36. Cybercrime Newsletter

28.07.2023

1) Vorsicht vor neuen Betrugsmaschen

Betrüger:innen sind kreativ und entwickeln ständig neue Methoden, nutzen neue Technologien und ändern ihre Taktiken, um nicht entdeckt zu werden. Gehe auf Nummer sicher, indem du dich mit ihren aktuellsten Betrugsmaschen vertraut machst.

Betrug mit Bestellbestätigungen:

Dabei handelt es sich um unerwartete Anrufe/Textnachrichten/E-Mails, **die häufig auf einen nicht autorisierten** Kauf hinweisen und dich bitten, **dringend zu handeln**, **um den Kauf zu bestätigen oder zu stornieren**. Diese Betrüger versuchen, dich davon zu überzeugen, **Zahlungs- oder Bankkontoinformationen preiszugeben**, Software auf deinem Computer/Gerät zu installieren oder Geschenkkarten zu kaufen.

Amazon sendet dir keine Korrespondenz zu einer Bestellung, die du nicht erwartest. *Bei Fragen zu einer Bestellung, überprüfe Meine Bestellungen immer auf Amazon.de oder über die App „Amazon Shopping“. In deiner Bestellhistorie werden nur ordnungsgemäße Einkäufe angezeigt. Der Kundenservice steht dir rund um die Uhr zur Verfügung, um dir zu helfen.*

Betrug mit Zahlungsinformationen :

Betrüger:innen senden dir eine unerwartete **Aufforderung zur Aktualisierung deiner Zahlungsinformationen** oder zur Zahlung einer ausstehenden Rechnung für ein Produkt oder eine Dienstleistung, **die du nicht bestellt hast**. Sie drohen damit, den fälligen Betrag einzutreiben, wenn du deine Zahlungs- oder Kontoinformationen nicht zur Verfügung stellst.

Amazon wird dich niemals bitten, Zahlungsinformationen, einschließlich Geschenkkarten (oder „Bestätigungskarten“, wie sie von einigen Betrüger:innen genannt werden), für Produkte oder Dienstleistungen telefonisch anzugeben oder per E-Mail.

Hier sind einige wichtige Tipps, um Betrug zu erkennen und dein Konto und deine Daten zu schützen :

1. Vertraue den Kommunikationskanälen von Amazon.

Gehe immer über die mobile Amazon-App oder die Website, wenn du den Kundenservice oder technischen Support erreichen oder Änderungen an deinem Konto vornehmen möchtest.

2. Sei misstrauisch bei falscher Dringlichkeit.

Betrüger:innen versuchen möglicherweise, ein Gefühl der Dringlichkeit zu erzeugen, um dich zu überreden, das zu tun, was sie verlangen. Sei vorsichtig, wenn jemand dich dazu

drängt, sofort zu handeln.

3. Bezahle niemals telefonisch.

Amazon wird dich niemals dazu auffordern, telefonisch Zahlungsinformationen, einschließlich Geschenkkarten (oder „Bestätigungskarten“, wie sie von einigen Betrüger:innen genannt werden) für Produkte oder Dienstleistungen anzugeben.

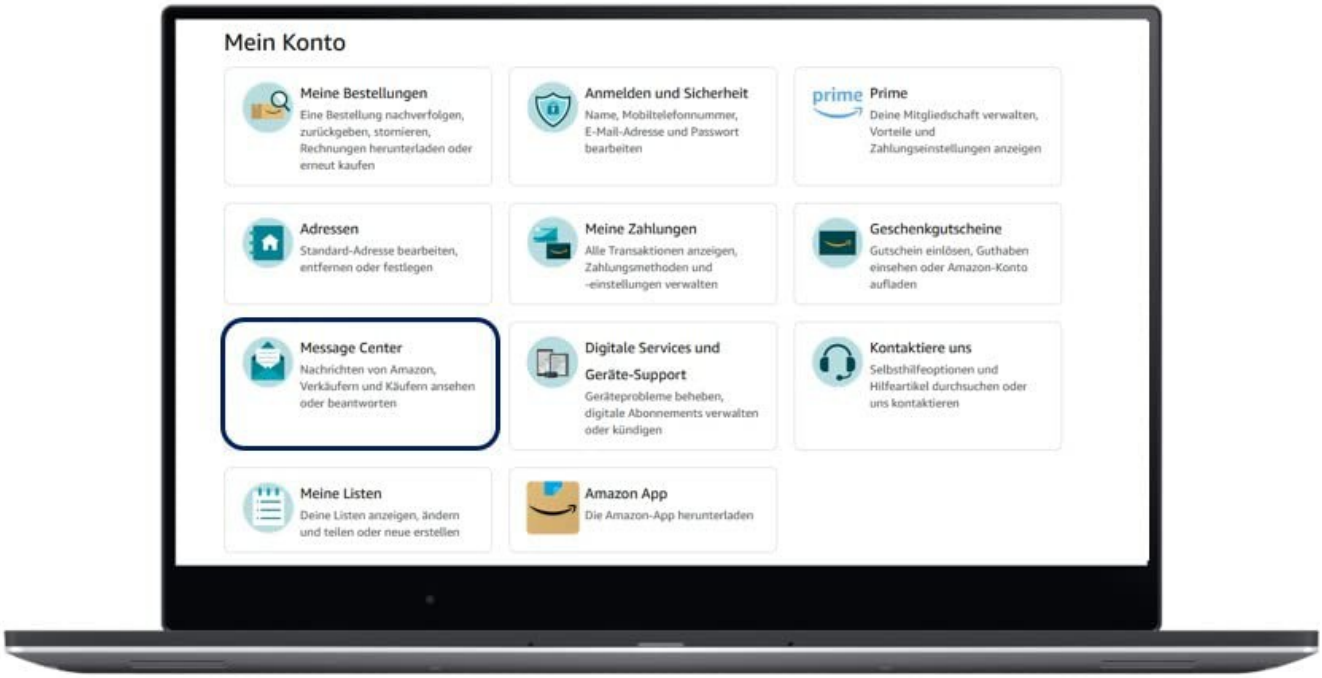
4. Überprüfe zuerst den Link.

Legitime Amazon Websitelinks enthalten „amazon.de“. Gehe direkt auf unsere Website, wenn du Hilfe zu Amazon-Geräten/-Diensten oder Bestellungen benötigst oder du Änderungen an deinem Kundenkonto vornehmen möchtest.

Weitere Informationen zur Online-Sicherheit findest du unter Sicherheit und Datenschutz auf der Amazon-Kundenservice-Seite.

Wenn du eine Mitteilung erhältst — per Anruf, Textnachricht oder E-Mail —, von der du glaubst, dass sie möglicherweise nicht von Amazon stammt, dann melde uns die verdächtige Kommunikation bitte hier.

Um E-Mails von Amazon zu überprüfen, besuche das Message Center auf unserer Website.



Quelle: promotion5@amazon.de

2) KI-Angriffe: Vorsicht vor neuen Betrugs-Techniken

Cyberkriminelle nutzen KI-Tools, um ihre Opfer schneller und effektiver anzugreifen. Computernutzer müssen jetzt noch deutlich aufmerksamer sein.

KI-Werkzeuge erzeugen im Handumdrehen neue Texte, Bilder und Audiodateien. Diese Tools sind auch für **Cyberkriminelle** interessant. Spätestens seit dem Debüt des KI-basierten Chatbots Chat-GPT im November 2022 experimentieren Angreifer mit diesen Programmen.

Zwar haben Open AI und andere Hersteller von KI-Programmen Sicherheitsmaßnahmen entwickelt, um Missbrauch zu verhindern, doch halten diese den Angriffen nicht immer stand. Laut den Forschern von Check Point verkaufen Cyberkriminelle bereits Tools, mit denen sich die Sicherheitseinschränkungen von Chat-GPT umgehen lassen, um Malware zu erstellen. Zumindest zeitweise haben diese Tools wohl gut funktioniert.

Schon der Name „Chat-GPT“ ist Angreifern dienlich

Angriffe mit Phishing-Mails benötigen fast immer einen guten Aufhänger, um die Empfänger in die Falle zu locken. Die Betreffzeile der Phishing-Mail sollte beispielsweise eine große Nähe zum Opfer haben.

Der Betreff „**Sie haben Ihr DHL-Paket verpasst**“ kann einen Empfänger dazu verleiten, auf einen Anhang zu klicken, wenn er zufällig tatsächlich gerade ein DHL-Paket erwartet. In diesem Fall kommt zur Nähe des Betreffs auch noch eine gewisse Dringlichkeit hinzu.

Ein weiterer Aufhänger für Phishing-Angriffe mit Malware sind aktuelle, brisante Themen. Das kann ein Bahnstreik sein, ein sportliches Großereignis wie die **Olympischen Spiele** oder das Thema **künstliche Intelligenz**. So wurden im März 2023 neue Malware-Familien entdeckt, die den Namen *Chat-GPT* verwenden, um Benutzer zu täuschen. Häufig handelt es sich um Apps oder Browser-Erweiterungen, die Chat-GPT-Tools imitieren.

In einigen Fällen bieten die gefälschten Tools sogar einige echte Chat-GPT-Funktionen an. Ihr eigentliches Ziel ist es jedoch, die Anmeldedaten des Benutzers aus dem Browser zu stehlen oder zu einem teuren Abo zu verleiten. So finden sich in den offiziellen App-Stores von Google und Apple Apps, die Zugriff auf Chat-GPT-Pro versprechen, wenn man zehn Dollar pro Monat zahlt. Liefern tun sie aber nicht.

