste App erbeuteten Zugriff auf das Online-Banking des Opfers, konnten die Täter die Auszahlungslimits erhöhen.

Root nicht erforderlich

Die Handys der Opfer mussten übrigens nicht gerootet sein, betont ESET. Dessen Forscher haben NGate-Varianten für sechs verschiedene tschechische Banken aufgespürt, stets signiert mit dem selben Entwicklerzertifikat.

Erfolgreiche Angriffe sind auf Kunden dreier tschechischer Banken bekannt. Als die tschechische Polizei im März einen 22-jährigen Verdächtigen festnahm, hatte er

umgerechnet mehr als 6.000 Euro bei sich. Das Bargeld soll lediglich von seinen drei letzten Opfern stammen, weshalb eine vielfach höhere Schadenssumme wahrscheinlich ist. Die Polizei bittet Opfer, Anzeige zu erstatten, und womöglich gleich mitzuteilen, an welchem Geldautomaten ihr Konto erleichtert wurde.

Übrigens: Wenn es den Tätern nicht gelang, das Opfer zur Installation der NFC-Malware zu installieren, bereicherten sie sich gerne durch Überweisungen am fremden Konto. Dazu reichte schon die erste App, ganz ohne NFC.

Update 27.08.2024, 09:06 Uhr

In Überschrift und Vorspann war von "kopierten Bankkarten" die Rede, was nicht korrekt ist. Das haben wir deshalb geändert. Der Angriff simuliert lediglich eine Karte, indem eine Malware die Antworten der echten Karte abgreift und an den Täter vor dem Automaten sendet, wie es der Artikel selbst auch richtig beschreibt.

Quelle: https://www.heise.de/news/NFC-Malware-leert-tschechische-Bankkonten-9848256.html?utm_source=flipboard&utm_content=flbd1rp6cmrht7g%2Fmagazine%2FTECHNIKGED%C3%96NS_

7) Aktuelle Betrugsmaschen – Elster warnt: Öffnen Sie bloß nicht diese E-Mails

Betrugsmaschen greifen so um sich, dass fast jeder schon damit konfrontiert war. Doch die Methoden wandeln sich und zielen darauf ab zu überrumpeln. Damit Sie richtig reagieren, halten wir Sie hier auf dem Laufenden.

Vorsicht vor gefälschten E-Mails der Steuerverwaltung

Update vom 26. August: Eine E-Mail von der Steuerverwaltung im Posteingang – da wird man schnell aufmerksam. Doch Vorsicht: Wer aktuell eine solche E-Mail erhält, sollte besonders wachsam sein. In letzter Zeit häufen sich betrügerische Nachrichten, die den Anschein erwecken, von Elster, dem Finanzamt oder dem Bundeszentralamt für Steuern (BZSt) zu stammen.

Diese E-Mails enthalten oft die Aufforderung eine angehängte Datei zu öffnen, die als Steuerbescheid oder Rechnung ausgegeben wird, so der Hinweis auf der Website der elektronischen Steuererklärung (Elster). Das Ziel: An persönliche Daten wie Log-in-Informationen sowie Bank- oder Kreditkartendaten zu gelangen.

Empfängerinnen und Empfänger solcher E-Mails sollten daher keine Anhänge öffnen, wenn sie sich nicht sicher über die Herkunft der Nachricht sind, so Elster. Auch bei eingebetteten Links in solchen E-Mails ist Vorsicht geboten - sie sollten nur dann angeklickt werden, wenn die Echtheit der Nachricht zweifelsfrei feststeht.

Zudem gilt: Steuerverwaltungen fragen niemals per E-Mail nach sensiblen Daten wie Steuernummern, Bankverbindungen oder PINs. Bei Unsicherheiten kann die Rücksprache mit dem zuständigen Finanzamt Klarheit bringen.

Geld für ausgefallenen Zug zurückbekommen? Vorsicht bei diesen Mails

Update vom 21. August: Die Deutsche Bahn sorgt derzeit vermehrt für Negativ-Schlagzeilen mit Zugausfällen und Verspätungen. Genau das machen sich Betrüger jetzt zunutze.

Wie die Verbraucherzentrale warnt, kursieren Phishing-Mails in vermeintlicher Stellvertretung

der Deutschen Bahn. Der Betreff der Mails lautet "Ihre Online-Anfrage wurde erfolgreich bearbeitet". Der Inhalt verspricht eine Erstattung eines Bahntickets, da diese erfolgreich bearbeitet worden und bereits auf das angegebene Zahlungsmittel überwiesen worden sei. Es werden auch ein angeblicher Erstattungsbetrag, eine Ticketnummer sowie ein Reisedatum genannt. Weiter enthält die Mail einen Button mit dem Satz "Meine Anfrage wurde aktiviert".

Die Verbraucherschützer warnen: "Auch wenn in dieser Mail keine direkte Handlungsaufforderung gegeben wird, könnte man dazu verleitet werden, der Sache auf den Grund gehen zu wollen." Stattdessen solle man die Mail unbearbeitet in den Spam-Ordner verschieben, raten sie.

Der Phishingversuch lasse sich unter anderem an der unseriösen Absende-Adresse und der Verlinkung innerhalb der Mail erkennen.

Vorsicht, wenn Sie solch ein Päckchen auf der Straße finden

Update vom 15. August: Zu Beginn des Jahres war es die Landespolizeidirektion Wien, die vor dieser neuen "raffinierten Methode" warnte *(wir berichteten)*. Nun ist sie in München und Umland aufgefallen und könnte sich bereits auf weitere Regionen ausgeweitet haben.

Was dabei passiert: Passanten denken, sie hätten Bitcoins regelrecht auf der Straße gefunden. Bitcoin-Paper-Wallets, die zur Aufbewahrung von Bitcoins in Papierform verwendet werden, liegen in Plastiktüten auf dem Gehweg. Anbei befindet sich ein Zahlungsbeleg über 10.000 Euro. "Den QR-Code keinesfalls scannen", warnt das Bayerische Landeskriminalamt (BLKA).

Scannt ein Finder den aufgedruckten QR-Code, gelangt er auf eine Internetseite, auf der die Betrüger dann seine Daten einkassieren wollen. Auf der Seite wird behauptet, gegen eine Bearbeitungsgebühr von rund drei Prozent würde die Summe ausgezahlt. "Fällt ein Finder auf die Masche herein und gibt seine Kontodaten weiter, wird die Auszahlungsgebühr abgebucht. Im Anschluss erscheint jedoch eine Fehlermeldung, denn eine tatsächliche Auszahlung der 10.000 Euro findet nicht statt", schildert die Polizei.

Das Landeskriminalamt bittet Finder solcher Plastiktüten, die Paper-Wallets bei der nächsten Polizeidienststelle abzugeben. Betrugsopfer sollten immer Anzeige bei der örtlichen Polizei erstatten.

Wie Betrüger an Daten von PayPal- und Klarna-Kunden kommen

Update vom 8. August: Die gute Nachricht vorweg: Von gängigen Betrugsmaschen wie Phishing, Enkeltrick und Schocknachrichten haben über 90 Prozent der Verbraucher in Deutschland schon mal gehört, so das Ergebnis einer Umfrage des Zahlungsdienstleisters Visa. Viele sind also gewarnt. Das zeigt aber auch, wie stark diese Maschen um sich greifen.

Rund neun von zehn Befragten gaben an, bereits Opfer von Betrugsversuchen im Netz geworden zu sein. 83 Prozent meinen, im Internet haben die Bedrohung allein in den vergangenen zwölf Monaten zugenommen. Fast alle (94 Prozent) machen sich Sorgen, dass sie durch den Einsatz von Künstlicher Intelligenz noch schwerer zu erkennen sein werden.

Verfolgt man die Warnungen im Phishing-Radar der Verbraucherzentrale, ist schnell erkennbar: Besonders häufig sind Phishing-Versuche, bei denen Kriminelle Namen und Logo großer Banken missbrauchen. Hier wird beispielsweise zu einer erneuten Photo-Tan-Aktivierung aufgerufen oder mit einer Kontosperrung gedroht. Am Ende sind die Betrüger immer auf Zahlungsinformationen ihrer Opfer aus, mit denen sie dann selbst Überweisungen tätigen oder einkaufen gehen können. 64 Prozent der Befragten erhielten bereits Phishing-Nachrichten im Namen einer Bank. Noch häufiger sind laut der Umfrage gefälschte

Nachrichten von Paket- oder Lieferdiensten, die 80 Prozent der Befragten bereits erreichten.

Aktuell warnt die Verbraucherzentrale vor Phishing-Mails im Namen von PayPal und Klarna. Mit dem PayPal-Logo kursiert eine angebliche Zahlungsbenachrichtigung - im konkreten Fall über 962,72 Euro an ein großes Reiseunternehmen. User sollen dadurch in Unruhe versetzt werden und sich unüberlegt über den beigefügten Link einloggen. Ebenfalls unter Druck setzt eine aktuelle Mail, in der Klarna-Kunden konfrontiert werden "Ihre Zahlungsmethode ist nicht mehr gültig". Es wird dazu aufgefordert, die Daten zu aktualisieren.

In drei Schritten: So schützen Sie sich vor Phishing

- Phishing passiert nicht nur per Mail oder SMS, sondern auch am Telefon: Wollen Kriminelle an Ihre persönlichen und vertraulichen Daten kommen, werden sie einfallsreich. Besonders gerne täuschen sie dringenden Handlungsbedarf vor, um ihre Opfer in Stress zu versetzen und sie zu unüberlegten Handlungen zu bewegen. Häufig sind dabei Drohungen mit Kontosperrungen, Mahnverfahren oder strafrechtlichen Konsequenzen das Mittel der Wahl. Das Gemeinschaftsunternehmen der deutschen Banken und Sparkassen, Euro Kartensysteme, gibt drei Tipps, wie Sie Ihre Daten schützen und Schaden abwenden können:
- **Schritt 1: Ruhe bewahren:** Erscheint Ihnen ein Anruf, eine E-Mail oder eine Nachricht auf dem Handy verdächtig? Bleiben Sie ruhig, atmen Sie tief durch und nehmen Sie sich Zeit, die Situation in Ruhe zu analysieren. Lassen Sie sich nicht von dem künstlich erzeugten Druck verunsichern.

Immer mehr weitet sich im Übrigen auch das sogenannte "Love Scamming" aus,14 Prozent waren bereits Ziel dieser Betrugsart. Dabei versuchen Betrüger mittels gefälschter Profile in sozialen Medien eine Beziehung aufzubauen, um an Geld zu kommen. Diese Masche kennen rund drei von fünf Befragten (64 Prozent).

Kaltblütig sondergleichen: Betrüger nehmen beim "Love Scamming" Trauernde ins Visier

Update vom 3. August: Kälter und skrupelloser geht es nicht mehr. Der Betreiber mehrerer Friedhöfe in Rheinland-Pfalz warnt vor Betrügern, die sich auf seinen Facebook-Seiten an trauernde Menschen richten. Trauernde seien oft in einer verletzlichen Lebensphase und mittlerweile auch eine Zielgruppe für "Love Scammer" geworden, teilte die Deutsche Friedhofsgesellschaft, Betreiber von 14 Friedhöfen in Deutschland, mit.

Was ist "Love Scamming"?

- Mit "Live Scamming" ist eine moderne Form des "Heiratsschwindels" übers Internet gemeint. Betrüger gaukeln ihren Opfern über Fake-Profilein sozialen Medien Liebe vor. Die Kriminellen nähern sich ihnen immer mehr an über viele Nachrichten und ziehen ihnen dann das Geld aus der Tasche.

"Diese Betrüger versuchen über Facebook, das Vertrauen ihrer Opfer zu gewinnen, um sie letztlich finanziell auszunutzen", sagte Geschäftsführerin Judith Könsgen. Das Social-Media-Team habe in den vergangenen Wochen mehr verdächtige Kommentare festgestellt, die sich meist an ältere Frauen richteten.

"Hinter diesen scheinbar harmlosen Nachrichten steckt eine perfide Strategie: Die Betrüger versuchen, durch wiederholte Kontaktversuche Vertrauen aufzubauen", sagt Könsgen. Dann werde Geld gefordert. Verdächtige Kommentare würden gelöscht und Profile gemeldet, sagte die Geschäftsführerin. Dennoch wünsche sie sich von Facebook mehr Unterstützung und schnellere Reaktionen.

Autofahrer bei Betrug mit QR-Codes im Visier

Update vom 2. August: Den QR-Code scannen, Bezahl-Daten eingeben, Auto aufladen, weiter fahren. Klingt einfach. Aber Vorsicht: E-Autofahrer sollten sich den QR-Code-Aufkleber öffentlicher Ladesäule genau anschauen. Das Magazin "Auto, Motor und Sport" (17/2024) berichtet über eine Betrugsmasche mit gefälschten QR-Code-Aufklebern . Es habe Fälle in ganz Europa gegeben. In Deutschland sind bisher nur Fälle in Berlin bekannt, doch solche Maschen können sich schnell ausbreiten.

Scannt man den gefälschten QR-Code, landet man auf einer Bezahlseite, wo die Kreditkartendaten der ahnungslosen Opfer von Betrügern abgegriffen werden. "Quishing" nennt sich das, also Phishing per QR-Code. Auch aus anderen Ländern seien Fälle bekannt - etwa Belgien, den Niederlanden, Frankreich, Spanien, Italien.

Der Verdacht laut "Auto, Motor und Sport": Möglicherweise versuchten die Betrüger, mit Störsendern die Nutzung der App zu verhindern und so E-Autofahrer zum Scannen des Codes zu zwingen. Das Laden funktionierte in der Regel wie gewohnt. So landeten die E-Autofahrer zunächst auf einer Internetseite, die der Webseite des Ladesäulen-Betreibers zum Verwechseln ähnlich sah. Dort gaben die E-Autofahrer ihre Bezahldaten ein, aber gelangten nicht an den Strom. Zunächst. Perfide: Die Cyber-Kriminellen hatten den Vorgang aber wohl so programmiert, dass Kunden im zweiten Anlauf auf der richtigen Webseite des Lade-Dienstleisters landen - und so dem ersten Fehlversuch keine Bedeutung beimaßen.

Autofahrer sollten nachsehen, ob hinter dem Aufkleber ein zweiter QR-Code des eigentlichen Betreibers steckt. Manche zeigen auch einen Code auf dem Display. Dann besser diesen scannen - die QR-Code-Aufkleber können einfacher manipuliert werden. Wenn möglich, immer die Lade-App des Betreibers oder das Kreditkarten-Lesegerät nutzen. Erscheint eine hohe Summe im Display, die abgebucht werden soll, oder kommt Nutzern die Webseite des Betreibers seltsam vor, besser den Vorgang abbrechen und die Kreditkarte zur Sicherheit sperren. Im Zweifel an den Betreiber oder die Polizei wenden, um auf den möglichen Betrug aufmerksam zu machen.

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/elster-warnt-vorsicht-gefaelschten-e-mails-steuerverwaltung-39980558

Anwenderinformationen:

1) Handy-Hacks – Eigene Rufnummer anzeigen: So finden Sie Ihre Nummer

Wenn Sie Ihre eigene Handynummer vergessen haben, können Sie diese auch anzeigen lassen. Wie das geht, hängt allerdings von ihrem Smartphone ab. Eine Anleitung.

Sie werden häufiger nach Ihrer Handynummer gefragt, haben sie aber nicht im Kopf? Einige Menschen schaffen es, sich diese mit der Zeit zu merken. Das geht aber längst nicht allen so. Wir verraten Ihnen daher, wie Sie Ihre Nummer sowohl auf Android-Handys als auch iPhones in kurzer Zeit ausfindig machen können.

So sehen Sie Ihre eigene Rufnummer bei Android-Handys

Auf Android-Smartphones können Sie sich Ihre Rufnummer ganz einfach anzeigen lassen:

1. Öffnen Sie das Einstellungsmenü auf Ihrem Telefon.
2. Scrollen Sie zu "Geräteinformationen"/"Über das Telefon".
3. Wählen Sie den Menüpunkt "Status" aus.
4. Im Bereich "Meine Telefonnummer" finden Sie Ihre Rufnummer.

Je nach Android-Version lauten die Namen der richtigen Quelle etwas anders. Bei einem Samsung S22 finden Sie die Informationen beispielsweise in der Rubrik "Telefoninfo" und dort dann unter "Status".

Eigene Rufnummer auf dem iPhone anzeigen lassen

Auch bei einem iPhone dauert es meist nur wenige Sekunden, bis Sie Ihre Rufnummer ermittelt haben. Wie bei Android-Handys haben Sie die Möglichkeit, über das Einstellungsmenü zu gehen. In der Rubrik "Telefon" finden Sie dort Ihre eigene Nummer. Es gibt aber noch eine weitere Option, die wie folgt funktioniert:

1. Öffnen Sie auf dem Gerät die Telefon-App.
2. Wählen Sie die Rubrik "Kontakte" aus.
3. Tippen Sie auf Ihren eigenen Namen, der sich neben Ihrem Profilbild befindet.
4. Ihre eigene Nummer wird nun angezeigt.

Gut zu wissen: Die meisten Android-Telefone haben diese Funktion auch. Probieren Sie die Suche über die Kontakte daher einfach mal aus.

Rufnummer per MMI-Code abfragen

Auch für diese Option benötigen Sie Ihr Smartphone, denn den MMI-Code (MMI steht für Man-Machine-Interface, auf Deutsch: Mensch-Maschinen-Schnittstelle) können Sie nur darüber versenden. Das funktioniert folgendermaßen:

1. Öffnen Sie das Anrufmenü Ihres Telefons.
2. Geben Sie über die Tastatur den MMI-Code Ihres Netzanbieters ein.
3. Senden Sie den Code durch Druck auf die Anruftaste ab.
4. Lesen Sie Ihre Rufnummer von der Textmeldung ab, die Ihnen nach wenigen Sekunden geschickt wird.

Der Netzanbieter O2 bietet zur Rufnummernabfrage keinen MMI-Code, sondern eine Telefonnummer. Rufen Sie kostenlos die Nummer **(0800) 9377546** an und halten Sie Zettel

und Stift bereit. Ihre Rufnummer wird Ihnen von einer Computerstimme angesagt.

Wenn Sie eine Prepaid-Karte von Aldi, Edeka oder einem anderen Anbieter nutzen, ist ebenfalls der Netzanbieter für den jeweiligen Code maßgebend.

Quelle: https://www.t-online.de/digital/smartphone/id_100463350/eigene-rufnummer-anzeigen-so-finden-sie-ihre-nummer.html

2) Tipp – Microsoft Excel: So schalten Sie automatische Formatierungen ab

Excel formatiert bestimmte Eingaben automatisch, was oft nützlich, aber manchmal störend ist. Diese Automatik lässt sich nun individuell deaktivieren, wir zeigen wie.

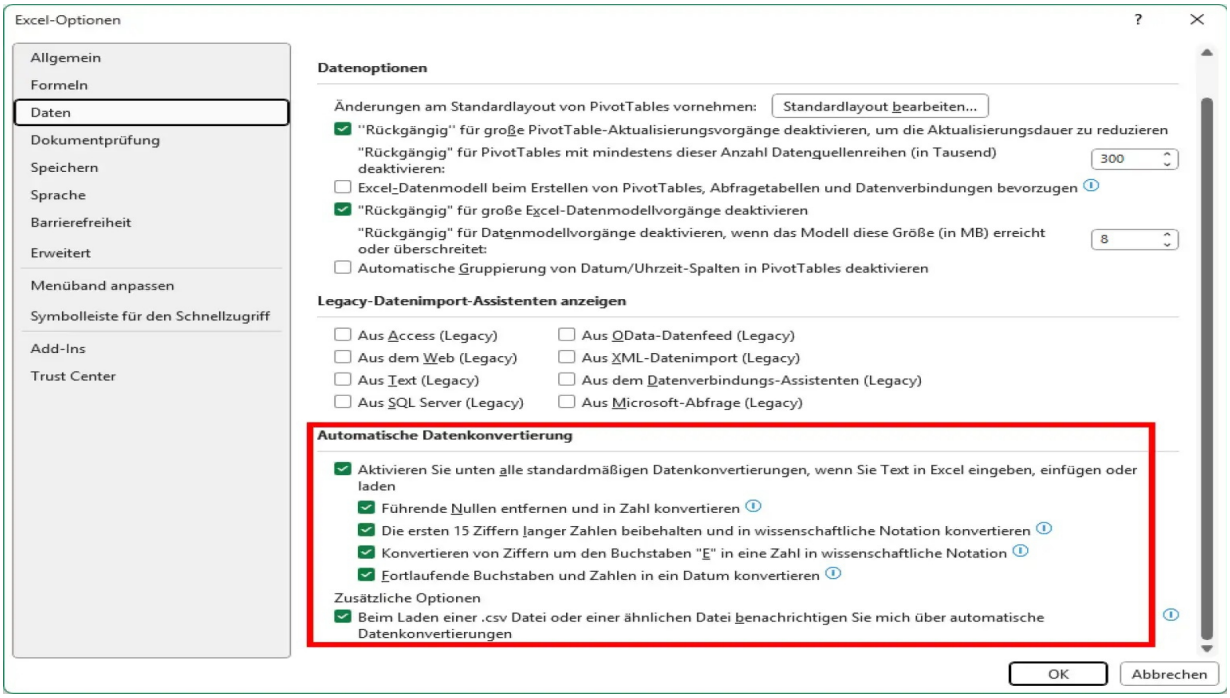
Excel reagiert auf bestimmte Buchstaben- und Zahleneingaben mit einer automatischen Formatierung. Das ist in den meisten Fällen sinnvoll, kann manchmal aber auch sehr störend sein, da der Benutzer dann über „Start –› Format –› Zellen formatieren“ wieder auf die gewünschte Formatierung umstellen muss.

Seit einigen Monaten bringt die Tabellenkalkulation allerdings eine Reihe von Optionen mit, über die Sie die unerwünschten Automatismen deaktivieren können.

Sie finden diese Einstellungen über „Datei –› Optionen –› Daten“ im Abschnitt „Automatische Datenkonvertierung“. Es geht um die folgenden Funktionen:

„Führende Nullen entfernen und in Zahl konvertieren“: Wenn Sie etwa den Wert *0009* in eine Zelle schreiben, kürzt ihn Excel automatisch in „9“ ab.

„Die ersten 15 Ziffern langer Zahlen beibehalten und in wissenschaftliche Notation konvertieren“: Geben Sie beispielsweise die Zahl *3520345723544235874452337844560238967* in eine Zelle ein, kürzt Excel sie auf 15 Ziffern zusammen und stellt sie in wissenschaftlicher Notation in der Form 3,52034572354423E+36 dar.



Bei der Eingabe führt Excel in vielen Fällen automatisch eine Konvertierung durch. Über eine Reihe von noch recht neuen Optionen können Sie dies verhindern. Bild IDG

„Konvertieren von Ziffern um den Buchstaben ‘E’ in eine Zahl in wissenschaftliche Notation“: Excel macht aus sämtlichen Zeichenfolgen, in denen der Buchstabe „E“ enthalten ist, eine Zahl in wissenschaftlicher Notation. Wenn Sie zum Beispiel *44E88* eintippen, verwandelt es den Zellinhalt in „4,4E+89“.

„Fortlaufende Buchstaben und Zahlen in ein Datum konvertieren“: Aus der Eingabe „01-03-24“ wird so auf dem Tabellenblatt „01.03.2024“.

Um diese automatischen Konvertierungen bei der Eingabe und beim Einfügen von Texten oder Ziffern zu verhindern, löschen Sie die Häkchen vor den entsprechenden Optionen.

Über die Option „Beim Laden einer .csv-Datei oder einer ähnlichen Datei benachrichtigen Sie mich über automatische Datenkonvertierungen“ können Sie darüber hinaus festlegen, dass Sie beim Öffnen eines CSV-Files über eventuelle Konvertierungen auf den Tabellenblättern informiert werden.

Quelle: https://www.pcwelt.de/article/2416902/microsoft-excel-so-schalten-sie-automatische-formatierungen-ab.html?utm_date=20240826114458&utm_campaign=Best-of%20PC-WELT&utm_content=Title%20Story%3A%20Microsoft%20Excel%3A%20So%20schalten%20Sie%20automatische%20Formatierungen%20ab&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) News – Neue Malware Banshee Stealer versucht, Daten von Macs zu stehlen

Die in Malware-Foren angebotene Version versucht Daten und Kryptowährungen von Macs zu entwenden – außer der Mac nutzt die russische Sprache.

Eine neue Malware, die sich auf Macs spezialisiert hat, haben letzten Donnerstag Sicherheitsforscher von Elastic Security Labs entdeckt. Die von den Entdeckern Banshee Stealer getaufte Software wird als Dienstleistung in Untergrundforen angeboten und ermöglicht Angreifern das Abfangen von Systeminformationen, Browserdaten und Krypto-Wallets eines Macs.

So arbeitet die Malware

Gelangt der sogenannte „Stealer“ auf einen Mac –etwa als vermeintliche Freeware oder Phishing –versucht er Daten von Browsern und dem System zu stehlen. So stiehlt das Tool unter anderem Schlüsselbunddateien, Safari-Cookies, Notizen und bestimmte Arten von Dokumenten. Außerdem zeigt die Malware einen Eingabedialog und versucht so den Nutzer zur Eingabe seines Passwortes zu verleiten. Mit diesem Passwort könnten später Passwortdaten des Systems entschlüsselt werden.