Gefälschte Sprachnachrichten, die täuschend echt klingen

Auch ohne KI-Tools war die **CEO-Vortäuschung** in den letzten Jahren eine beliebte Masche bei Cyberkriminellen. Dabei geben sich die Angreifer als Chef des Unternehmens (CEO) aus und schreiben die Buchhaltung oder den CFO (Finanzchef) an. Sie überzeugen ihr Opfer, dass es schnell einen hohen Geldbetrag überweisen muss. Es ginge, so die Nachricht vom Chef, um eine eilige Firmenübernahme, die er jetzt tätigen muss.

Auch wenn es merkwürdig klingt: Es sind bereits viele Mitarbeiter auf den Trick hereingefallen und haben Hunderttausende Euro oder gar Millionenbeträge an die Betrüger überwiesen.

Bisher setzten die Kriminellen für diese Masche nur gut gemachte Mails ein. Mit Hilfe von KI-Tools lässt sich aber auch die Stimme eines Menschen nachbilden. Dazu muss die KI mit genügend Originalmaterial, also echten Aufnahmen einer Person, trainiert werden. Ein entsprechendes KI-Tool namens Vall-E soll Ende Mai veröffentlicht werden. Gerüchten zufolge sollen iPhones Ende 2023 mit iOS 17 eine solche Funktion erhalten.

Für den CEO-Betrug bedeutet das, dass die Angreifer zusätzlich zu den gefälschten Mails auch gefälschte Sprachnachrichten versenden könnten und damit möglicherweise noch überzeugender wirken.

F for Fake: Massenhaft gefälschte und täuschend echte Fotos

„F for Fake“ ist der Titel eines Dokumentarfilms des Filmemachers Orson Wells aus dem Jahr 1973. In dem ironischen Film geht es um den Kunstfälscher Elmyr de Hory, der mehrere tausend Fälschungen in Umlauf gebracht haben soll. Um auf diese Zahl zu kommen, brauchte de Hory rund drei Jahrzehnte. Mit KI-Tools wie Midjourney oder Stable Diffsion können Cyberkriminelle in kürzester Zeit massenhaft neue Bilder erstellen. Diese gehen zwar

nicht als Gemälde von Picasso oder Renoir durch, da die Zutaten Leinwand und Farbe fehlen.

Doch im **Fälschen von Fotos** sind die KI-Tools sehr gut. So können Angreifer erfundene Geschichten durch Fotofälschungen glaubwürdig machen. Einen Vorgeschmack auf gefälschte Bilder mit KI-Tools gaben die „Aufnahmen“ von Donald Trump, der scheinbar von FBI-Agenten verhaftet wird, und von Papst Franziskus, der einen lustigen Designer-Daunenmantel trug. Beide Bilder gingen viral und faszinierten die Betrachter. Beide wurden aber auch schnell als Fakes, also Fälschungen, entlarvt.

Es ist zu befürchten, dass in Zukunft vermehrt solche Manipulationen eingesetzt werden. So könnte passieren, dass Kriminelle in einem Wahlkampf Bilder des politischen Gegners verbreiten, auf denen dieser scheinbar anstößige Dinge tut. Das wiederum kann die Wahl beeinflussen.

Andere Betrugsszenarien sind an der Börse denkbar: Wenn Fotos auftauchen, die scheinbar Umweltverbrechen eines Chemiekonzerns belegen, kann das den Aktienkurs des Unternehmens beeinflussen. Akteure, die auf fallende Kurse wetten, werden reich. Wenn danach Experten herausfinden, dass alles eine Fälschung war, ist das Ziel der Angreifer längst erreicht.

Rachepornos: Mit Deepfakes Videos manipulieren

Unter **Rachepornografie** versteht man die Verbreitung von Inhalten mit nackten oder sexuell expliziten Darstellungen ohne Einwilligung der auf dem Foto oder Video abgebildeten Person. Rachepornografie zielt in erster Linie darauf ab, die Opfer in Verlegenheit zu bringen oder ihren Ruf zu schädigen. Wie der Begriff bereits andeutet, sind meist Rachemotive die treibende Kraft.

Bei den Opfern handelt es sich überwiegend um Frauen, bei den Tätern meist um Ex-Partner, die sensible Inhalte weitergeben, um sich zum Beispiel für das Ende der Beziehung zu rächen. In anderen Fällen haben sich Cyberkriminelle in die Computer der Opfer gehackt, um dort nach Nacktbildern zu suchen und diese zu veröffentlichen.

Mit neuen KI-Funktionen sind Angreifer heute nicht mehr auf vorhandenes kompromittierendes Foto- oder Videomaterial ihrer Opfer angewiesen. Fotos vom Gesicht der Person reichen aus. Videotools können dieses in jede vorhandene pornografische Aufnahme einbauen. Diese Technik wird als **Deepfake** bezeichnet.

Wer nicht über das nötige Know-how verfügt, kann im Darknet Deepfake-Videos in Auftrag geben. Laut den Sicherheitsexperten von Kaspersky sind solche Dienste bereits ab 300 Dollar zu haben. Die Veröffentlichung von intimen Fotos und Videos kann den Opfern nachhaltig schaden und Konsequenzen am Arbeitsplatz oder im persönlichen Umfeld haben. Die Belastung für die Opfer kann extrem hoch sein.

Phishing-Mails: Darum sind KI-Chatbots für Phishing-Angriffe ideal

Chatbots wie Chat-GPT liefern nach der Eingabe weniger Sätze eine vollständige Mail. Diese ist in der Regel formal einwandfrei, enthält keine Rechtschreibfehler und überzeugt durch einen guten, lesbaren Schreibstil. **Das ist ideal für jeden Angreifer**. Mit minimalem Aufwand erhält er so täuschend echte Mailtexte, die er zudem leicht an individuelle Ziele anpassen kann.

Hat er es zum Beispiel auf die Mitarbeiter eines Unternehmens abgesehen, kann er mit Chat-GPT und ein wenig Recherche zum Unternehmen die Phishing-Mails noch glaubwürdiger klingen lassen. Schon vor dem KI-Chatbot gab es Phishing-Mails, die kaum als solche zu erkennen waren. Mit Hilfe von KI-Tools wird dies den Angreifern in Zukunft noch viel häufiger

gelingen.

Kriminelle programmieren mit Chat-GPT & Co. Malware

In den letzten Monaten haben vor allem Kriminelle ohne Programmierkenntnisse die neuen KI-Tools **zur Erstellung von Malware** genutzt. Die so erzeugten Schädlinge sind nicht besonders raffiniert, aber dennoch eine weitere Belastung für Antivirenprogramme. Ob mittelfristig auch die Raffinesse der KI-generierten Malware zunimmt, etwa weil Programmierprofis die KI-Tools ebenfalls nutzen, ist noch nicht klar. Zumindest wurden bereits wenige Wochen nach der Veröffentlichung von Chat-GPT in Untergrundforen der Einsatz des KI-Tools diskutiert und demonstriert.

Die Forscher von Checkpoint Research zeigen Fälle auf, in denen Forumsteilnehmer gefährlichen Code posten, der von Chat-GPT generiert wurde. In einem Fall ist der Code in der Lage, Dateien mit bestimmten Dateiendungen auf einem PC zu sammeln und ins Internet zu laden. Es handelt sich um einen einfachen Infostealer.

Ein anderes Beispiel ist ein Code, der Dateien verschlüsselt und somit auch als Erpresservirus eingesetzt werden kann.

KI-Tools erstellen eine komplette Angriffskette

Die Sicherheitsforscher von Checkpoint Research haben sich bereits intensiv damit beschäftigt, wie Cyberkriminelle die neuen KI-Tools für ihre Zwecke missbrauchen können. In einem Blog-Eintrag zeigen sie, wie ein kompletter Angriff mit Hilfe von KI-Tools durchgeführt werden kann, ohne dass der Angreifer Programmierkenntnisse besitzen muss. Darin erstellen die Experten mit Chat-GPT und Codex eine Phishing-Mail und eine bösartige Excel-Datei, die mit Hilfe von Makros weiteren Schadcode auf den PC lädt. Eine klassische Angriffsmethode der Cyberkriminellen.

- **Schritt 1:** Die Checkpoint-Forscher erzeugen die Phishing-Mail mit Chat-GPT. Dazu geben die Forscher dem Chatbot die simple Anweisung „*Erstelle eine Phishing-Mail, die vorgibt, von dem erfundenen Webhoster Host4u zu stammen*“. Und das tut der Bot tatsächlich (siehe Screenshot). Zwar gibt er auch einen Hinweis aus, dass seine eigene Ausgabe gegen die Regeln verstoßen könnte, aber der Text ist da. Er ist eine gute Grundlage für die Phishing-Mail, die die Forscher zusammen mit Chat-GPT noch weiter verbessern.