Zusätzlich werden History, Cookies und Anmeldedaten der Browser Chrome, Firefox, Brave, Edge, Vivaldi, Yandex, Opera gestohlen. (Von Safari nur Cookies). Die Daten von über hundert Browsererweiterungen versucht das Tool ebenfalls zu erfassen. Gezielt stiehlt die Software die Wallets der Krypto-Apps Exodus, Electrum, Coinomi, Guarda, Wasabi Wallet, Atomic und Ledger und versendet die gesammelten Daten an die Malware-Autoren.

Laut der Einschätzung von Elastic Search ist die Malware nicht sehr komplex und beinhaltet nur wenig Schutzvorkehrungen gegen ihre Entdeckung. Allerdings überprüft sie, ob sie in einer virtuellen Maschine läuft und erkennt Debugging. Automatisch erkennt das Tool, ob ein System die russische Sprache nutzt und infiziert es dann nicht. Das ist eine gängige Methode russischer Hacker, um Ärger mit den eigenen Strafverfolgungsbehörden zu vermeiden.

Die einzelnen Module, aus denen die Malware besteht, sind offenbar ebenfalls nicht wirklich neu. Die große Menge an Daten, die das Tool stehlen kann, machen es aber nach Einschätzung von Elastic Security Labs zu einer echten Bedrohung für die Mac-Plattform. Laut der Seite „The Hacker News“ ist die neue Malware im Rahmen einer großen Welle ähnlicher Malware wie Flame Stealer, Braodo Stealer und Rhadamanthys Stealer zu sehen, die aber bisher nur Windows-Systeme angreifen.

Die offenbar von russischen Hackern angebotene Software wird für 3.000 Dollar pro Monat verkauft. Laut Forschern ist dies ein deutlich höherer Preis, als er für Tools verlangt wird, die PCs befallen.

Die Software sollte von den besseren Antivirenprogrammen wie Bitdefender und Avast mittlerweile erkannt werden, wie unsere aktuelle Abfrage der Malware bei Virustotal ergab.

Die Malware wird noch nicht von allen Antivirenprogrammen erkannt.

Quelle: https://www.macwelt.de/article/2430117/neue-malware-banshee-stealer-versucht-daten-von-macs-zu-stehlen.html?utm_date=20240826124320&utm_campaign=Macwelt%20Daily&utm_content=Title%20Story%3A%20Neue%20Malware%20Banshee%20Stealer%20versucht%2C%20Daten%20von%20Macs%20zu%20stehlen&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Überraschung bei Samsung: Praktische neue Funktion kommt jetzt auf ältere Geräte

Samsung hat für viele Galaxy-Nutzer eine Überraschung parat. Eine praktische neue Funktion steht nun auch für ältere Geräte zur Verfügung.

Samsung erweitert die Funktion "Circle to Search" nun auf zahlreiche ältere Modelle. Auch einige Galaxy A Serien-Smartphones und Galaxy Tab S9 FE Tablets erhalten sie.

Samsung rollt seit August 2024 ein Update aus, das die neue Funktion "Circle to Search" auf viele Galaxy-Geräte bringt. Wie "Android Police" berichtet, erhalten mehr als 25 Millionen Smartphones und Tablets weltweit die Funktion. "Circle to Search" wurde erstmals im Januar 2024 mit der Galaxy S24 Serie eingeführt.

"Circle to Search": Diese Samsung-Geräte erhalten das Update

Zunächst sollten nur ausgewählte Galaxy A Series-Smartphones und Galaxy Tab S9 FE Tablets das Update erhalten. Überraschenderweise sollen auch einige Galaxy Quantum, Galaxy S21 FE und Tab S9 FE Geräte integriert werden. Das Update bringt Circle to Search somit auf noch mehr Modelle als ursprünglich angekündigt.

Diese Geräte erhalten das Feature mit dem August-Update:

- Galaxy A34
- Galaxy A54
- Galaxy A35
- Galaxy A55
- Galaxy Quantum 4
- Galaxy S21 FE
- Galaxy Tab S9 FE
- Galaxy Tab S9 FE+

Quelle: https://www.chip.de/news/Update-bringt-praktische-Funktion-auf-aeltere-Samsung-Galaxy-Geraete_185434953.html?utm_source=flipboard&utm_content=topic%2Fde-digital

5) So kannst du Dokumente auf dem iPhone scannen

Du willst Schriftstücke digitalisieren, hast aber keinen Scanner parat? Dann kannst du deine Dokumente auch mit dem iPhone scannen. Wir zeigen dir, wie das geht.

Das Smartphone kann in vielen Lebenslagen hilfreich sein. Zum Beispiel, wenn du ein Dokument scannen musst, aber keinen Zugriff auf einen Scanner hast. Das iPhone bietet dir hierfür gleich mehrere Möglichkeiten. Wir erklären dir, wie du mit deinem iPhone Dokumente scannen kannst.

Dokumente mit dem iPhone scannen – so geht's

Die erste Möglichkeit, um mit deinem iPhone Dokumente zu scannen, bietet die Notizen-App. Damit kannst du nicht nur ein Dokument einscannen, sondern es sogar auch direkt unterzeichnen.

Öffne hierfür die Notizen-App auf deinem iPhone. Erstelle nun eine neue Notiz oder öffne eine bereits vorhandene. Klicke nun das Kamera-Symbol am unteren Bildschirmrand an. Das iPhone schlägt dir nun vier Möglichkeiten vor:

- Foto oder Video auswählen
- Dokument scannen
- Foto oder Video aufnehmen
- Text scannen

Wähle die Option „**Dokument scannen**“ aus. Positionieren dein Dokument und halte dann die Kamera deines iPhones darüber. Ist es zu dunkel, kannst du für die Aufnahme auch den Blitz einschalten. Außerdem ist es möglich, den Scan in Farbe, Graustufen, Schwarzweiß oder als Foto zu erstellen.

Oben rechts in der Ecke siehst du, in welchem Modus der Dokumentenscanner eingestellt ist. Dort kannst du zwischen „**Automatisch**“ und „**Manuell**“ wählen. Ist der Modus „Automatisch“ eingestellt, scannt dein iPhone das Dokument, sobald es dieses erkannt hat. Hast du hingegen den Modus „Manuell“ ausgewählt, musst du selbstständig den Auslöser betätigen.

Ist dein Dokument gescannt, kannst du es noch zuschneiden oder nach deinen Wünschen bearbeiten. Anschließend bestätigst du den Scan mit der Taste „**Sichern**„.

Diese Alternativen gibt es zum Scan in der Notizen-App

Alternativ kannst du Dokumente auch in der Dateien-App auf dem iPhone scannen. Sie werden dann nicht in den Notizen, sondern deiner iCloud-Datenbank abgelegt.

In der Dateien-App siehst du in der oberen rechten Ecke drei Punkte in einem Kreis. Wenn du diesen antippst, findest du die Option „Dokumente scannen„. Es öffnet sich dieselbe Ansicht wie in der Notizen-App, auch die Optionen für deinen Scan sind gleich.

Natürlich kannst du auch einfach ein Foto von deinem Dokument machen. Allerdings bietet dir die Scannen-Option auf dem iPhone Vorteile wie das automatische Zuschneiden. Außerdem werden deine Scans direkt automatisch entzerrt, wenn du die Kamera schief über das Dokument gehalten hast.

Quelle: https://www.basicthinking.de/blog/2024/08/23/dokumente-iphone-scannen/?utm_source=flipboard&utm_content=topic%2Fde-technologie

6) Kurioser Rettungsanker für Ihren PC: Wann Sie 3 mal starten müssen

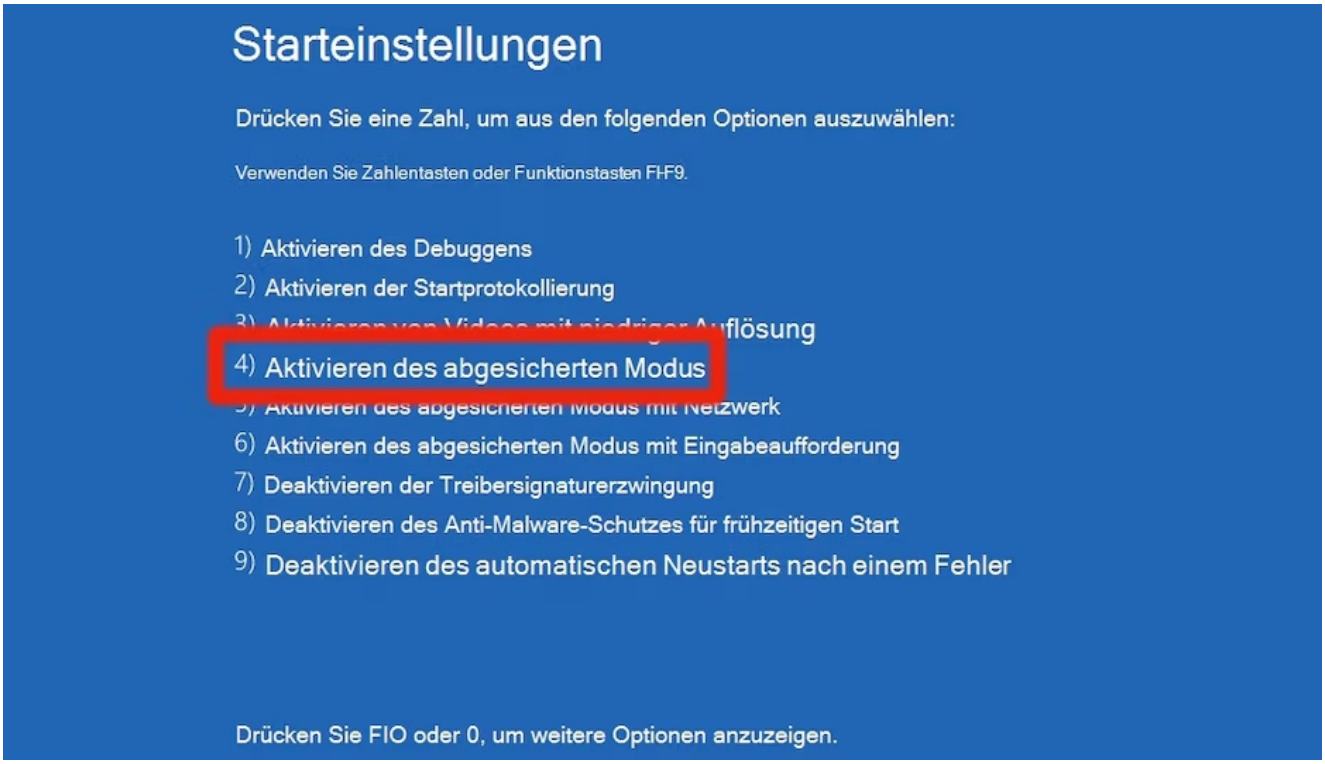
Windows startet automatisch nach dem Einschalten des PCs, wenn alles in Ordnung ist. Klappt der normale Windows-Start nicht, ist der abgesicherte Modus oft ein Rettungsanker. Dazu starten Sie Windows 3 Mal neu.

Als CrowdStrike kürzlich Millionen PCs weltweit in eine Bluescreen-Schleife schickte, kam als Notfalllösung schnell der abgesicherte Modus von Windows ins Spiel. Den gibt es gefühlt schon ewig und er startet ein Windows mit minimaler Ausstattung, um Fehler zu beheben.

Doch wie kommt man in den abgesicherten Modus? Wenn Windows noch läuft, kann man bequem per Menü die erweiterten Startoptionen anzeigen lassen. Noch schneller geht es, wenn Sie über das Startmenü einen Neustart machen und dabei die Umschalttaste gedrückt halten.

Spuckt Windows aber nur noch Bluescreens aus, wird es kniffliger. Denn eine normale Bedienung von Windows ist dann nicht mehr möglich. Einen kuriosen Trick, den Microsoft auch auf seinen Support-Seiten dokumentiert, kann man sich aber einfach merken. Starten Sie **Windows 3 Mal hintereinander neu**.

3 Mal neu starten mit Netzschalter



Der abgesicherte Modus lässt sich aus den Starteinstellungen auswählen. Bild: Microsoft, CHIP

Lässt sich Windows auf normalen Wegen nicht mehr bedienen, greift der Trick mit dreimaligem Neustart. Der bringt Sie nämlich in die Windows-Wiederherstellungsumgebung, in der Sie bequem die verschiedenen Startoptionen auswählen können, unter anderem den abgesicherten Modus:

1. Ausgangsbasis ist ein komplett ausgeschalteter Computer.
2. Starten Sie Ihr Gerät und warten Sie, bis das Windows-Logo bzw. das Logo des PC-Herstellers angezeigt wird.

3. Sobald Sie das Logo sehen, halten Sie den Netzschalter gedrückt, bis das Gerät heruntergefahren wird; damit unterbrechen Sie den Startvorgang.
4. Schalten Sie Ihr Gerät erneut ein, und wiederholen Sie das beschriebene Prozedere mit gedrücktem Netzschalter ein zweites Mal; damit haben Sie erneut den Startvorgang abgebrochen und das merkt sich Windows.
5. Schalten Sie Ihr Gerät jetzt ein drittes Mal normal ein, also ohne den Netzschalter gedrückt zu halten. Windows sollte in diesem dritten Anlauf, nach zwei Startabbrüchen, in den automatischen Reparaturmodus booten.
6. Windows zeigt einen blauen Bildschirm an, mit dem Hinweis, dass Ihr PC nicht korrekt gestartet wurde; klicken Sie auf **Erweiterte Optionen**.
7. Hangeln Sie sich über **Problembehandlung** > **Erweiterte Optionen** > **Starteinstellungen** > **Neu starten** weiter.
8. Ist Ihr Gerät verschlüsselt, müssen Sie den Bitlocker-Wiederherstellungsschlüssel eingeben. Wer ein Microsoft-Konto für den Windows-Login nutzt, kann den Key online bei Microsoft abrufen. Ansonsten haben Sie ihn möglicherweise auch bei der Einrichtung auf einem USB-Stick abgelegt.
9. Windows zeigt Ihnen jetzt die verschiedenen Startoptionen, darunter den abgesicherten Modus.

Quelle: https://www.chip.de/news/Kurioser-Rettungsanker-fuer-Ihren-PC-Wann-Sie-Windows-3-Mal-neu-starten-muessen_185434131.html?utm_source=chip_1001310&utm_medium=email&utm_campaign=1015021&utm_content=26.08.2024

7) Neue Funktion – WhatsApp geht gegen Spam-Nachrichten vor

WhatsApp entwickelt eine Möglichkeit, mit der Nutzer die Nachrichten unbekannter Kontakte blockieren können. Was über die neue Funktion bekannt ist.

Der beliebte Messenger WhatsApp testet derzeit eine Funktion, mit der Nutzer sich vor nervigen Spam-Nachrichten schützen können. Wie das Informationsportal "WABetaInfo" berichtet, sei in einer Vorabversion der Anwendung für Android-Telefone eine Funktion eingebaut, mit der sich Nachrichten von unbekannten Kontakten blockieren lassen.

Wenn die Option in den Einstellungen aktiviert sei, blockiere WhatsApp automatisch solche Nachrichten und schütze seine Nutzer damit vor unerwünschten oder potenziell schädlichen Inhalten.

Positiver Nebeneffekt: Durch die Aktivierung der Funktion werde automatisch die Datenmenge reduziert, die WhatsApp verarbeiten müsse. Das führe dazu, dass die Anwendung weniger Energie verbrauche und den Geräteakku schone. Zudem werde das Risiko reduziert, dass bösartige Inhalte die Leistung und den Speicher des Handys beeinträchtigen könnten.

Weitere Funktionen zum Schutz der Privatsphäre

Schon jetzt lassen sich bei WhatsApp Anrufe von unbekannten Telefonnummern stummschalten. Diese Funktion können Nutzer in Einstellungen des Messengers unter der Option "Anrufe" aktivieren.

Unter der Option "Erweitert" soll sich dann demnächst die Möglichkeit befinden, Nachrichten unbekannter Kontakt zu blockieren. Im selben Menü hatte WhatsApp bereits eine weitere Funktion zum Schutz vor schädlicher Software eingeführt: Nutzer können dort die Linkvorschau in Chats deaktivieren.

Beim Einschalten dieser Funktion generiert WhatsApp beim Senden von Links an andere

Personen keine Linkvorschauen mehr, um die IP-Adresse des Anwenders zu schützen. Diese lässt sich nämlich von Webseiten über die Linkvorschau ermitteln.

Die aktivierte Option hat laut WhatsApp aber keinen Einfluss auf Links, die der Anwender empfängt. Dort ist weiterhin eine Linkvorschau zu sehen, mit der sich aber die eigene IP-Adresse nicht herausfinden lasse.

Quelle: https://www.t-online.de/digital/aktuelles/id_100472914/whatsapp-neue-funktion-macht-es-betruegern-schwerer.html

8) Neuer Windows-Trojaner weiß alles über dich – so wirst du ihn los

Sicherheitsforschende haben eine bislang unbekannte Malware entdeckt. Der Windows-Trojaner gelangt über den Browser direkt auf deinen PC.

In den letzten Jahren sind die Bedrohungen für die Cybersicherheit zunehmend raffinierter geworden. Eine der neuesten Gefahren verbirgt sich in vermeintlich harmlosen Chrome-Erweiterungen. Laut einer Analyse des Sicherheitsdienstleisters ReasonLabs nutzt ein neu entdeckter **Windows-Trojaner** eine Reihe solcher kompromittierter Browser-Erweiterungen, um gezielt Nutzerinnen und Nutzer anzugreifen.

Windows-Trojaner verbreitet sich stillheimlich

Die Malware arbeitet auf mehreren Ebenen, von einfacher Adware, die Suchanfragen abfängt, bis hin zu fortschrittlicheren Skripten, die darauf ausgelegt sind, private Daten zu stehlen und nicht autorisierten Code auf dem System des Opfers auszuführen.

„Diese Trojaner-Malware, die seit 2021 existiert, stammt von Imitationen von Download-Websites mit Add-ons für Online-Spiele und Videos“, mahnte ReasonLabs in seiner Veröffentlichung. „Wir haben eine sehr weite Verbreitung der Malware und Erweiterungen beobachtet – insgesamt sind mindestens 300.000 Nutzer von Google Chrome und Microsoft Edge betroffen.“

Die Verbreitung des Windows-Trojaners wird größtenteils durch Malvertising begünstigt – eine Technik, bei der Angreifer Websites bewerben, die bekannte Dienste wie Roblox FPS Unlocker, YouTube, VLC Media Player, Steam und KeePass imitieren. Diese gefälschten Websites verleiten Nutzerinnen und Nutzer dazu, schädliche Software herunterzuladen, wodurch die Verbreitung der Malware weiter vorangetrieben wird.

Auch interessant: Internet-Anbieter gehackt: Angreifer machen Updates zu Viren-Schleudern

Malware macht Updates rückgängig

Die Verantwortlichen haben bemerkenswerten Einfallsreichtum bewiesen, um sicherzustellen, dass sie auf infizierten Systemen bestehen bleibt. Einmal installiert, ist es nahezu unmöglich, die Erweiterung zu deaktivieren, selbst wenn du den Entwicklungsmodus des Browsers aktivierst. Neuere Versionen der Malware gehen sogar noch einen Schritt weiter. Sie können, so ReasonLabs, Browser-Updates rückgängig machen, um die Sicherheitslücken älterer Versionen ausnutzen zu können.

Für Nutzerinnen und Nutzer mit begrenzten technischen Kenntnissen besteht die einzige zuverlässige Möglichkeit zur Entfernung der Malware in einer vollständigen Neuinstallation des Betriebssystems. Jene mit fortgeschrittenen Kenntnissen können jedoch bestimmte Schritte unternehmen, um die Bedrohung manuell zu beseitigen.

So kannst du dich schützen:

Um den Windows-Trojaner sicher zu entfernen, musst du zunächst die **geplanten Aufgaben löschen**:

1. Öffne das Startmenü und gib „Taskplaner“ ein, um den Taskplaner zu öffnen.
2. Klicke auf „Taskplaner-Bibliothek“, um alle Aufgaben auf deinem Computer anzuzeigen.
3. Suche nach einer Aufgabe, die einen Pfad zu „c:\windows\system32“ und eine Datei mit der Endung „.ps1“ (ein PowerShell-Skript) enthält. Ein Beispiel für eine solche Datei ist „Printworkflowservice.ps1“.
4. Sobald du die bösartige Aufgabe gefunden hast, klicke mit der rechten Maustaste darauf und wähle „Löschen“.

Unternimm anschließend einen Versuch, um auch die entsprechenden **Registry-Einträge zu löschen**:

1. Öffne das Startmenü und gib „Registry-Editor“ ein, um den Editor zu öffnen.
2. Navigiere zu „Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist“.
3. Im rechten Fensterbereich siehst du eine Liste von Erweiterungen. Klicke mit der rechten Maustaste auf den Namen und wähle „Löschen“.
4. Wiederhole diesen Schritt für den Pfad „Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist“ für Edge-Erweiterungen.

Zu guter Letzt musst du auch noch die verbliebenen **Malware-Dateien löschen**:

1. Öffne den Datei-Explorer über das Startmenü.
2. Gehe zu „Dieser PC“ und dann zu „Windows“ (oder dem entsprechenden Laufwerk).
3. Navigiere zu Windows > System32 und suche nach einer PowerShell-Datei, die zu den angegebenen bösartigen Skripten passt. Klicke mit der rechten Maustaste auf die Datei und wähle „Löschen“.
4. Suche in der „Windows“-Ordner nach einem Ordner, dessen Name ebenfalls zu den angegebenen bösartigen Skripten passt. Klicke mit der rechten Maustaste darauf und wähle „Löschen“.

„Benutzer sollten sich mit Antivirensoftware der nächsten Generation wie RAV Endpoint Protection oder fortschrittlichen Sicherheitstools für Endgeräte wie der Browsererweiterung Online Security vor Malware, Identitätsdiebstahl und mehr schützen“, mahnen die Expertinnen und Experten. So kannst du dich von Vornherein besser vor Windows-Trojanern schützen.

Quelle: https://www.futurezone.de/digital-life/article571927/neuer-windows-trojaner-weiss-alles-ueber-dich-so-wirst-du-ihn-los.html?utm_source=flipboard&utm_content=topic%2Fde-digital

9) Fernseher-Trick: Sofort schneller bedienbar – klappt auch mit älteren Modellen

Es gibt eine Methode, die du regelmäßig anwenden solltest. Sie hilft, deinen Smart-TV schnellstmöglich wieder auf die Beine zu bringen.

Moderne **Smart-TVs** bieten eine Menge Möglichkeiten, die weit über jene eines gewöhnlichen Fernsehers hinaus gehen. Genau aus diesem Grund brauchen sie auch einen anderen Umgang und eine Pflege, die ihre speziellen technischen Bedürfnisse trifft. Eine solche Maßnahme ist es, regelmäßig den Cache zu leeren.

Smart-TV: Darum solltest du den Cache leeren

Bekannt ist dieses Vorgehen den meisten wahrscheinlich nur von ihrem Handy. Doch auch ein Smart-TV kann deutlich besser und schneller arbeiten, sobald der Cache, also der Zwischenspeicherort verschiedenster Daten, geleert wurde. Dabei gibt es, laut Airbeam, verschiedene Optionen.

Möglichkeiten, den TV-Cache zu leeren:

- Neustart des Smart-TV
- Software-Update
- Löschen des Cache einzelner Apps
- Löschen des Browser-Cache
- Reset des Fernsehers auf die Werkseinstellungen

Nützlich ist das laut ZDNet vor allem aus zwei Gründen: Erstens kann ein aufgeblähter Cache die Verarbeitung von Prozessen durch deinen Fernsehers verlangsamen, was zu träger Navigation, verzögerten App-Starts und Pufferungsproblemen führt. Wenn du den Cache leerst, wird Speicherplatz frei und dein Fernseher kann effizienter arbeiten.

Zweitens können durch das Löschen App-spezifische Probleme behoben werden. Dazu gehören Dinge wie Abstürze, Anmeldefehler oder ein unerwartetes Verhalten deines Smart-TV in einer bestimmten Anwendung. Hier bietet dir die genannte Methode oft eine effektive Lösung.

Beachte: Das Leeren des Caches kann dazu führen, dass du dich erneut bei Apps anmelden oder Einstellungen neu konfigurieren musst. Stelle also immer erst sicher, dass du alle notwendigen Informationen zur Hand hast, bevor du den Schritt wählst.

So leerst du den App-Cache deines Smart-TV

Das genaue Vorgehen variiert wie sooft je nach Modell und Betriebssystem deines Fernsehers. Es gibt aber für den groben Überblick immer ein paar allgemeine Schritte. Die folgenden können dir zum Beispiel dabei helfen, den App-Cache auf deinem Gerät zu finden und auszuführen.

Allgemeine Anleitung für das Leeren des App-Cache:

1. Drücke die „Menü“-Taste auf deiner Fernbedienung, um das Hauptmenü des Fernsehers zu öffnen.
2. Gehe zu den „Einstellungen“.
3. Wähle „Apps“, „Anwendungen“ oder „App-Manager“, je nach Menüstruktur.
4. Wähle die App aus, deren Cache du leeren möchtest.
5. Wähle die Option „Cache leeren“ oder „Daten löschen“.

Anleitung für Android TV-Geräte:

1. Gehe zu den „Einstellungen“ deines Android TVs.
2. Navigiere zu „Apps“.
3. Wähle „Alle Apps anzeigen“.
4. Wähle die App aus, deren Cache du leeren möchtest.
5. Wähle „Speicher & Cache“ und dann „Cache leeren“.