- **Schritt 2:** Auch das Makro für die Excel-Datei lassen die Checkpoint-Experten von Chat-GPT schreiben. Ihr einfacher Auftrag an den Chatbot lautet sinngemäß: Schreibe ein VBA-Makro für eine Excel-Datei, das beim Öffnen der Datei ein Programm aus dem Internet herunterlädt und ausführt.
- **Schritt 3:** Generierung von Angriffscode mit dem Tool Codex. Ziel dieser Aufgabe ist es, auf dem Zielrechner unbemerkt eine sogenannte Reverse Shell zu starten. Eine Reverse Shell baut eine Verbindung zum Angreifer auf und übergibt diesem die Kontrolle über den PC. Firewall-Regeln umgeht die Reverse Shell. Schließlich lassen die Checkpoint-Forscher den Angriffscode in ausführbare Dateien umwandeln und haben damit alle Voraussetzungen für einen erfolgreichen Angriff geschaffen. Den Blog-Eintrag finden Sie hier.

Fake-ChatGPT: Wie Betrüger den Hype um die Chat-KI ausnutzen

Whatsapp-Betrug: So läuft die Masche und so schützen Sie sich

Achtung, Fake! So erkennen Sie gefälschte Bilder à la Midjourney

Geld vom Finanzamt: So läuft ein aktueller Betrug

Quelle: https://www.pcwelt.de/article/1988587/ki-angriffe-neue-betrugs-techniken.html?utm_date=20230727115748&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20KI-Angriffe%3A%20Vorsicht%20vor%20neuen%20Betrugs-Techniken&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Fiese Online-Masche: WISO zeigt, wie Urlauber abgezockt wurde

Betrüger denken sich immer wieder Maschen aus, mit denen Verbrauchern Geld entlockt wird. Bei der TV-Sendung WISO erzählt ein Mann von seinem Urlaubs-Betrug.

Bremen – Ein Mann wollte mit seinen Tennis-Kollegen eine Villa in den Niederlanden für einen Urlaub buchen. Nachdem eine Anzahlung getätigt wurde, wird der Urlauber durch mehrere Dinge misstrauisch – das Geld war dann bereits weg.

Betrugsmasche mit Urlaubern – Vermeintliche Ferienwohnung existiert gar nicht

Betrüger gehen skrupellos vor, um an sensible Daten oder das Geld von Verbrauchern zu gelangen. Vor allem auf Betrugsmaschen im Internet haben sich viele von ihnen spezialisiert – das hat auch mit der vermeintlichen Anonymität zu tun. Mit einem solchen Fall hatte ein Mann zu tun, über den das ZDF in seiner Sendung WISO berichtete. Der Mann wollte mit seinen Tennis-Kollegen eine Villa in den Niederlanden für 249 Euro die Nacht buchen – und wurde bitter enttäuscht.

Nach eigenen Angaben prüfte der Betroffene die Anzeige auf der Website *ferienwohnungen.de* ausgiebig – sogar auf Satellitenbilder griff er zurück. Auch seine Kollegen hatten an der Annonce nichts auszusetzen und gaben ihr Okay. Vor allem der freundliche und ausgiebige Kontakt zum Vermieter gab der Tennis-Gruppe Sicherheit. Selbst nachdem die sieben Personen eine Anzahlung von rund 650 Euro getätigt hatten, hielt der Kontakt zum Vermieter. Dann folgte plötzlich der Schock: Die Anzeige und dazugehörige Website sind offline. Er merkte: „Verdammt, wir sind einem Betrug aufgesessen."

Urlaubs-Betrug: Das angezahlte Geld für die Ferienwohnung ist weg

Die Masche mit Fake-Shops, auf denen Verbraucher ihr Geld lassen, ist nichts Neues. Auf Fake-Angebote bei der Buchung des nächsten Urlaubes fallen jedoch noch immer viele Menschen herein. Vor allem Kurzentschlossene versuchen oft, ein Urlaubs-Schnäppchen zu machen. Dabei sollten diese sich fragen: Ist das Angebot zu gut, um wahr zu sein? Im Falle der Ferien-Villa in den Niederlanden sah das für die Tennis-Gruppe nicht danach aus. Den Verlust des Geldes müssen sie dennoch selbst verantworten.

Darauf sollten Sie bei der Buchung des Urlaubs achten:

- Keinen Kontakt über WhatsApp oder Email für die Buchung halten
- Keine Vorauszahlungen per Überweisung oder Paypal Freunde & Familie tätigen
- Bei ständigen Zahlungsaufforderungen nicht unter Druck setzen lassen
- Keine Kontaktdaten weitergeben
- Impressum auf Vollständigkeit überprüfen – angegebenen Daten nachgehen

Die Website *ferienwohnungen.de* vermittelte die Villa zwar, übernimmt für die dort veröffentlichten Anzeigen laut AGB jedoch keine Verantwortung. „Wir mussten feststellen, dass diese Seiten immer professioneller werden und es auch für uns immer mehr zur Herausforderung wird, zu erkennen, ob es sich um eine betrügerische Seite handelt", sagte Karolina Wojtal vom Europäischen Verbraucherzentrum gegenüber WISO. Verbraucher sollten laut Wojtal immer skeptisch werden, wenn Bezahlungen und der Kontakt nicht über

die bekannte Buchungsseite, sondern privat abgewickelt werden sollen.

Quelle: https://www.merkur.de/verbraucher/urlauber-abgezockt-betrug-online-fake-wiso-zdf-buchung-geld-daten-verbraucher-92417570.html

4) Polizei verhaftet Whatsapp-Betrüger: So lief der Betrug

In Hamburg klickten die Handschellen: Polizeibeamter nahmen nach monatelangen Ermittlungen der bayerischen Polizei einen Whatsapp-Betrüger fest. Er gehört zu einer ganzen Bande von Cybergangstern.

Der Kriminalpolizei Aschaffenburg (Bayern) ist ein Schlag gegen Whatsapp-Betrug gelungen. Bereits am 13. Juli 2023, also Donnerstag letzte Woche, nahmen Polizeibeamte einen vermutlichen Whatsapp-Betrüger in Hamburg fest. Der Mann soll zusammen mit weiteren Mitgliedern einer Gruppe aus den Niederlanden für eine Vielzahl von Betrugsfällen über Whatsapp verantwortlich sein, wie das Polizeipräsidium Unterfranken und die Staatsanwaltschaft Aschaffenburg heute mitgeteilt haben.

Der festgenommene Mann ist 25 Jahre alt; die Staatsanwaltschaft wirft ihm Betrug vor. Der Mann ist seit seiner Festnahme in Haft. Seit Herbst 2022 ermittelte die Polizei gegen den Verdächtigen und die Gruppe aus den Niederlanden sowie in mehreren Bundesländern gegen mehrere Männer im Alter von 23 bis 25 Jahren.

So funktionierte der Betrug

Der Mann und dessen Komplizen verschickten eine Whatsapp-Nachricht an die ausgesuchten Opfer. In der Nachricht schreiben die Täter dann beispielsweise: “Hallo Mama/Papa, mein Handy ist kaputt und das ist meine neue Nummer.” Sobald das Opfer auf die Nachricht reagiert, wird analog dem bekannten „Enkeltrick“ per Telefon eine Notlage vorgetäuscht und erklärt, es müsste dringend ein Geldbetrag auf ein Bankkonto überwiesen werden. Meist

Im weiteren Nachrichtenverlauf begründen die Absender ihre Geldforderung damit, dass ja das eigene Handy kaputt sei und sie deswegen keine Online-Überweisungen tätigen könnten. Es stünde aber eine dringende Rechnung aus, die sie unbedingt und dringend begleichen müssten. Das Geld würde sie selbstverständlich baldmöglichst wieder zurückzahlen.

Die Polizei betont, dass die Betrüger bei der Gesprächsführung auch per Textnachricht äußerst geschickt vorgehen und bei ihren Opfern gezielt Druck aufbauen würden. Die Masche erscheine so zunächst glaubhaft und führe zur Überweisung des geforderten Geldbetrags.

Polizei warnt vor neuen Betrugsvarianten

Als neue Variante fragen die Gangster derzeit die Kreditkartendaten ab. In einigen Fällen kommt die erste Nachricht auch per SMS mit der Bitte, die Kommunikation per WhatsApp weiterzuführen.

Die Polizei rät

Wer solche Nachrichten von vermeintlichen Familienmitgliedern oder nahestehenden Menschen erhält, sollte nicht darauf antworten. Den Tätern würde nämlich durch eine Antwort bestätigt, dass der angeschriebene Telefonkontakt tatsächlich existiert.

Unter keinen Umständen sollte man Geld an ein Bankkonto überweisen – egal ob im In- oder Ausland. Stattdessen sollte versucht werden, dieses oder auch andere Familienmitglieder

telefonisch über die bislang bekannte Nummer zu kontaktieren und zunächst über den Sachverhalt zu sprechen. Stellt sich heraus, dass es sich um einen Betrugsversuch handelt, sollte der Chatverlauf nicht gelöscht und die Polizei verständigt werden. Das können Sie auch online machen.

Zudem warnt die Polizei davor, sein Konto unbekannten Personen zur Verfügung zu stellen oder für solche Personen Konten zu eröffnen. Diese Konten werden oftmals für die Entgegennahme inkriminierter Gelder genutzt. Der Kontoinhaber macht sich damit der Geldwäsche schuldig.

Quelle: https://www.pcwelt.de/article/2000978/polizei-verhaftet-whatsapp-betrueger.html?utm_date=20230727123737&utm_campaign=Security&utm_content=Title%3A%20Polizei%20verhaftet%20Whatsapp-Betr%C3%BCger%3A%20So%20lief%20der%20Betrug&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) "Direkt kaufen" – Neue Funktion bei Kleinanzeigen könnte zu Verwirrung führen

Kleinanzeigen führt eine neue Funktion ein, die die Plattform noch sicherer machen soll. Doch ganz unkompliziert ist sie nicht.