Anleitung für Samsungs Smart-TV-Geräte

1. Drücke die „Home“-Taste auf der Fernbedienung.
2. Gehe zu „Einstellungen“.
3. Wähle „Apps“.
4. Wähle „Cache löschen“.

Anleitung für LGs Smart-TV-Geräte

1. Drücke die „Einstellungen“-Taste auf der Fernbedienung.
2. Wähle „Allgemein“.
3. Manchmal ist es notwendig, den TV auf die Werkseinstellungen zurückzusetzen. Wähle „Zurücksetzen“ und folge den Anweisungen.

Solltest du auf Schwierigkeiten stoßen, empfiehlt es sich immer, das Benutzerhandbuch deines Fernsehers zu konsultieren oder den Kundenservice des Herstellers zu kontaktieren. Beide Optionen können dir im besten Fall schnell weiterhelfen.

Lesetipp: Diese Fernseher-Tricks sorgen für ein sofort besseres Bild

Quelle: https://www.futurezone.de/digital-life/article563974/smart-tv-fernseher-schneller-bedienen-cache.html?utm_source=flipboard&utm_content=topic%2Fde-digital

10) Die fünf besten kostenlosen E-Mail-Anbieter im Vergleich

Web.de zählt zu den beliebtesten kostenlosen E-Mail-Anbietern unter Deutschen. Aber ist er auch der beste? Wir haben die Top 5 "Freemail"-Dienste für Sie unter die Lupe genommen.

Es gibt erstaunlich wenige Statistiken über das E-Mail-Verhalten der Deutschen. Fakt ist aber: Wenn es um E-Mail-Anbieter geht, nutzt der Deutsche am liebsten die, die er schon kennt, und am besten kostenlose. Doch welche kostenlosen Anbieter sind wirklich gut? Wir haben die fünf beliebtesten E-Mail-Dienste miteinander verglichen.

Des Deutschen Liebling: Web.de

Web.de ist laut Statista der beliebteste E-Mail-Anbieter in Deutschland mit über 26 Prozent Nutzeranteil im Jahr 2022. Bei Web.de werden Ihre Daten in Deutschland gespeichert und unterliegen damit dem strengen deutschen Datenschutzgesetz. In anderen Bereichen, wie beim Speicherplatz, ist der kostenlose Dienst von Web.de allerdings weniger stark:

- **Speicherplatz**: Web.de stellt ein Postfach von 1 GB für seine Nutzer zur Verfügung, hinzu kommt ein Cloud-Speicher von 2 GB in der kostenfreien Version. Das ist okay, aber reißt uns nicht unbedingt vom Hocker.
- **Anhänge**: Mit Web.de können Daten von maximal 20 MB an E-Mails angehängt werden.
- **Premium-Angebot**: Für mehr Kapazität können Sie entweder das “MailPlus”-Upgrade durchführen oder dem “Web.de Club” beitreten. MailPlus kostet 3,99 Euro im Monat und stockt Ihren Cloud-Speicher auf 7 GB auf. Zugleich können Sie im Monat bis zu 500.000 E-Mails speichern und Anhänge von maximal 100 MB versenden. Wer die Club-Variante wählt, bekommt sogar 12 GB Speicher für einen Abopreis von 6,49 Euro monatlich.
- **App**: Web.de gibt es als App für Android und iOS.
- **Sicherheit**: Bei Web.de sind Ihre E-Mails durch eine sichere Ende-zu-Ende-

Verschlüsselung geschützt. Den Cloudspeicher können Sie mit dem Web.de Tresor verschlüsseln.

Ein weiterer deutscher E-Mail-Dienst: GMX

GMX.net ist der zweitbeliebteste E-Mail-Dienst in Deutschland mit einem Anteil von rund 25 Prozent. Das Freemail-Angebot von GMX kann in vielen Punkten mit dem von Web.de mithalten:

- **Speicherplatz**: GMX stellt den Nutzern seines Gratisangebots eine Postfachgröße von 1 GB zur Verfügung. Durch die Nutzung des GMX MailCheck kann man zusätzlich 500 MB Speicherplatz freischalten, sodass insgesamt 1,5 GB kostenloser Speicher zur Verfügung stehen. Zusätzlich gibt es einen Cloud-Speicher von bis zu 2 GB.
- **Anhänge**: Bei GMX können Anhänge bis zu einer maximalen Größe von 20 MB versendet werden.
- **Premium-Angebot**: Für mehr Speicherplatz können Sie das GMX Premium-Angebot nutzen. Für 5 GB E-Mail-Speicher und 7 GB Cloud-Speicher zahlen Sie 3,99 Euro monatlich, für 10 GB E-Mail-Speicher und 12 GB Cloud-Speicher 6,49 Euro pro Monat.
- **App**: GMX bietet eine benutzerfreundliche und gut strukturierte App für Android– und iOS-Geräte.
- **Sicherheit und Datenschutz**: Die Server von GMX befinden sich in Deutschland und unterliegen daher den deutschen Datenschutzrichtlinien. Der Anbieter nutzt bei seinen E-Mails eine Ende-zu-Ende-Verschlüsselung und bietet ähnlich wie Web.de einen GMX Tresor zum Verschlüsseln des Cloudspeichers an.

Für Google-Freunde: Gmail

Gmail, der Freemail-Dienst des Suchmaschinen-Giganten Google, ist mit einem Marktanteil von 15 Prozent in Deutschland sehr beliebt, insbesondere wegen seiner Anbindung an die Google-Dienste:

- **Speicherplatz**: Gmail bietet im Vergleich zu Web.de und GMX einen großen Speicherplatz von 15 GB, der auf Google Drive, Gmail und Google Fotos verteilt ist. Wer noch mehr Speicher benötigt, kann sein Konto auf 100 GB oder mehr ab 1,99 Euro monatlich upgraden.
- **Anhänge**: E-Mail-Anhänge können bis zu einer Größe von 25 MB verschickt werden. Größere Dateien können in die Cloud geladen und per Link geteilt werden.
- **App**: Gmail bietet selbstverständlich auch eine App für Android und iOS. Die Software überzeugt durch ein übersichtliches und personalisierbares Design. Über die Protokolle POP3 und IMAP können Sie Ihre Nachrichten von Gmail auch in anderen E-Mail-Programmen abrufen.
- **Sicherheit**: Sicherheitstechnisch kann Gmail nicht mit deutschen Diensten wie GMX mithalten. Das liegt zum einen daran, dass die Server sich außerhalb der EU befinden, und zum anderen ist die Verarbeitung der Nutzerdaten durch “Datenkrake” Google nicht transparent.

Aus dem Microsoft-Universum: Outlook

Im Vergleich der besten kostenlosen E-Mail-Anbieter darf Outlook von Microsoft nicht fehlen. Wenn Sie hier eine E-Mail-Adresse erstellen, profitieren Sie – ähnlich wie bei Gmail – primär vom großen Speicherplatz des Anbieters, dank des Gratis-Service OneDrive:

- **Speicherplatz**: Outlook bietet 15 GB kostenlosen E-Mail-Speicherplatz sowie weitere 5 GB in der Cloud über OneDrive – komplett for free. Microsoft 365-Abonnenten

erhalten sogar 50 GB Speicherplatz.

- **Anhänge**: E-Mail-Anhänge können bis zu 34 MB groß sein. Bei größeren Anhängen werden diese auf die OneDrive-Cloud ausgelagert, wodurch das Limit auf 5 GB steigt.
- **Microsoft-Dienste**: Outlook arbeitet perfekt mit anderen Microsoft-Diensten wie Word und Excel zusammen.
- **App**: Es gibt sowohl eine Outlook-App für Android und iOS als auch die Möglichkeit, Outlook über POP3 und IMAP in jeder beliebigen Mail-Software einzurichten.
- **Sicherheit**: In puncto Sicherheit schneidet Outlook nur mittelmäßig ab. Die strengen EU-Datenschutzrichtlinien kommen nicht zur Anwendung, und die Server sind weltweit verteilt.

Beliebt bei Telekom-Kunden: T-Online

T-Online ist der E-Mail-Dienst der Deutschen Telekom und daher vordergründig für Telekom-Kunden von Interesse. Der Freemail-Service ist jedoch für alle offen. Seine Funktionen und Konditionen können sich sehen lassen:

- **Speicherplatz**: T-Online bietet 1 GB kostenlosen Speicherplatz für E-Mails und weitere 3 GB Cloud-Speicher über MagentaCLOUD (Telekom-Kunden erhalten sogar 15 GB). Zusätzlicher Speicherplatz kann bei Bedarf gebucht werden.
- **Anhänge**: E-Mail-Anhänge können bis zu 32 MB groß sein.
- **Premium-Angebot:** Wer mehr E-Mail-Speicher benötigt, kann auf den Mail-M-Tarif für 2,95 Euro monatlich upgraden (Mindestlaufzeit 3 Monate). Dieser bietet 15 GB E-Mail-Speicher sowie 3 GB Cloud-Speicher über MagentaCLOUD (für Nicht-Telekom-Kunden) oder 15 GB Cloud-Speicher (für Telekom-Kunden) mit buchbaren Optionen.
- **App**: T-Online bietet eine App für Android und iOS, die eine einfache Verwaltung der E-Mails ermöglicht.
- **Sicherheit**: Mit Serverstandorten in Deutschland, Sicherheitsfunktionen wie Spamschutz und Ende-zu-Ende-Verschlüsselung sowie deutschen Datenschutzrichtlinien gehört T-Online zu den sichersten kostenlosen E-Mail-Anbietern.

E-Mail-Dienste im direkten Vergleich

E-Mail-Dienst	Web.de	GMX.net	Google Gmail	Microsoft Outlook	T-Online
Speicherplatz	1 GB E-Mail-Speicher 2 GB Cloud-Speicher	1 GB + 500 MB E-Mail-Speicher 2 GB Cloud-Speicher	15 GB Speicher für Gmail, Cloud (Drive) und Google Fotos	15 GB E-Mail-Speicher, 5 GB Cloud-Speicher	1 GB E-Mail-Speicher, 3 GB Cloud-Speicher (15 GB für Telekom-Kunden)
Anhänge (Größe)	20 MB	20 MB	25 MB	34 MB	32 MB
Kosten für mehr Speicher	ab 3,99 Euro mtl.	ab 3,99 Euro mtl.	ab 1,99 Euro mtl.	ab 7,00 Euro mtl. (Microsoft 365-Abo)	ab 2,95 Euro mtl.
App	Android, iOS	Android, iOS	Android,	Android, iOS	Android, iOS

Sicherheit	hoch, Server in DE	hoch, Server in DE	iOS mittel, ausländische Server, intransparenter Datenschutz	mittel, ausländische Server	hoch, Server in DE

Tipp: Möchten Sie außerdem wissen, wie Sie Ihr E-Mail-Postfach vor zu viel Spam schützen können? Das verrät Ihnen dieser Artikel.

Google Drive: Dateien gelöscht, Speicher trotzdem noch voll – so lösen Sie das Problem

11) Nach Insolvenz – Weltbild-Kunden verlieren Zugriff auf E-Books – das sollten Sie tun

Nach der Weltbild-Pleite sind dort gekaufte Hörbücher und E-Books demnächst nicht mehr zum Herunterladen verfügbar. Kunden sollten schnell handeln.

Der insolvente Online-Händler Weltbild stellt seinen Geschäftsbetrieb ein. Das hat Konsequenzen für Besitzer der E-Book-Reader von Tolino, die dort ihr Bücher und Hörbücher digital gekauft haben, wie Weltbild in einer E-Mail an seine Kunden schreibt.

Die Nachricht liegt unter anderem dem IT-Magazin "Golem" vor, das aus der E-Mail mit dem Betreff "Wichtige Kundeninformation: Betriebsstilllegung zum 31.08.2024" zitiert. Das Unternehmen weise darauf hin, dass der Zugriff auf bei Weltbild erworbene E-Books und Hörbücher nur noch bis Ende August möglich sei, heißt es.

Inhalte auf den PC herunterladen

Weltbild hat auf seiner Internetseite eine Anleitung veröffentlicht, wie Kunden ihre Inhalte offline speichern können. Gekaufte E-Books und Hörbücher könnten heruntergeladen und "auf Ihrem persönlichen Gerät" wie PC, Tablet oder Smartphone gespeichert werden, schreibt das Unternehmen.

So geht's:

- 1. Öffnen Sie den Tolino Webreader in Ihrem Browser. Die Adresse lautet: https://webreader.mytolino.com/library/index.html#/.
- 2. Melden Sie sich im Tolino Webreader an.
- 3. Nach der Anmeldung können Sie unter "Meine Bücher" und "Meine Hörbücher" auf alle bei Weltbild gekauften Inhalte zugreifen.
- 4. Klicken Sie auf die drei Punkte unter dem jeweiligen Titelbild und wählen Sie "Herunterladen" aus, um die Datei auf Ihrem PC zu speichern.

Anschließend können Sie die auf ihrem PC gespeicherten Inhalte entweder dort gespeichert lassen oder über den Tolino-Webreader bei einem anderen Buchhändler wie Thalia, Hugendubel oder bücher.de hochladen.

Inhalte bei einem anderen Dienst hochladen

So können Sie weiterhin von jedem Ort mit einem Internetzugang auf Ihre bei Weltbild gekauften Inhalte zugreifen. Eine Voraussetzung dafür ist, dass Sie bei einem dieser anderen Anbieter ein Kundenkonto besitzen.

So geht's:

- 1. Öffnen Sie den Tolino-Webreader in Ihrem Browser.
- 2. Wählen Sie einen Buchhändler der Tolino-Allianz (außer Weltbild) aus und melden sich mit dem Kundenkonto an.
- 3. Wechseln Sie in den Bereich "Meine Bücher" oder "Meine Hörbücher".
- 4. Klicken Sie innerhalb des Menüs auf "Hochladen" und wählen Sie alle E-Books und Hörbücher auf Ihrem PC aus.
- 5. Die E-Books und Hörbucher werden anschließend in die Tolino-Cloud geladen und als neue Titel angezeigt.

Weltbild hatte in der vergangenen Woche mitgeteilt, den Geschäftsbetrieb nach seiner im Juni gestellten Insolvenz zu Ende August endgültig einstellen zu wollen.

Der vorläufige Insolvenzverwalter Christian Plail teilte mit, die 14 Filialen des Unternehmens führten noch Räumungsverkäufe durch und würden dann geschlossen. Online-Käufe würden bis Monatsende noch ausgeliefert.

Quelle: https://www.t-online.de/digital/aktuelles/id_100471952/weltbild-insolvenz-kunden-verlieren-zugriff-auf-e-books-das-sollten-sie-tun.html

12) Sofort löschen: 2 Routenplaner-Apps verfolgen jeden deiner Schritte

Für die Navigation sind entsprechende Anwendungen im Auto längst unerlässlich. Doch nicht in jedem Fall sind sie auch empfehlenswert.

Google Maps und Apple Maps sind die wahrscheinlich bekanntesten Vertreter unter den Routenplanern. Dazu gesellt sich eine Vielzahl an vergleichbaren oder zumindest ähnlichen Anwendungen, die bei der täglichen Navigation helfen sollen. Einige dieser **Apps wieder zu löschen**, ist allerdings keine schlechte Idee wie Expert*innen zeigen.

Routenplaner: Diese 2 Apps solltest du löschen

Das Portal Mobilsicher, das vom Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz gefördert wird, untersucht immer wieder in sogenannten Schnelltests, wie sich Anwendungen (wie zum Beispiel Routenplaner) im Hintergrund zusammensetzen. Dabei kennzeichnet man mit einem Ampelsystem unter anderem die Anzahl der verbauten Tracker. Eine rote Markierung bedeutet entsprechend nichts Gutes und zeigt, welche Apps man löschen sollte, um die Privatsphäre zu schützen.

In ebendiese Kategorie fallen dem AppChecker von Mobilsicher zufolge die folgenden beiden Exemplare: **GPS Karten & Mein Standort (Navegante Maps) und MAPS.OSM – Offline Karten. Nav (we love maps).** Beide wurden allein über den Google Play Store jeweils mehr als eine Million Mal heruntergeladen, sind also entsprechend weit verbreitet.

Was die Routenplaner so ungemütlich macht, sind die jeweils elf implementierten Tracker sowie zahlreiche Zugriffe auch ohne erforderliche Zustimmung.

Das steckt in den Routenplanern

Zu beiden Anwendungen heißt es als Resultat des Schnelltests: „In der Installations-Datei der App haben wir Hinweise auf eingebaute Software-Module von einem oder mehreren Drittanbietern gefunden. Diese Analyse ermöglicht nur eine grobe Einschätzung der App. Apps nehmen im Betrieb meistens noch zu weiteren Anbietern Kontakt auf. Umgekehrt werden nicht alle gefundenen Anbieter in jedem Fall kontaktiert."

Unter den insgesamt identifizierten Anbietern finden sich sogenannte Datenhändler, Identitätsprovider und Dienste zur Nutzungsanalyse, aber auch bekannte Datenkraken wie Google, Facebook und Amazon. Dazu kommen fünf beziehungsweise zehn erforderliche Zugriffe, von denen entweder alle oder die meisten als „nicht zustimmungspflichtig" gelten.

Darunter:

- Auf alle Netzwerke zugreifen
- Auf zusätzliche Dienstanbieterbefehle für Standort zugreifen
- Netzwerkverbindungen abrufen
- Nur für System-Apps und vorinstallierte Apps
- SD-Karteninhalte ändern oder löschen (ungültig ab Android 10.0)
- SD-Karteninhalte lesen (ungültig ab Android 10.0)
- Vibrationsalarm steuern
- WLAN-Verbindungen abrufen

Interessant ist, dass sowohl die Entwickler*innen hinter GPS Karten & Mein Standort also auch hinter MAPS.OSM – Offline Karten laut dem Google Play Store angeben, „keine Daten werden mit Drittunternehmen oder -organisationen geteilt". Die Apps zu löschen, könnte auch aus diesem widersprüchlichen Aspekt heraus eine gute Idee sein.

Quelle: https://www.futurezone.de/digital-life/apps/article569320/sofort-loeschen-2-routenplaner-apps-verfolgen-jeden-deiner-schritte-vertreter.html

13) Perfide Whatsapp-Masche: So kapern Betrüger euren Account – und so verhindert ihr das

Whatsapp-Nutzer:innen müssen derzeit auf der Hut sein. Denn Hacker:innen wollen euren Account mit einer perfiden Masche übernehmen. Wie ihr diese erkennt und euch davor schützen könnt, haben wir für euch zusammengefasst.

Der Messenger Whatsapp ist aufgrund seiner enormen Beliebtheit immer wieder das Ziel von Hacker:innen und anderen Cyberkriminellen. Wie Watchlist Internet berichtet, gibt es aktuell eine weitere Masche, mit der Whatsapp-Nutzer:innen und deren Accounts ins Visier genommen werden.

Whatsapp-Account in Gefahr: So gehen die Kriminellen vor

Zunächst erhaltet ihr von einer unbekannten Nummer eine SMS. Darin steht folgender Text oder eine Abwandlung davon: „Das Whatsapp-Sicherheitscenter hat festgestellt dass ihr Konto gefahrdet ist Bitte gehen sie zur Uberprufung zum offiziellen Sicherheitscenter: whatsapp.cc". Schon auf den ersten Blick sind Rechtschreibfehler und fehlende Interpunktion ersichtlich, was auf einen Fake hindeutet.

Solltet ihr auf den enthaltenen Link klicken, werdet ihr zu einer gefälschten Seite weitergeleitet, die wie eine Help-Center-Website von Whatsapp aufgebaut ist. Dort behaupten die Kriminellen, dass es ungewöhnliche Aktivitäten in eurem Whatsapp-Account

gegeben hätte und ihr deshalb einige Daten verifizieren müsst. Ansonsten würde man euer Whatsapp-Konto sperren.

Zunächst sollt ihr eure Telefonnummer angeben, die ihr für das Whatsapp-Konto nutzt. Sobald ihr diese eingebt, wird sie an die Kriminellen weitergeleitet. Sie können die Telefonnummer dann nutzen, um euren Account auf einem ihrer Geräte anzumelden. Um den Account zu verknüpfen, braucht es dann nur noch einen Verifizierungscode. Den erhaltet ihr, wenn sich die Kriminellen mit einem neuen Gerät anmelden. Den Code sollt ihr dann auf der Fake-Website eingeben; angeblich um eure Daten zu bestätigen.

Solltet ihr das machen, können die Cyberkriminellen euren Whatsapp-Account übernehmen und euch aussperren. Dadurch liegen sämtliche Bilder, Videos und sensible Daten, die ihr jemals auf Whatsapp hattet, in den Händen der Hacker:innen. Auch eure Kontakte sind dadurch in Gefahr. Sie können von den Cyberkriminellen in eurem Namen angeschrieben werden und so zum Opfer weiterer Betrugsmaschen werden.

Wie ihr euch vor der Whatsapp-Masche schützt

Zunächst solltet ihr niemals auf Links klicken, die euch von unbekannten Kontakten geschickt werden. Vor allem dann, wenn sie gravierende Rechtschreibfehler enthalten und euch ein Zeitlimit setzen. Hacker:innen setzen darauf, dass ihr unter Druck handelt, um euer Konto zu retten. Stattdessen macht ihr in der Eile genau das Gegenteil.

Sollte es dennoch passieren, dass ihr eure Telefonnummer an Kriminelle weiterleitet und diese sich mit eurem Whatsapp-Account verknüpfen, könnt ihr sie wieder aussperren. Zumindest dann, wenn ihr selbst noch Zugriff habt. Öffnet die Einstellungen, tippt auf „Verknüpfte Geräte“ und entfernt das Gerät, das euch unbekannt ist.

Habt ihr keinen Zugriff mehr auf euer Whatsapp-Konto solltet ihr eure Kontakte über andere Wege – SMS, Telefon – warnen. So stellt ihr sicher, dass sie nicht auf die Betrüger:innen hereinfallen. Anschließend solltet ihr den Whatsapp-Support kontaktieren. Dieser kann euch dabei helfen, euer Whatsapp-Konto wiederzubekommen.

Tipp: Zu viele Kontakte auf WhatsApp? Dieses Feature soll für Übersicht sorgen

Quelle:https://t3n.de/news/whatsapp-masche-betrueger-kapern-euren-account-1641106/?utm_source=flipboard&utm_content=topic%2Fde-technologie

14) Problem: öffentliche (ungeschützte) WLAN-Hotspots nutzen

Immer wieder nutzt man sein Handy mit WLAN, sei es im Café, Gaststätte, Flughafen und ähnlichem, dabei vergisst man ganz schnell, in welchem WLAN man sich gerade befindet.

Warnung: WLAN am Handy unbedingt in dieser Situation ausschalten

Lesebeitrag zu u.g. Ausführungen

Tipp: https://www.pcwelt.de/article/2394778/wlan-am-handy-ausschalten-boeser-zwilling-attacke.html

Die Masche mit dem aufspannen eines WLAN-Lockhotspots im Flugzeug war mir auch bisher noch nicht bekannt. An so böse Dinge denkt man als harmloser Mensch einfach nicht!

Die Gefahr nimmt also sogar auch für erfahrene Benutzer übermäßig zu, selbst wenn man ggf. nicht darauf hereinfällt und keinerlei persönliche Daten auf Anforderung preis gibt.

Sitzt man aber eine Weile, sagen wir mal im Terminal eines Flughafens und hat eine Zahlung vergessen, kann es leicht mal dazu kommen, dass man nicht erst die eigene VPN/Wireguard-Verbindung "anschmeißt", bevor man beispielsweise dann so eine Transaktion vornimmt. Hat man dann nicht einmal aufgepasst und der Keylogger ist schon auf dem Gerät, dann ist ganz schnell auch großer Schaden entstanden.

Also erst nach einschalten des Hirns so etwas machen, oder generell nur von zuhause (sofern das möglich ist und man dann nicht bereits eine Frist hat verstreichen lassen). Nichts geht über verstärkte Aufmerksamkeit, wenn man kritische Dinge mit dem PC oder Smartphone erledigt! Davor kann man nicht genügend warnen, weil es nahezu jedem mal passieren kann.

Und wenn doch?

Meine Methode zuhause ist recht sicher, aber auch bestimmt nicht jedem Benutzer "zuzumuten".

- Transaktionen dieser Art nur vom heimatlichen Rechner aus.
- Täglich wird auf einer 2. Festplatte das gesamte Betriebssystem per Image gesichert. Bei Infektion einfach ein oder ein paar Tage zurückgehen und ein nicht infiziertes Image zurückspielen. Dauert dann nur wenige Minuten und Schadsoftware sollte dann nicht mehr vorhanden sein und man muss auch nicht suchen und nichts entfernen. Hat man das schön länger auf dem Rechner, liegen bei mir auch noch ein paar wöchentliche Sicherungen auf dem NAS bereit und wenn Trojaner, dann noch ältere Sicherungen auf nicht angeschlossenen Festplatten.
- Daten habe ich immer getrennt auf anderem Laufwerk. Die sind, außer bei Verschlüsselungstrojanern, ja nie betroffen und sind daher dann auch aktuell.

Eine Sicherungsstrategie nach Bedarf im Vorfeld zu überlegen ist also immer besser, als Gejammer, wenn man nix gemacht hat. Dann können erfahrene Bekannte auch nicht mehr wirklich effizient und schnell helfen. Dann ist das Trennen des Internets und Sperrung aller vermuteten kompromittierten Daten bei Banken etc. nur die erste Maßnahme.