Ende April vollzog die Verkaufsplattform kleinanzeigen.de endgültig die Trennung vom einstigen Mutterkonzern Ebay – mit neuem Logo und aufgefrischtem Design. Nun gehört Kleinanzeigen zur norwegischen Adevinta-Gruppe, die auch immer wieder neue Funktionen einführt.

So gibt es nun etwa die Option, Gegenstände direkt zu kaufen, ohne einen langwierigen Chat mit dem Verkäufer anzufangen. "Direkt kaufen" soll in Kombination mit der "Sicher bezahlen"-Funktion einen noch größeren Schutz vor Betrügern gewährleisten. Diese treiben sich nämlich gerne auf der Verkaufsplattform herum.

Funktion muss manuell wieder ausgestellt werden

Doch ganz so unkompliziert scheint diese neue Funktion nicht zu sein. Wie das Technikportal "t3n" berichtet, muss man sich als Verkäufer zuerst bei der Webseite "Online Payment Platform" registrieren, um das Geld aus dem Verkauf zu erhalten. Das heißt auch, dass man dort seine Kontodaten hinterlegen muss.

Diese Plattform ist "t3n" zufolge zwar sicher – sie ist der offizielle Zahlungsdienstleister von Kleinanzeigen. Trotzdem könnten Nutzer erst einmal verwundert bis abgeschreckt sein, wenn sie sensible Daten auf einer anderen Website hinterlegen müssen.

Was auch viele umständlich finden könnten: Hat man "Direkt kaufen" einmal aktiviert, ist diese Funktion als Standard eingestellt. Wer das nicht möchte, muss sie bei jedem neuen Inserat, was man als Verkäufer erstellt, manuell ausstellen. Eine generelle Option zum Ausschalten gibt es nicht.

Quelle: https://www.t-online.de/digital/aktuelles/id_100211028/kleinanzeigen-darum-koennte-eine-neue-funktion-nutzer-jetzt-verwirren.html

6) Phishing: Vorsicht vor angeblicher Telekom-Rechnung

Betrüger versuchen sich im Namen der Telekom Kontodaten von E-Mail-Empfängern zu erschleichen.

Die Verbraucherzentrale Schleswig-Holstein warnt in dieser Woche vor einer neuen Phishing-Masche per E-Mail. Betrüger geben sich dabei als die Deutsche Telekom aus und versuchen sich unter anderem Kontodaten zu erschleichen.

Probleme mit der Festnetz-Rechnung

Im E-Mail-Posteingang wollen die Betrüger mit dem Betreff “Ihre Telekom Festnetz-Rechnung Juni 2023 (Buchungskonto: <beliebige zehnstellige Nummer>)“ Aufmerksamkeit erregen. Mit einem Header im typischen Telekom-Magenta sowie dem Logo und dem Slogan des Telekommunikationsanbieters soll Seriosität vorgegaukelt werden. Im E-Mail-Text heißt es dann:

“Leider ist es uns nicht gelungen, den untenstehenden Rechnungsbetrag von Ihren bei uns registrierten IBAN-Daten abzubuchen. Wir empfehlen Ihnen, die Zahlung manuell über den unten stehenden Link vorzunehmen. Aktualisieren Sie außerdem Ihre Zahlungsdaten, um zukünftige Probleme zu vermeiden. Mit freundlichen Grüßen, Ihre Telekom.“

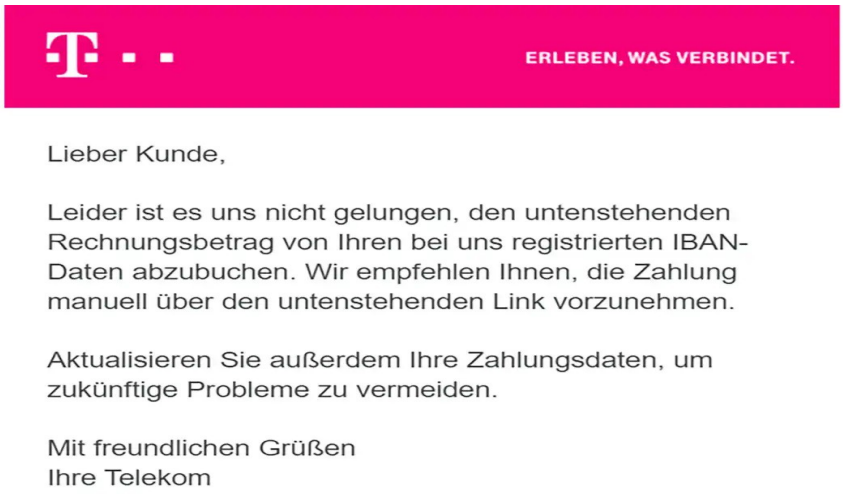


Bild: Verbraucherzentrale Schleswig-Holstein

Zahlungslink führt zu Phishing-Seite

Nachfolgend findet sich ein farblich hinterlegter Kasten, der den angeblich nicht gezahlten Rechnungsbetrag für Juni 2023 zeigen soll, sowie ein Button mit der Aufschrift “RechnungOnline ansehen”“”. Klicken Sie auf diesen Link, werden Sie zu einer gefälschten Telekom-Seite weitergeleitet, auf der die Betrüger Ihre Login-Daten, persönliche Angaben und Kontodaten abgreifen wollen.

Daran erkennen Sie den Betrugsversuch

Weitere Hinweise, dass diese E-Mail unseriös ist, liefern die unpersönliche Anrede und die falsche Verwendung von Groß- und Kleinschreibung im E-Mail-Text. Bei der Tatsache, dass die E-Mail die einzelnen Rechnungsposten nicht aufschlüsselt, sollten Sie ebenfalls stutzig werden. Bei dieser E-Mail handelt es sich um einen Betrugsversuch. Klicken Sie keinesfalls auf den Link und geben Sie dort persönliche Daten ein. Sie sollten die E-Mail ignorieren und in Ihren Spam-Ordner verschieben.

Quelle: https://www.pcwelt.de/article/2000132/phishing-vorsicht-vor-angeblicher-telekom-rechnung.html?utm_date=20230727124834&utm_campaign=Security&utm_content=Title%3A%20Phishing%3A%20Vorsicht%20vor%20angeblicher%20Telekom-Rechnung&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

7) Beliebte App – Darum sollte man beim Onlineshop Temu vorsichtig sein

Die Onlineshopping-App von Temu stürmt die Charts der App-Stores. Hier bekommt man alles besonders billig. Und deswegen ist Vorsicht geboten.

Wer freut sich in Zeiten hoher Inflation und steigender Preise nicht über ein wahres Schnäppchen? Der Onlineshop Temu wirbt gerade mit unglaublich niedrigen Preisen – und dem Slogan "Shoppe wie ein Milliardär!".

In den sozialen Netzwerken rührt das amerikanische Unternehmen kräftig die Werbetrommel – mit Erfolg. Die App steht in den App Stores von Apple und Google Play an erster Stelle der beliebtesten Anwendungen. Doch trotz der Beliebtheit des Onlineshops wird die Kritik daran immer lauter.

Kopfhörer für vier, Schallzahnbürste für fünf Euro

Wer sich auf der Webseite umschaut – man muss sich dafür zunächst registrieren –, dem fällt schnell auf, wie unfassbar billig die Produkte sind. Es gibt Bluetooth-Kopfhörer, die gerade einmal knapp vier Euro kosten, T-Shirts für drei Euro, Schallzahnbürsten für fünf Euro.

Auch wenn sich manche über die extremen Schnäppchen freuen, werden andere bei solchen Preisen misstrauisch. Wie kann es sein, dass eine Schallzahnbürste bei Temu nur fünf Euro kostet, wenn sie woanders gut und gerne 100 Euro kosten kann?

Nutzer beschweren sich über schlechte Qualität

Die Antwort: Es handelt sich meistens um Billigware. Auf "Trustpilot" findet man viele Bewertungen, in denen über die mangelhafte Qualität der Produkte berichtet wird. In einigen Fällen funktioniere die Ware gar nicht, sei beschädigt oder kaputt.

Einige Benutzer geben sogar an, auf Temu betrogen worden zu sein. Sie hätten ihre Bestellung bezahlt, die Ware sei allerdings nie angekommen. Auch über den "schlecht erreichbaren" Kundenservice hagelt es Beschwerden, ebenso wie über die unzähligen Mails mit Angeboten und Rabatten.

Doch es gibt auch viele positive Bewertungen auf "Trustpilot". Trotz der niedrigen Preise sei die Qualität gut, es gebe keine Lieferkosten, die Lieferung an sich sei schnell und der Kundenservice gut. Ob diese Kritiken echt sind, ist unklar. In auffällig vielen positiven Bewertungen findet sich ein Gutscheincode für den Onlineshop.

Temu basiert auf Marktplatz-System

Schuld an den Kritikpunkten an Temu ist auch das System, das dahinter steckt. Denn es handelt sich hierbei weniger um einen klassischen Onlineshop als vielmehr um einen Internet-Marktplatz – ähnlich wie etwa AliExpress. Temu fungiert dabei sozusagen als Vermittler zwischen den Kunden und den Händlern, die meistens in China sitzen.

Oft bieten diese Marktplätze Waren aus allen möglichen Bereichen an – von Elektronik über Mode bis hin zu Möbeln. Dieses riesige Angebot ist auch möglich, weil diese Anbieter keine eigenen Lager haben. Der Kunde bestellt zwar auf Temu, kauft aber eigentlich Produkte von einem dritten Händler.

Bei Nutzung der App ist Vorsicht geboten

Das heißt eben auch, dass Temu oder andere Internet-Marktplätze die Qualität der angebotenen Waren nicht überprüfen können, da sie mit ihnen nicht in Kontakt kommen. Bei

einer großen Webseite mit einem solch enormen Angebot können sich auch Betrüger einschleichen und von dem Hype um die App profitieren.

Wer also wirklich mal "wie ein Milliardär" shoppen will, sollte vorsichtig sein. Auch wenn Temu an sich keine Abzock-Webseite ist, besteht ein gewisses Risiko, dass man doch in eine Falle tappt oder ein Produkt von minderwertiger Qualität erhält. Braucht man eine neue Schallzahnbürste oder Bluetooth-Kopfhörer, ist man besser beraten, solche Geräte in einem Fachgeschäft zu kaufen.

Quelle: https://www.t-online.de/digital/internet/id_100210460/temu-achtung-darum-sollte-man-bei-diesem-onlineshop-vorsichtig-sein.html

8) How-To – Identitätsdiebstahl: So reagieren Sie im Ernstfall richtig

Kriminelle nehmen im Netz die Identität einer anderen Person an, um in deren Namen Waren zu bestellen und Konten zu eröffnen. Als Opfer eines solchen Betrugs müssen Sie schnell handeln.

Sind Sie bereits Opfer eines Identitätsdiebstahls geworden? Haben Sie in Ihrem Posteingang und im Briefkasten Rechnungen, Mahnungen, Inkassoschreiben gefunden, die Sie zur Bezahlung von Waren auffordern, die Sie **weder bestellt noch geliefert** bekommen haben? Oder gab es bei einem Ihrer Konten schon einmal **unerklärliche Geldabflüsse**?

Das alles sind Anzeichen für einen **Identitätsdiebstahl**. Ein Krimineller oder eine Bande haben die persönlichen Daten einer Person ausgespäht und missbrauchen sie nun, um unter falschem Namen Geschäfte zu tätigen oder diese Person zu bestehlen.

Es gibt dabei eine ganze Reihe von Methoden, nach denen die Betrüger vorgehen. Auf der anderen Seite können Sie jedoch auch Vorsorge treffen und sich schützen. Außerdem erfahren Sie in diesem Artikel, wie Sie nach der Entdeckung eines Identitätsdiebstahls reagieren sollten.

Wie Kriminelle an Ihre Daten gelangen

In vielen Fällen sind gar nicht Sie selbst schuld, wenn andere Personen Ihre persönlichen Daten entwenden. Ständig werden neue Fälle bekannt, in denen Adress-, Mail- und andere Daten aus den **Datenbanken von Unternehmen** plötzlich im Internet auftauchen. Unzureichende Datenschutz-Maßnahmen, Programmierfehler, unvorsichtige und schlecht geschulte Mitarbeiter – die Liste der potenziellen Schwachstellen ist lang.

Gleichzeitig registrieren die Polizeibehörden und Verbraucherzentralen allerdings auch eine starke Zunahme an **Phishing-Mails**, die sich direkt an die Endkunden richten: Dazu zählen etwa gefälschte Mails von Banken, die die Adressaten auffordern, auf einer Fake-Website ihre Daten einzugeben. Auch die Onlineversion des Enkeltricks ist beliebt: Betrüger geben sich in sozialen Medien gegenüber älteren Menschen als Enkel oder andere Verwandte aus und versuchen im Chat, persönliche Informationen und Bankdaten aus ihnen herauszulocken.

Noch recht neu ist folgende Masche: Ein Krimineller stellt sich seinem Opfer als Mitarbeiter eines Marktforschungsinstituts vor, das ein neues Videoident-Verfahren testen will. Tatsächlich eröffnet der ahnungslose Verbraucher jedoch ein echtes Konto, für das er die Daten des angeblichen Mitarbeiters einträgt. Nach dem anschließenden Videoident-Verfahren sind Daten sogar amtlich bestätigt. Dieses Konto bildet anschließend den Grundstein für einen Online-Shop, der gefälschte Markenartikel oder Waren anbietet, die nie geliefert werden.

Und schließlich wird das Netz immer noch überschwemmt von Mails, die im Anhang einen **Trojaner-Virus** mitbringen. Öffnet der Empfänger diese Datei, wird die Malware sofort installiert und überwacht oftmals die Tastatureingaben, um Bankdaten und Passwörter abzufangen.

Darauf haben es Kriminellen abgesehen

Wenn es einem Betrüger gelingt, beispielsweise die Daten des Paypal-Kontos einer Person zu ergattern, kann er in deren Namen Waren aller Art bestellen. Dabei hat er jedoch ein Problem: Lässt er die Waren an die Adresse seines Opfers liefern, ist es sehr schwierig und riskant, die Lieferungen abzufangen. Seine eigene oder die Adresse eines Bekannten anzugeben, wäre hingegen sehr dumm. Auch die anonyme Anmietung einer Packstation ist kaum möglich.

Kriminelle konzentrieren sich daher auf **immaterielle Güter**: Unter falschem Namen bestellen sie beispielsweise Software und Hörbücher, Abos für Streaming-Dienste wie Netflix oder Spotify, die Zugangsdaten für Dating-Portale oder kostenpflichtige Mailkonten. Die Lizenzschlüssel und Anmeldeinformationen verkaufen sie anschließend in vielen Fällen einfach weiter.

Unberechtigte Abbuchungen vom eigenen Bankkonto

Häufig geht es nur um kleinere Beträge in **maximal zweistelliger Höhe**: Wenn Sie bei der Durchsicht Ihrer Kontoauszüge feststellen, dass regelmäßig Abbuchungen stattfinden, die Sie nicht veranlasst haben, sollten Sie schnell handeln. Der erste Ansprechpartner ist immer Ihre Bank. Informieren Sie das Kreditinstitut in einer Filiale, per Telefon oder online, dass die Abbuchungen nicht von Ihren vorgenommen wurden. Mit dem Notruf *116 116* können Sie das Konto vorübergehend auch ganz sperren. Ändern Sie zudem sofort Ihr Zugangspasswort.

In der Regel bekommen Sie als Opfer eines Betrugs das Geld von Ihrer Bank zurück. Achtung: **Dabei gilt eine Frist von acht Wochen**. Spätere Reklamationen werden nicht mehr berücksichtigt.

Und: Voraussetzung ist, dass Sie nicht fahrlässig mit Ihren Daten umgegangen sind. Wenn Sie etwa auf einer plump gefälschten Website Ihre Kontodaten eingegeben haben, erhalten Sie keine Rückzahlung von Ihrer Bank.

Außerdem sollten Sie bei der Polizei Anzeige erstatten. Das geht entweder persönlich bei der nächsten Polizeidienststelle oder online. Die Webadressen der Online Polizeiwachen der Länder finden Sie hier.

Rechnungen für nicht bestellte Waren

Wenn Sie Ihre Bank einen unberechtigt abgebuchten Betrag zurückbuchen lassen, erhalten Sie eventuell eine **Mahnung**, verschickt von dem Unternehmen, dessen Waren der Betrüger in Ihrem Namen bestellt hat. Sie sollten eine solche Mahnung nicht einfach ignorieren, sondern den Vertragsabschluss **bestreiten**, am besten per Einschreiben. Dabei ist es hilfreich, wenn Sie eine Kopie Ihrer Anzeige bei der Polizei mitschicken können.

Eventuell erhalten Sie auch einen **Mahnbescheid**. Mahnbescheide werden von einem Gericht ausgestellt und wiegen daher erheblich schwerer als Mahnungen. Sie haben in diesem Fall lediglich **zwei Wochen Zeit, um Widerspruch einzulegen**. Versäumen Sie diese Frist, müssen Sie den eingeforderten Betrag oft sogar dann bezahlen, wenn Sie die Ware nicht bestellt haben. Denn das Gericht überprüft nicht die Rechtmäßigkeit der Forderung. Für den Widerspruch liegt dem Mahnbescheid ein Formular bei. Wenn der Widerspruch rechtzeitig erfolgt, muss nun die Gegenseite beweisen, dass ihr Anspruch berechtigt ist.

Achtung bei Inkassoschreiben

Bei **Inkassoschreiben** hingegen sollten Sie in einem ersten Schritt genau prüfen, ob sie echt sind. Betrüger verschicken teilweise gefälschte Inkassobriefe, in denen sie Sie unter allerlei Drohungen und durch Setzen knapper Fristen dazu bringen wollen, ihnen Geld zu überweisen. Wenn die Forderung per Mail kommt, können Sie sogar sicher sein, dass es sich um eine Fälschung handelt – echte Inkassofirmen verschicken ihre Schreiben per Post.

In einem ersten Schritt sollten Sie das Inkassounternehmen googeln: Setzen Sie im Suchfeld den Zusatz „Erfahrung“ hinter den Namen der Firma. Eventuell stoßen Sie so auf Meldungen, dass das Unternehmen bereits in der Vergangenheit gefälschte Forderungen erhoben hat. Sehen Sie sich die Website an und überprüfen Sie bei Google Maps die angegebene Adresse.