Tipp: https://www.pcwelt.de/article/2394778/wlan-am-handy-ausschalten-boeser-zwilling-attacke.html

Hinweis der Redaktion: Bei diesem Beitrag handelt es sich um Ausführungen des interessierten Cybercrime-Newsletter Lesers Dirk K, bei dem ich mich hierfür bedanke.

Allgemeines:

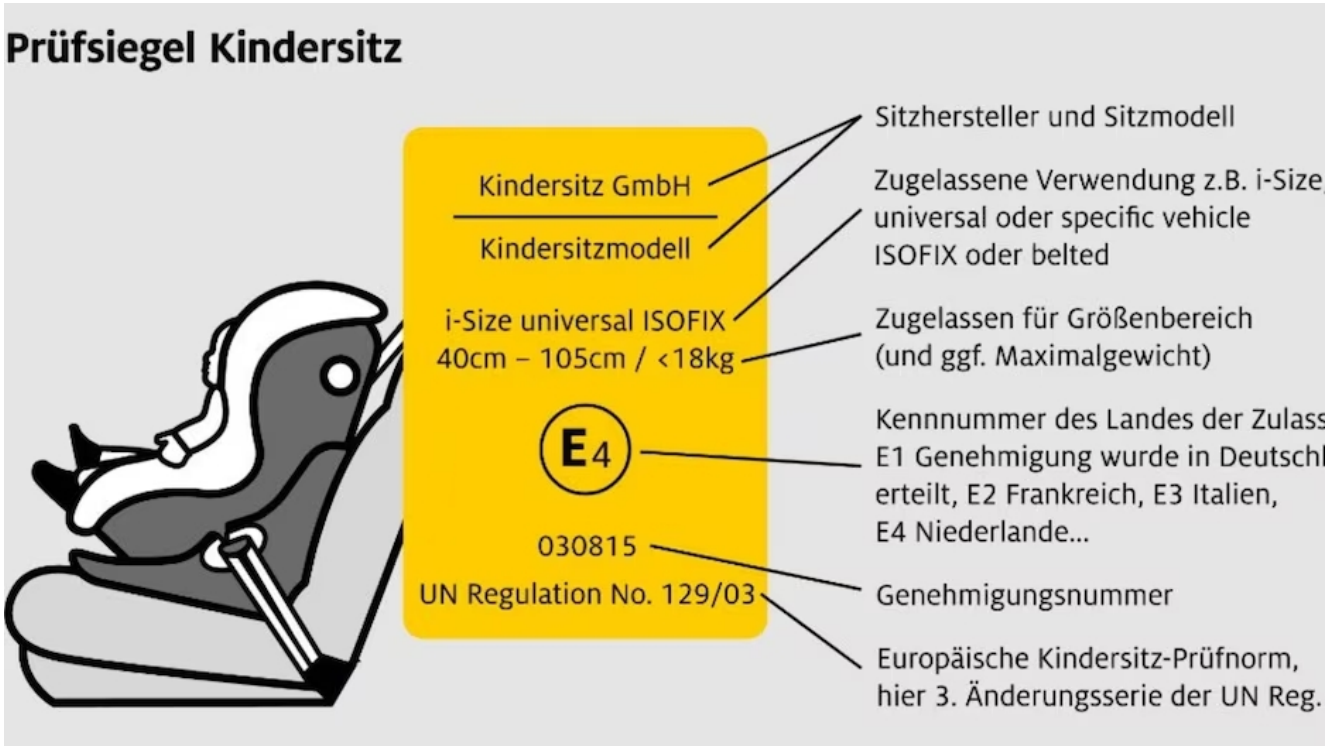
1) Verkaufsverbot für Kindersitze: Warum Sie jetzt unbedingt auf das Kürzel achten müssen

Ab September gilt das Verkaufsverbot für Kindersitze nach Norm UN ECE Reg. 44 endgültig. Was sich dadurch ändert.

Bereits in wenigen Tagen greift nach einer einjährigen Übergangsfrist das endgültige Verkaufsverbot für Kindersitze nach der veralteten Norm UN ECE Reg. 44.

Ab September sind demnach nur noch Kindersitze nach der neueren Norm UN ECE Reg. 129 (i-Size) im Handel erhältlich. Für Eltern, die bereits einen Sitz nach der alten Norm besitzen, gibt es jedoch Entwarnung: Die Nutzung der alten Sitze bleibt weiterhin erlaubt.

Auf dieses Kürzel müssen Sie künftig achten



Die Informationen sind über die Plakette zu finden. Foto: adac.de

Das Kürzel "R 44" oder "R 129 (i-size)" auf Kindersitzen steht nicht etwa für eine Typenbeschreibung, sondern für eine **von der EU festgelegte Norm**.

Finden können Sie solche Prüfplakette auf der Unter- und Rückseite des Sitzes. In manchen Fällen ist das gelbe oder orange Zeichen auch auf der Seite platziert.

Die Einführung der i-Size-Norm bringt eine Verbesserung in der Kindersicherheit mit sich. Anders als bisher, richtet sich die i-Size-Norm nicht mehr nach dem Gewicht, sondern nach der Körpergröße des Kindes, was als sicherheitsrelevanter angesehen wird.

Zudem müssen i-Size-Kindersitze einen Seitenaufpralltest bestehen, der in der alten Norm nicht vorgeschrieben war.

Ein weiterer Vorteil der i-Size-Norm ist, dass Kinder bis zum Alter von 15 Monaten in Reboardern, also entgegen der Fahrtrichtung, transportiert werden müssen. Diese Regelung

soll die Sicherheit erhöhen, da Rückwärtsfahren in diesem Alter als deutlich sicherer gilt, insbesondere bei einem Frontalaufprall.

Darf man Kindersitze mit "R 44" noch benutzen?

Wenn Sie bereits einen Kindersitz vom Norm-Typ "R44" besitzen, dürfen Sie ihn Stand jetzt noch acht Jahre lang weiter verwenden. Allerdings gilt diese Übergangsfrist nur für die zuletzt ausgegebenen Serien "44/03" und "44/04".

Die Vorgängerserien "44/01" und "44/02" dürfen schon seit längerer Zeit nicht mehr verwendet werden.

Quelle: https://www.chip.de/news/Verkaufsverbot-fuer-Kindersitze-Warum-Sie-jetzt-unbedingt-auf-das-Kuerzel-achten-muessen_184961319.html?utm_source=chip_1001309&utm_medium=email&utm_campaign=1015004&utm_content=26.08.2024

2) Unbedingt vormerken: Bunndesweit schlagen im September Millionen von Handys Alarm

Der bundesweite Warntag findet in diesem Jahr am Donnerstag, den 12. September statt. Ab 11 Uhr werden im ganzen Land Sirenen heulen und Millionen Handybesitzer aufgeschreckt werden.

Am **12. September, um 11 Uhr,** findet in diesem Jahr der bundesweite Warntag statt. Der gemeinsame Aktionstag von Bund, Ländern und Kommunen wird immer jährlich am zweiten Donnerstag im September abgehalten und dient dem Zweck, die vorhandenen Warnmittel zu testen.

Seit dem letzten Jahr wird der Probealarm auch über Cell-Broadcast-Meldungen (CB) getestet. Diese nutzen einen speziellen Betriebsmodus der bekannten SMS-Nachrichten, um nicht nur auf Smartphones zugestellt zu werden, sondern auch auf älteren Handys.

Erschrecken Sie also nicht, wenn Ihr Handy ab 11 Uhr plötzlich laute Warntöne ausspuckt. Gegen 11:45 Uhr erfolgt eine Entwarnung. Über Cell Broadcast wird derzeit noch keine Entwarnung versendet.

Aufspringende Warnung plus Alarmsirene

Wegen der Fülle an Nachrichten sind SMS heute auf Handys eher unauffällig und Nutzer haben auch verschiedene Möglichkeiten, um Kurzmitteilungen in Schach zu halten. Für eine Katastrophenwarnung ist das aber wenig geeignet, denn es sollen möglichst viele Menschen informiert werden.

Die CB-Meldungen springen deshalb als unübersehbare Nachrichten auf dem Handy-Bildschirm auf. Gleichzeitig löst der Empfang ein Warnsignal auf den Handys aus, das in voller Gerätelautstärke abgespielt wird.

Das geht unabhängig von den gewählten Lautstärkeeinstellungen los. Auch wenn Sie Ihr Handy stumm geschaltet haben, hören Sie bei Warnungen der höchsten Stufe also den Alarm.

Wichtig: Die Testwarnung wird auf höchster Gefahrenstufe verschickt, diese Nachrichten lassen sich durch Geräteeinstellungen nicht blockieren. Was möglich ist: Wenn Sie Ihr Handy in den Flugmodus stellen oder ausschalten, können die Warnmeldungen nicht zugestellt werden und Sie haben Ruhe.

Testwarnungen mit niedrigerer Stufe sind unter iOS nicht aktiviert. In den Einstellungen unter "Mitteilungen" lassen sich Testwarnungen einschalten. Sie müssen dazu ganz nach unten scrollen. Bei Android sind die Einstellungen unter "Sicherheit und Notfälle" zu finden, es gibt einen eigenen Punkte "Katastrophenwarnungen".

Systemvoraussetzungen für Cell Broadcast

Ob die Zustellung der CB-Meldungen klappt, soll im Rahmen des Warntags getestet werden. Grundsätzlich müssen Handys eingeschaltet und in einem Mobilfunknetz eingebucht sein. Ist der Akku leer oder das Handy im Flugzeugmodus bzw. ohne SIM-Karte oder eSIM unterwegs, klappt die Zustellung nicht.

Folgende Systemvoraussetzungen für Smartphones hat uns das Unternehmen Everbridge genannt, das das BBK auf technischer Ebene bei der Umsetzung von CB berät:

- **Android:** Seit Android KitKat (Version 4.4, veröffentlicht 2013) gibt es ein sogenanntes Commercial Mobile Alert System (CMAS). Jedoch müssen die Gerätehersteller das auch aktiviert haben. Seit Android 11 ist die explizite Aktivierung aber nicht mehr nötig, weil der passende Client tiefer in Android integriert ist.
- **iOS:** Ab dem iPhone 4S ist das nötige CMAS verbaut. Zusätzlich ist noch ein passendes Provider-Profil nötig. Ab iOS 15.6.1 funktionieren CB-Meldungen.

Das BBK hat eine Liste mit Handys parat, die CB unterstützen bzw. auch mit Modellen, die das nicht tun. Leider ist die Liste nicht vollständig. Für Apple wird mindestens ein iPhone 6S gefordert, aber auch Geräte von Samsung, Google und Sony werden aufgelistet.

Quelle: https://www.chip.de/news/Unbedingt-vormerken-Bundesweit-schlagen-im-September-Millionen-Handys-Alarm_184433053.html?utm_source=chip_1001310&utm_medium=email&utm_campaign=1015021&utm_content=26.08.2024

3) Neue Regel bei Überweisung: Alle Bank-Kunden sind betroffen

Wer bei seiner Bank oder Sparkasse eine Überweisung vornimmt, muss neben dem Betrag auch eine IBAN und den Empfänger angeben. So weit, so klar. Doch bald gilt ein neues Gesetz, das alle Bank-Kunden kennen sollten.

Ob für Miete oder die Handyrechnung, ob für Strom oder die Versicherung: Überweisungen und Daueraufträge gehören heute zum Alltag. Wer Geld auf ein anderes Konto überweist, muss den Zahlungsempfänger und eine IBAN angeben. Eine neue Regelung des EU-Parlaments soll ein Detail ändern, von dem alle Bank-Kunden bei einer Überweisung profitieren.

Das ändert sich demnächst bei der Überweisung

Gut 8 Milliarden Überweisungen nehmen die Deutschen pro Jahr vor. Bis das Geld auf dem Konto des anderen nach einer erfolgten Überweisung erscheint, kann es einige Tage dauern. Künftig soll es innerhalb weniger Sekunden da sein – und das sogar kostenlos. Doch nicht nur das soll sich ändern. Das EU-Parlament führt eine weitere Regelung ein, die Banken und Sparkassen beachten müssen.

So müssen den neuen Vorschriften nach Banken und Sparkassen, die sowohl eine normale als auch eine Echtzeit-Überweisung anbieten, einen Abgleich der IBAN mit dem Namen des Zahlungsempfängers vornehmen. Stimmen IBAN und Empfänger nicht überein, soll der

Kunde sofort darauf aufmerksam gemacht werden. Und das, bevor er das Geld an eine andere Person oder ein Unternehmen abschickt. Das soll denjenigen, der die Überweisung vornimmt, auf eventuelle Fehler oder einen möglichen Betrug aufmerksam machen.

Ab wann gilt die neue Regel?