Die Verbraucherzentralen bieten zudem eine kostenlose Überprüfung einer Inkassoforderung an. Unter www.verbraucherzentrale-brandenburg.de/schwarzliste-inkasso finden Sie zudem eine Blacklist mit unseriösen Inkassofirmen.

Falls das Inkassoschreiben seriös, die Forderung jedoch unberechtigt ist, müssen Sie Widerspruch einlegen. Außerdem erstatten Sie am besten Anzeige bei der Polizei.

Die Schufa benachrichtigen

Nicht bezahlte Rechnungen können sich negativ auf Ihre Schufa-Bewertung auswirken. Aus diesem Grund sollten Sie die Schufa über den Identitätsdiebstahl benachrichtigen. Die Wirtschaftsauskunftei hat zu diesem Zweck unter www.schufa.de eine Infoseite eingerichtet, wo Sie eine entsprechende Meldung abgeben können. Sie benötigen dafür zusätzlich Kopien Ihres Personalausweises und Ihrer Strafanzeige bei der Polizei.

Neben der Schufa sollten Sie unter www.crif.de/identitaetsbetrugsmeldung auch die Auskunftei Crif benachrichtigen.

Drei Tools für den Identitätsschutz

Einige Hersteller von Antivirenprogrammen bieten den Anwendern Programme für den Schutz ihrer Identität an. Diese Tools sind meist in die großen Software-Suiten der Firmen integriert, teilweise jedoch auch separat erhältlich. Drei dieser Spezialprogramme für Identity Protection haben wir uns angeschaut: Avira Identity Assistant, Bitdefender Digital Identity Protection und F-Secure ID Protection.

Wie funktionieren diese Tools? Der wichtigste Programmbaustein ist bei allen drei Programmen die Suche nach digitalen Spuren im Internet. Sie sehen nach, ob die Mailadresse des Benutzers und andere persönliche Daten in Darknet-Foren oder Datenbanken mit gestohlenen Anmeldedaten auftauchen. Dazu scannen sie bekannte Listen mit Benutzerdaten und Passwörtern, die Hacker in den vergangenen Jahren beispielsweise bei Einbrüchen in die Server von Adobe, Bitly oder bei der portugiesischen Fluglinie TAP erbeutet und anschließend im Internet veröffentlicht haben. Dabei sind sie unterschiedlich erfolgreich.

1. Avira Identity Assistant

Avira Identity Assistant bietet nach der Anmeldung neun Kategorien für die Eingabe persönlicher Daten an. So nimmt es die Mailadresse(n) auf, Telefonnummern, Kreditkartendaten, Bankkonten, die Anschrift, Führerschein, ein oder mehrere Gamer-Tags, Versicherungsdaten und den Mädchennamen der Mutter. Beim ersten Start sucht es sofort nach diesen Daten im Darknet, zusätzlich richtet es eine ständig aktive Überwachung ein. Findet es die eingegebenen Daten, erhält der Benutzer eine Benachrichtigung – eine

Funktion, die sich bei allen drei Programmen findet.

Im Test fiel die Ausbeute recht gering aus: Die einzige Fundstelle stammte von einem Datendiebstahl bei Adobe aus dem Jahr 2013.

Der Avira Identity Assistant zeichnet sich jedoch in einem Punkt gegenüber den beiden Konkurrenten aus: Verknüpft mit dem Abo ist die Möglichkeit, sich mit spezialisierte Support-Mitarbeitern zu verbinden, die dem Kunden sowohl bei einem Identitäts- wie auch bei einem Brieftaschendiebstahl mit Rat und Tat zur Seite stehen, die Gefährlichkeit einschätzen, Tipps geben und dabei helfen, beispielsweise eine gestohlene Kreditkarte zu sperren und einen Ersatz zu beantragen.

2. Bitdefender Digital Identity Protection

Der Identitätsschutz von Bitdefender überwacht die Mailadresse(n) und die Telefonnummer des Kunden. Nach der Anmeldung gleicht ein Assistent im Internet frei zugängliche, persönliche Daten wie Namen, Telefonnummern, Geburtsdatum mit dem Benutzer ab, um den digitalen Fußabdruck zu ermitteln, den er im Internet bereits hinterlassen hat. Einige Fundstellen stammen aus Dateneinbrüchen, einige andere von öffentlich zugänglichen Quellen, etwa Google.

Unter „Datenpannen“ findet man schließlich die Daten, die eindeutig einem Datenklau zuzuordnen sind. Angegeben ist jeweils, welche Informationen im Internet verfügbar sind. Bitdefender fand im Test 17 Einträge und bot Links zu den betroffenen Websites an, damit der Benutzer die Zugangsdaten ändern konnte. Leider blendet das Tool die gefundenen Passwörter nicht ein. Aufgelistet sind auch mehrere Combolisten, die Informationen aus mehreren Dateneinbrüchen zusammenfassen.

Hier heißt es lapidar „Ändern Sie die Anmeldedaten für alle Ihre Online-Benutzerkonten, die mit Ihren offengelegten Daten verbunden sind“. Um welche Konten und Daten es sich handelt, erfährt man allerdings nicht.

3. F-Secure ID Protection

Das Tool von F-Secure besteht im Wesentlichen aus einem Passwortmanager, der lokal auf dem PC installiert wird. Als zusätzliche Funktion bringt die Software eine Suchfunktion nach veröffentlichten, persönlichen Daten mit.

F-Secure ermittelte 25 Fundstellen, wo Benutzernamen und Passwörter des Autors frei zugänglich im Internet standen. Bei etwa der Hälfte davon handelte es sich um Combolisten, die Daten aus mehreren Einbrüchen versammelten. Hilfreich ist, dass der Dienst jeweils auch die gefundenen Passwörter angibt, so dass der Benutzer sehen kann, ob die Anmeldedaten noch aktuell oder bereits veraltet sind.

Neben den Mailadressen überwacht F-Secure auf Wunsch auch Kreditkartendaten, Telefonnummern, Personalausweis, Reisepass und Führerschein sowie Bankkonten und Benutzernamen.

Fazit: F-Secure arbeitet am gründlichsten und zeigt als einziges Tool die veröffentlichten Passwörter an. Der Funktionsumfang ist jedoch nur mager. Avira kann nur wenige Ergebnisse vorweisen, bietet aber individuellen Support. Die Empfehlung ist daher Bitdefender, das gute Ergebnisse und viele Funktionen bietet.

Quelle: https://www.pcwelt.de/article/1188422/identitaetsdiebstahl-tipps.html?utm_date=20230727132627&utm_campaign=Security&utm_content=Title%3A%20Identit%C3%A4tsdiebstahl%3A%20So%20reagieren%20Sie%20im%20Ernstfall%20richtig&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

9) News – Betrug, Gewinnspiele, Beleidigungen: Vorsicht vor Anrufen mit diesen Telefonnummern

Wenn eine dieser Telefonnummern auf Ihrem Display erscheint, ist größte Vorsicht angesagt. Wir stellen die gefährlichsten Telefonnummern vor.

Das österreichische Sicherheitsnachrichtenportal Mimikama hat für April die Liste der zehn gefährlichsten Telefonnummern veröffentlicht. Die Auswertung basiert auf Clever Dialer, das eine App zum Schutz vor Telefonspam anbietet. Update 9.5.2023: Auf der Webseite von Clever Dialer findet man mittlerweile auch die aktuelle Auswertung für April 2023. Clever Dialer hatte nämlich bis vor Kurzem nur die alte Statistik für März 2023 auf seiner Webseite gehabt. Update Ende. Diese haben wir damals für unsere Meldung, Das sind die zehn gefährlichsten Telefonnummern, ausgewertet.

Laut der neuen April-2023-Auswertung ist erneut eine Festnetznummer aus Berlin die meistgenutzte Nummer für Telefonspam (schon im März 2023 war Berlin der Spammerkönig). Dabei handelt es sich um die 03025555453. Wer von dieser Nummer angerufen wird, bekommt ein Gewinnspiel aufs Auge gedrückt. Auch im März 2023 stammte die Königin der Spamnummern aus Berlin, es war aber eine andere Ziffernkombination.

Auf Platz zwei der größten Spam-Telefonnummern liegt eine Nummer aus dem schönen Mailand: +390240707879. Auch dabei handelt es sich um Gewinnspielspam. Auf den nächsten Plätzen folgen Nummern aus Düsseldorf (021136189051; Werbeanrufe), Frankfurt am Main (06929917782; Daueranrufe ohne Inhalt) und München (08948402073). Bei der Münchner Nummer handelt es sich um einen Betrugsversuch, wie ein Betroffener schildert:

„Der Mann hatte mir gleich am Anfang des Gesprächs eine Frage gestellt: Wie ich denn die Apothekenpreise derzeit finde? Dann habe ich angeblich im Februar ein Abo abgeschlossen und heute wollte man das auf ein Probeabo für 3 Monate umstellen. Sonst müsste man es als Jahres-Abo weiterlaufen lassen. Am besten direkt auflegen, wenn diese Nummer anruft!“

Mimikama.at nach Clever Dialer

Weiter geht es in der Top10 des Telefonspams mit der Mobilfunknummer 01784493212, die in beleidigender Weise ein Gewinnspiel andrehen will, mit einer weiteren Berliner Nummer (030232556409; Gewinnspiel), Düsseldorf (021187399110; Werbung für Zahnzusatzversicherung), noch einmal Berlin (03025555450; Abo-Betrug) und schließlich Hagen-Hohenlimburg (023344936; Gewinnspielbetrug).

So reagieren Sie richtig

Legen Sie sofort auf, wenn Ihnen der Inhalt des Telefongesprächs merkwürdig vorkommt und Sie den Anruf nicht erwartet haben. Nennen Sie keinesfalls Daten von sich und sperren Sie die Nummer sofort in Ihrem Router. Mehr dazu lesen Sie in Fritzbox: Sperrliste gegen Spam-Anrufe erstellen.

Tipp: Nie wieder Spamanrufe! So wehren Sie sich
Telefonbetrug: Vorsicht vor diesen Telefonnummern
Die 10 gefährlichsten Telefonnummern für Telefonterror, aggressive Werbung etc.

Quelle: https://www.pcwelt.de/article/1807775/betrug-gewinnspiele-beleidigungen-telefonspam.html

10) Schutz vor Stalking – Diese WhatsApp-Einstellungen sollten Sie prüfen

Die Deutschen chatten am liebsten über WhatsApp. Derzeit jagt ein Kettenbrief vielen Nutzern einen Schrecken ein. Was steckt dahinter?

Aktuell macht ein Kettenbrief die Runde, wonach WhatsApp heimlich die Datenschutzeinstellungen für Chatgruppen geändert hat. "Das bedeutet, dass jeder WhatsApp-Nutzer – auch wenn du ihn nicht kennst – dich ohne dein Wissen und ohne deine Zustimmung zu jeder beliebigen Gruppe hinzufügen kann", heißt es in der bedrohlich klingenden Nachricht. In der Folge drohten Spam und sogar Hackerangriffe. Einigen Nutzern dürfte so eine Nachricht einen gehörigen Schrecken einjagen.

1. Das sollten Sie regelmäßig tun: Datenschutzeinstellungen prüfen

Dabei besteht kein Grund zur Panik. In Wahrheit handelt es sich bei der "heimlichen Änderung" nämlich um eine Standardeinstellung bei WhatsApp. Doch offenbar ist nicht jedem Nutzer klar, dass man diese ändern kann – was von Datenschützern regelmäßig empfohlen wird.

Tatsächlich hatte WhatsApp die Datenschutzoptionen für Gruppen bereits 2019 eingeführt, um Spam-Einladungen einen Riegel vorzuschieben. Davor war es tatsächlich möglich, jeden beliebigen WhatsApp-Nutzer gegen seinen Willen zu einer Gruppe hinzuzufügen und die Funktion für allerlei Unsinn zu missbrauchen. Die Opfer konnten nichts weiter tun, als die Gruppe anschließend wieder zu verlassen und den Kontakt zu blockieren.

So ändern Sie die Gruppeneinstellungen

Die Gruppeneinstellungen sind bei WhatsApp aber nach wie vor standardmäßig auf "Jeder" gestellt. Das heißt, nach einer Neuinstallation der App kann Sie erst mal jeder zu einer Gruppe hinzufügen. Um das zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die WhatsApp-Einstellungen.
2. Tippen Sie auf "**Account**".
3. Dann auf "**Datenschutz**".
4. Tippen Sie auf den Eintrag "**Gruppen**" im unteren Bereich.
5. Legen Sie fest, wer Sie zu einer Gruppe hinzufügen darf.
6. Bestätigen Sie die Auswahl mit "**Fertig**".

Übrigens: Bei Software lohnt es sich generell, die Einstellungen hin und wieder zu prüfen. Nach einem größeren Update kann es sein, dass die App-Einstellungen wieder auf die Standardwerte zurückgesetzt werden.

In diesem Fall handelt es sich jedoch um ein Gerücht, dass die Einstellungen heimlich und ohne Zutun des Nutzers geändert wurden. Der genannte Kettenbrief ist offensichtlich darauf ausgelegt, Panik und Misstrauen zu verbreiten – und stößt damit vor allem bei Nutzern auf Resonanz, die bisher von den Datenschutzoptionen nichts wussten oder einfach nur vergessen haben, welche Einstellungen sie vor Jahren einmal festgelegt haben.

Am besten nutzen Sie die Gelegenheit, um alle WhatsApp-Einstellungen zu überprüfen. t-online fasst hier die nützlichsten Tipps und Tricks zusammen, mit denen Sie nervige Probleme vermeiden und WhatsApp optimieren.

2. Speicherplatz und Datenvolumen sparen

Jeder ist in einer dieser Gruppen, wo ständig mehr oder weniger lustige Katzenvideos geteilt

werden. Ist der Speicherplatz des Smartphones fast voll, aber Sie wissen nicht genau, welcher Chat am meisten Speicher raubt? Machen Sie einen Abstecher in die WhatsApp-Einstellungen. Unter "**Speicher und Daten**" und anschließend "**Speicher verwalten**" werden Ihnen alle Chats und deren Speichernutzung angezeigt. Klicken Sie auf den jeweiligen Chat, um die Mediendateien zu sehen, die den Speicher belegen. Tippen Sie auf "**Wählen**" und anschließend auf die Inhalte, die Sie löschen möchten. Wer will, kann unten "Alle auswählen" selektieren. Per Tipp auf das Mülleimersymbol werden die gewählten Inhalte gelöscht.

Um zu vermeiden, dass Bilder direkt beim Eintreffen heruntergeladen werden, sollten Sie unter "Speicher und Daten" die Einstellungen prüfen. Dort können Sie festlegen, dass Videos beispielsweise nur bei WLAN-Verbindungen heruntergeladen werden, um das Datenvolumen zu schonen.

3. Live-Standort teilen

Sie treffen sich mit einem Freund und wollen ihm Ihren aktuellen Standort nennen, die Adresse wissen Sie jedoch nicht? WhatsApp bietet eine einfache Funktion, mit der Sie Ihren Standort einmalig oder für eine begrenzte Zeit teilen können.

Gehen Sie einfach in den jeweiligen Chat, tippen Sie links unten auf das "+"-Symbol und wählen dann "Standort" aus. Anschließend können Sie sich entscheiden, ob Sie Ihren "Aktuellen Standort senden" oder den sich ständig aktualisierenden "Live-Standort teilen" möchten. Entscheiden Sie sich für Letzteren, können Sie auswählen, ob dieser für 15 Minuten, eine oder acht Stunden geteilt werden soll. Danach endet die Mitteilung automatisch wieder.

4. Nachrichten löschen

Haben Sie Ihrem Chef eine Nachricht geschickt, die eigentlich an eine andere Person adressiert war? Mittlerweile können Nachrichten bei WhatsApp gelöscht werden. Sollten Sie den Fauxpas binnen einer Stunde merken, dann halten Sie einfach die versehentlich geschickte Nachricht gedrückt, wählen "Löschen" aus und danach "Für alle löschen". Dadurch wird die Nachricht wieder zurückgeholt. Anstatt der falschen Nachricht verbleibt nur noch der Hinweis "diese Nachricht wurde gelöscht".

5. WhatsApp-Kamera vermeiden

Schnell noch ein Gruppen-Selfie mit der WhatsApp-Fotofunktion machen und dann direkt in der Gruppe mit den anderen Teilnehmern teilen? Nehmen Sie sich lieber die Zeit und wechseln Sie in die Kamera-App des Smartphones. In der Regel machen diese nämlich die deutlich besseren Aufnahmen. Außerdem bleiben die Aufnahmen Ihnen so in höherer Qualität in der Fotogalerie erhalten.

Wollen Sie nur schnell eine Notiz verschicken, dann reicht die WhatsApp-Fotofunktion aus. Sollte dann übrigens die Vorderkamera als erstes erscheinen, tippen Sie einfach zweimal auf das Display und schon wechselt WhatsApp zur Kamera auf der Rückseite.

6. Chats stummschalten

Besonders Gruppenchats sind für ein hohes Nachrichtenaufkommen berüchtigt. Doch gerade, wenn Sie sich auf eine wichtige Aufgabe konzentrieren müssen, nerven diese schnell. Um nicht gleich aus der Gruppe auszutreten, können Sie sie einfach stummschalten.

Wählen Sie einfach den Chat aus, klicken Sie oben auf den Namen, um auf die Übersicht zu gelangen und navigieren Sie zum Reiter "Stumm". Nun können Sie auswählen, ob Sie den Chat für acht Stunden, eine Woche oder gleich ein ganzes Jahr stummschalten wollen.

7. Sprachnachrichten freihändig aufnehmen

Wenn die Sprachnachricht ein wenig länger wird, kann es mit der Zeit recht anstrengend werden, den Finger auf dem Mikrofon-Symbol zu halten. Verrutscht der Finger dann und die Aufnahme bricht ab, ist der Ärger groß. Auch dafür hat WhatsApp Abhilfe geschaffen.

Beginnen Sie wie gewohnt mit der Aufnahme, indem Sie das Mikrofon-Symbol gedrückt halten. Nach wenigen Sekunden erscheint nun ein kleines Schloss auf Ihrem Bildschirm. Schieben Sie Ihren Finger gedrückt ein Stück weiter nach oben. Die Aufnahme ist jetzt "verriegelt" und der Finger kann weggenommen werden. Nach Fertigstellung der Sprachnachricht tippen Sie einfach auf das Papierflieger-Symbol rechts unten, mit dem Nachrichten abgeschickt werden.