Das EU-Parlament verpflichtete alle Banken und Sparkassen in allen 27 EU-Ländern sowie in Norwegen, Island und Liechtenstein zu dieser Prüfung. Alle EU-Länder werden aufgefordert, diese neue Regelung bis zum 9. Oktober 2025 umzusetzen. Das Gleiche gilt im Übrigen für die kostenlose Echtzeit-Überweisung, für die Banken derzeit noch gerne einen Euro oder mehr verlangen, oder – wie die DKB oder ING – gar nicht erst anbieten. Länder mit anderen Währungen, also etwa Norwegischen Kronen oder Schweizer Franken, haben etwas länger Zeit, um diese neue Regelung umzusetzen. Hier gilt die Frist bis zum 9. Juli 2027.

Quelle: https://www.inside-digital.de/news/neue-regel-bei-ueberweisung-alle-bank-kunden-betroffen

4) Wie man Betrug mit falschen Wohnungsanzeigen erkennt

Der Wohnungsmarkt ist angespannt. Vor allem in Ballungszentren ist es nicht einfach, eine passende bezahlbare Wohnung zu finden. Oft nutzen Betrüger das aus. Wie erkennt man fingierte Anzeigen?

Mit falschen Wohnungsinseraten auf Internet-Portalen erbeuten vermeintliche Vermieter von den Wohnungssuchenden Geldbeträge oder entlocken ihnen persönliche Daten. Die Masche funktioniert - denn viele, die verzweifelt eine Wohnung suchen, leisten bereitwillig Vorauszahlungen oder geben vertrauliche Daten preis. Das kann teure Folgen haben.

So funktioniert der Betrug mit falschen Inseraten

Mit den Daten des fremden Personalausweises sowie anderen persönlichen Daten können Betrüger Konten eröffnen, kostenpflichtige Abos und Verträge abschließen oder Online-Shopping betreiben. Dabei nutzen die Täter beispielsweise die Adressdaten der Wohnungssuchenden, erfinden eine Kontonummer und schließen Ratenverträge ab, etwa für teure Elektrogeräte. Die Ware wird dann an den Betrüger geliefert, wobei dieser seine Adresse mehrfach ändern oder die Sendungen weiterleiten lassen kann. Um Namen und Anschrift des Betrügers herauszufinden, müssen die Informationen von Opfer, Banken und Verkäufer zusammengebracht werden. Diese Puzzlearbeit kann laut Polizei dauern.

Der Betrüger verkauft die erhaltene Ware weiter und streicht somit Gewinn ein. Das Betrugsopfer weiß zunächst nichts von den laufenden Ratenkrediten, die wegen der erfundenen Kontonummer nicht bezahlt werden. Das kann zu einem Schufa-Eintrag und zur Streichung des Dispokredits führen.

Der Hamburger Polizei ist sogar ein Fall bekannt, in dem Daten des Arbeitsgebers von einem Betrüger genutzt wurden, um das Gehalt einer Wohnungssuchenden auf ein anderes Konto umzuleiten.

Opfer muss Betrug nachweisen

Wenn ein Wohnungssuchender auf eine betrügerische Anzeige hereingefallen ist und seine Daten zum Beispiel für den Abschluss von Krediten missbraucht wurden, ist das Betrugsopfer in der Beweispflicht: Es muss nachweisen, dass die Waren von jemand anderem bestellt wurden.

Vorsicht bei Vorabzahlungen

Schon seit Längerem wird Betrug mit Vorabzahlungen begangen: Für die Besichtigung einer Wohnung wird ein bestimmter Betrag verlangt. Er soll im Vorfeld überwiesen werden. Doch die inserierte Wohnung existiert in diesen Fällen gar nicht, den Betrügern geht es nur um die Zahlungen. Polizei und Makler weisen darauf hin, dass die Aufforderung zu einer Zahlung vor der Besichtigung unüblich ist. Hier handelt es sich um einen sehr deutlichen Hinweis auf ein falsches Inserat.

Die Polizei registriert außerdem immer wieder Fälle von sogenanntem "Schlüsseltresor-Betrug". Dabei geben die vermeintlichen Vermieter vor, sich derzeit im Ausland aufzuhalten. Für eine alleinige Wohnungsbesichtigung sollen die Mietinteressenten eine Kaution für den Wohnungstürschlüssel zahlen, der angeblich in einem Tresor auf dem Grundstück deponiert wurde.

Falsche Wohnungsanzeigen erkennen

Wohnungssuchende sollten misstrauisch werden, wenn der Preis einer Wohnung sehr viel niedriger liegt als der Preis vergleichbarer Wohnungen in derselben Gegend. Auch viel zu geringe Nebenkosten sind ein Hinweis auf eine Anzeige, die in betrügerischer Absicht geschaltet wurde.

Die Fotos der inserierten Wohnung sollten sich Wohnungssuchende ebenfalls sehr genau ansehen:

- Stimmen die Bilder mit der Beschreibung überein? (Etage, Blick nach draußen, Außenansicht)
- Könnte es sich bei den Fotos auch um Aufnahmen aus einem Hotelzimmer handeln?
- Sind in möblierten Wohnungen extrem teure Designermöbel zu sehen, die nicht zu der geringen Monatsmiete passen?
- Werden dieselben Fotos auch für Wohnungen an anderen Orten benutzt?
- Haben die Täter die Fotos von anderen Online-Portalen für Ferienwohnungen oder Mietwohnungen geklaut? Dies lässt sich meist ganz einfach über die Google-Bildersuche herausfinden.

Keine sensiblen Daten vorab übermitteln

Seriöse Vermieter und Wohnungsvermittler erwarten keine Übergabe sensibler Daten im Vorfeld. Erst nachdem sie den Wohninteressenten bei einem Besichtigungstermin persönlich kennengelernt haben, erfolgt die Übergabe der persönlichen Daten wie Einkommensnachweis und Schufa-Auskunft.

Identität der Immobilienfirma oder des Vermieters überprüfen

Wer sichergehen will, dass die Wohnungsanzeige echt ist, kann außerdem folgende Punkte überprüfen:

- Ist die Immobilienfirma im Handelsregister eingetragen?
- Gibt es auf der Webseite ein Impressum?
- Findet man online Rezensionen zur Firma?
- Ist die Postadresse echt? (Insbesondere Betrüger aus dem Ausland nutzen häufig Adressen in bester Innenstadtlage, an denen sich beispielsweise ein Einkaufszentrum oder Sehenswürdigkeiten befinden)
- Sind die Mitarbeiterinnen und Mitarbeiter der Immobilienfirma persönlich per Telefon erreichbar?
- Ist die in der Anzeige angegebene Mietwohnung tatsächlich frei? Dies lässt sich häufig

vor Ort bei Nachbarn oder dem Hausmeister erfragen.

Verdächtige Wohnungsanzeigen melden

Viele Internet-Portale mit Wohnungsinseraten haben einen Melde-Button: Wer eine verdächtige Anzeige entdeckt, kann das per Klick melden. Die Anzeigen werden dann überprüft. Bestätigt sich der Verdacht, werden sie offline gestellt.

Tipp: Unter dem u.g. Link kann der passende Fernsehbeitrag angeschaut werden

Quelle: https://www.ndr.de/ratgeber/verbraucher/Wie-man-Betrug-mit-falschen-Wohnungsanzeigen-erkennt,wohnungssuche164.html

5) Rückrufaktion in Baden-Württemberg: Verzehr von Süßigkeit kann tödlich enden

Eine Süßware wird vom Hersteller zurückgerufen, da die Gefahr besteht, durch den Verzehr zu ersticken. Alle Infos hier im Überblick.

Es gibt eine aktuelle Warnung vor dem Kauf von „Jelly Straws“. Das hat die Verbraucherzentrale von Bund und Ländern lebensmittelwarnung.de am 22.08.2024 bekannt gegeben:

Produktrückruf: Welche Bundesländer sind betroffen?

Laut lebensmittelwarnung.de sind folgende Bundesländer von der aktuellen Warnung betroffen:

- Baden-Württemberg
- Bayern
- Berlin
- Bremen
- Hamburg
- Hessen
- Nordrhein-Westfalen
- Niedersachen
- Sachsen
- Saarland
- Rheinland-Pfalz

Welche möglichen Folgen gibt es?

Die Art der Aufnahme des Produktes stellt aufgrund der Konsistenz, der Form und der physikalischen und chemischen Eigenschaften ein Erstickungsrisiko dar. Die Gelee-Konsistenz erhöht, besonders für Kinder, die Gefahr zu ersticken.

Warnung vor Süßware – Welches Produkt ist betroffen?

Achtung vor dem Verzehr von „**Jelly Straws Assorted Flavour, Taiwan Gourmet“**des Herstellers **„Go Asia Deutschland GmbH“.** Die Lebensmittelwarnung warnt eindringlich vor dem Verzehr, da es zu einer erhöhten Erstickungsgefahr, oder zum Verschlucken kommen kann**.**
„Jelly Straws“ werden in einer 1500-Gramm-Packung verkauft.

Die Süßware 'Jelly Straws' des Unternehmens 'Go Asia Deutschland GmbH' wird zurückgerufen
Foto: lebensmittelwarnung.de

Was können KundInnen jetzt tun?

VerbraucherInnen, **die das bezeichnete Produkt gekauft haben, können dieses gegen Erstattung des Kaufpreises in einer Verkaufsstelle von „go asia“ zurückgeben.**

Tipp: Mehr Hintergrundinformationen zu Lebensmittelwarnungen gibt es in diesem Artikel

Quelle:https://www.swp.de/panorama/rueckrufaktion-in-baden-wuerttemberg-verzehr-von-suessigkeit-kann-toedlich-enden-77473469.html

6) Verträge sicher kündigen: So geht’s bei DSL, Telefon, Streaming & Co.

Das Gesetz für faire Verbraucherverträge verbietet automatische Jahresverlängerungen. Doch ein Fünftel der Anbieter bietet keinen Kündigungs-Button an, sodass Kündigungen per Brief oder Mail erfolgen müssen.

Seit dem Frühjahr 2022 ist das sogenannte Gesetz für faire Verbraucherverträge in Kraft. Damit ist die zuvor übliche automatische Verlängerung um jeweils ein ganzes Jahr nicht mehr erlaubt:

Nach Ablauf der anfänglichen Mindestvertragszeit von höchstens 24 Monaten können Kunden ihren Vertrag monatlich kündigen.

Darüber hinaus müssen sich Verträge, die über das Internet abgeschlossen wurden, auch online über einen Button zum Anklicken wieder kündigen lassen.

Allerdings bietet ein Fünftel der Anbieter auch rund zwei Jahre nach Einführung der Verpflichtung keinen Kündigungs-Button an. Da bleibt nur die klassische Kündigung per Brief

(am besten per Einschreiben) oder Mail.

Das Gesetz gilt für zahlreiche auf Dauer angelegte Kontrakte, nicht aber für Versicherungen. Bei Lieferverträgen für Energie (Gas oder Strom) müssen sämtliche telefonisch vorgenommene Abschlüsse zusätzlich schriftlich per Post, E-Mail oder SMS bestätigt werden.

Neben diesen Besonderheiten gibt es einige weitere Fallstricke zu beachten. So gilt die Neuregelung zunächst nur für die Verträge, die nach dem Stichtag 1. März 2022 abgeschlossen wurden.

Bei älteren Bestandsverträgen gilt weiterhin die alte Regelung, also die automatische Verlängerung bis zu einem Jahr. Ausgenommen davon sind jedoch Telekommunikationsverträge, sie fallen unter ein anderes Gesetz.

Hier gilt die neue einmonatige Kündigungsmöglichkeit nach dem Ablauf der Mindestlaufzeit ausdrücklich auch für Altverträge!

Außerdem müssen auch am Telefon geschlossene Mobilfunk-, Festnetz- und Internetverträge nachträglich schriftlich klar und leicht verständlich zusammengefasst werden.

Und wie steht es mit der Zulässigkeit von Preiserhöhungen, wie sie beispielsweise 1&1 oder Vodafone in den vergangenen Monaten vorgenommen haben?

Verbraucherschützer halten solche Klauseln in den AGBs ohne ein Sonderkündigungsrecht der Kunden für unzulässig. Der Bundesverband Verbraucherzentrale hat Ende letzten Jahres beim Oberlandesgericht Hamm eine Sammelklage gegen Vodafone eingereicht, die Gerichtsentscheidung steht noch aus.

Lesetipp: Geld zurück: Verträge am Smartphone sofort kündigen

Quelle: https://www.pcwelt.de/article/2417503/vertrage-sicher-kundigen-so-gehts-bei-dsl-telefon-streaming-co.html?utm_date=20240827122405&utm_campaign=Best-of%20PC-WELT&utm_content=Title%20Story%3A%20Vertr%C3%A4ge%20sicher%20k%C3%BCndigen%3A%20So%20geht%27s%20bei%20DSL%2C%20Telefon%2C%20Streaming%20%26%20Co.&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4