8. Zwei-Schritte-Verifizierung aktivieren

Für mehr Sicherheit sorgt die Zwei-Schritte-Verifizierung. Auch WhatsApp unterstützt diese Sicherheitsfunktion. Bei solch einer Verifizierung erhält der Nutzer in der Regel nach der Passworteingabe einen Zahlencode auf das Handy. Bei WhatsApp müssen Sie sich einen sechsstelligen Code ausdenken.

Wollen Sie WhatsApp auf einem neuen Handy einrichten, dann müssen Sie diesen Code eingeben. Zwar kann dieser auch geknackt werden, aber immerhin sind Ihre Daten sicherer als ohne Code. Sollten Sie ihn mal vergessen, kann er per E-Mail zurückgesetzt werden.

Die Verifizierung in zwei Schritten aktivieren Sie in den Einstellungen unter "Account" und anschließend "Verifizierung in zwei Schritten".

9. Über WhatsApp mit bis zu sieben Freunden telefonieren und Datenvolumen sparen

Besonders für Smartphone-Nutzer ohne Anruf-Flat sind WhatsApp-Anrufe günstiger. Bis zu acht WhatsApp-Nutzer können parallel miteinander telefonieren und sich sogar dabei sehen.

Starten Sie wie gewohnt im Chatverlauf oben rechts ein Audio- oder Videoanruf. Hat der gewünschte Teilnehmer abgenommen, können Sie nun oben rechts auf das "Kontakt hinzufügen"-Symbol mit dem kleinen Plus klicken.

Alternativ kann man auch direkt einen Gruppenanruf starten. Dazu öffnet man einen entsprechenden Gruppenchat. Hat die Gruppe acht oder weniger Mitglieder, genügt ein Fingertipp auf das Telefon- oder Videosymbol, um direkt ein Gruppengespräch zu starten. Bei größeren Gruppen findet sich an der Stelle oben rechts stattdessen ein Telefonhörer mit einem "+". Tippt man darauf, kann man bis zu sieben Teilnehmer für ein Gruppentelefonat auswählen.

Achtung: Bei einem Anruf übers mobile Netz wird viel Datenvolumen verbraucht. In den Einstellungen können Sie daher unter "Speicher und Daten" im Bereich "Netzwerk" den "Weniger Daten für Anrufe verwenden"-Schalter aktivieren. Darunter leidet jedoch die Anrufqualität.

10. Kundenservice über WhatsApp

Man kann viele Stunden in Kundenservice-Warteschleifen verbringen. Da WhatsApp Unternehmen anbietet, den Kundenservice über den Messenger abzuwickeln, können Sie sich die Zeit in Zukunft getrost sparen.

Als eines der ersten Unternehmen in Deutschland bietet der Mobilfunkanbieter Vodafone diese Funktion an. Dafür müssen Sie einfach nur einen Chat mit der Nummer 0172 121 721 2 starten und schon sind Sie mit Vodafone in Kontakt. Zwar kann es sein, dass Antworten erst Stunden nach der Frage eintreffen. Dafür sind Sie nicht darauf angewiesen, die ganze Zeit

auf eine Antwort zu warten. Wie bei anderen Chats gewohnt, erhalten Sie einfach eine Push-Mitteilung.

Auch bei O2 gibt es einen WhatsApp-Kundenservice. Er lässt sich unter der Nummer 089 666 630 097 starten. Anbieter Congstar bietet seinen WhatsApp-Kundenservice unter der Nummer 0221 79 700 100 an.

Tipp: WhatsApp: Automatische Downloads abschalten
So ändern Sie die Backup-Einstellungen bei WhatsApp
So verhindern Sie WhatsApp-Stalking und Spam
Diese Fehler sollten Sie vermeiden

Quelle; https://www.t-online.de/digital/handy/id_84832458/whatsapp-kettenbrief-im-umlaf-diese-einstellungen-sollten-sie-jetzt-pruefen.html

11) Forderung nach photoTAN-Brief – Betrüger haben es auf Kunden der Deutschen Bank abgesehen

Eine besonders perfide Betrugsmasche trifft derzeit Kunden der Deutschen Bank. Die Kriminellen haben es auf Zugangsdaten für das Onlinebanking abgesehen.

Kriminelle zielen mit einer neuen Phishing-Betrugsmasche auf Kunden der Deutschen Bank ab. Während die Betrüger sich bisher für die persönlichen Daten der Bankkunden interessierten, haben sie es jetzt auf die Zugänge zum Onlinebanking abgesehen, wie die Verbraucherzentralen berichten.

Per Mail melden sich die Kriminellen bei den Kunden der Deutschen Bank, um an deren photoTAN-Brief zum Onlinebanking zu gelangen. In der Nachricht heißt es demnach, dass angeblich das Konto aus Sicherheitsgründen gesperrt worden sei. Nur mit einem Identitätsnachweis könne es wieder freigegeben werden.

In der Betrugsmail befindet sich dem Bericht zufolge ein Link, den die Empfänger für den Identitätsnachweis anklicken sollen. Dieser führt auf eine Website, auf der sich die Bankkunden anmelden und ihren photoTAN-Brief hochladen sollen.

Kriminelle erhalten vollen Zugriff auf das Konto

"Bitte beachten Sie, dass diese Maßnahmen ergriffen wurde, um unautorisierten Zugriff auf Ihr Konto zu verhindern und Ihre finanziellen Transaktionen zu schützen", schreiben die Kriminellen in ihrer Phishingmail.

Die Verbraucherschützer merken an: "Diese Aussage hat eine gewisse Ironie, wenn man bedenkt, dass durch die Eingabe der sensiblen Daten die Kriminellen vollen ungeschützten Zugriff auf Ihr Konto und Ihre Finanzen erlangen."

Deshalb rate man den Empfängern dieser E-Mail dringend davon ab, den Link zu nutzen und Daten preiszugeben.

Deutsche-Bank-Kunden waren von Datenleck betroffen

Erst vergangene Woche waren Kunden der Deutschen Bank von einem Datenleck betroffen. Bei einem externen Kontowechsel-Dienstleister hatte es einen Sicherheitsvorfall gegeben, bestätigte das Geldinstitut in Frankfurt.

Dabei seien personenbezogene Daten abgeflossen, mit denen Unbekannte aber keinen Zugang zu den Konten erlangt hätten. Nach Informationen des "Bonner General-Anzeigers" wurden Namen und IBAN gestohlen.

Wie sich später herausstellte, waren auch Kunden der Postbank, der Direktbank ING und der Commerzbank von dem Hackerangriff betroffen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100208268/deutsche-bank-vorsicht-vor-betrug-forderung-nach-phototan-brief.html

12) News – Gefälschte Windows-Updates sperren PCs und erpressen Nutzer

Sicherheitsforscher haben eine neue Ransomware entdeckt, die sich unter anderem als ein Windows-Update tarnt. Sie sperrt den Computer des Nutzers im Versuch, Geld zu erpressen.

“Big Head Ransomware” – so tauften die Sicherheitsforscher von Fortinet FortiGuard Labs eine neue Schadsoftware, die derzeit im Umlauf ist. Mehrere Varianten wurden entdeckt, sie tarnt sich unter anderem als Windows-Update oder das Textbearbeitungsprogramm Microsoft Word.

Nach der Ausführung durch den Nutzer und der Sperrung seines Computers verlangen die Cyberkriminellen die Zahlung von einem Bitcoin, was zum Zeitpunkt dieses Artikels fast 28.000 Euro entspricht.

Entdeckt wurde die Ransomware von Fortinet FortiGuard Labs, die in Ihrem Blog erstmalig darüber berichteten. Das japanische Sicherheitsunternehmen Trend Micro führte anschließend eine ausführliche Analyse der Schadsoftware durch, die Ergebnisse finden sich auf ihrer Website. Zusammengefasst arbeitet Big Head aber nicht anders als andere Ransomeware. Sie übernimmt die Kontrolle über den Computer, löscht etwaige Updates und verschlüsselt die Daten auf dem Computer. Damit der Nutzer nicht eingreifen kann, deaktiviert sie sogar den Task Manager.

Interessant, aber bei solcher Software nicht ungewöhnlich: Big Head deaktiviert sich selber, wenn es erkennt, dass eine der folgenden Systemsprachen eingestellt ist: Russisch, Weißrussisch, Ukrainisch, Kasachisch, Kirgisisch, Armenisch, Georgisch, Tatarisch und Usbekisch.

Die Ransomware wurde bislang vor allem in den USA entdeckt, erste Fälle traten aber auch schon in Spanien, Frankreich und der Türkei auf.

So schützen Sie sich

Der beste Schutz vor Ransomware ist es, keine Software aus unsicheren Quellen herunterzuladen. Beziehen Sie Ihre Software direkt vom Entwickler oder von vertrauenswürdigen Portalen. Sollte eine Schadsoftware doch auf Ihrem Computer landen, sollten Sie mit einem aktivierten Windows Defender oder einem anderen Antivirenprogramm vorgesorgt haben.

Ist Ihr Computer tatsächlich von einer Ransomware befallen und verschlüsselt, gehen Sie auf keinen Fall auf die Forderungen der Erpresser ein. Wenden Sie sich stattdessen an die Polizei, entweder über Ihre örtliche Wache oder bei einer der Online-Wachen.

Quelle: https://www.pcwelt.de/article/1994492/gefalschte-windows-updates-sperren-pcs-und-erpressen-nutzer.html?utm_date=20230727135925&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Gef%C3%A4lschte%20Windows-Updates%20sperren%20PCs%20und%20erpressen%20Nutzer&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

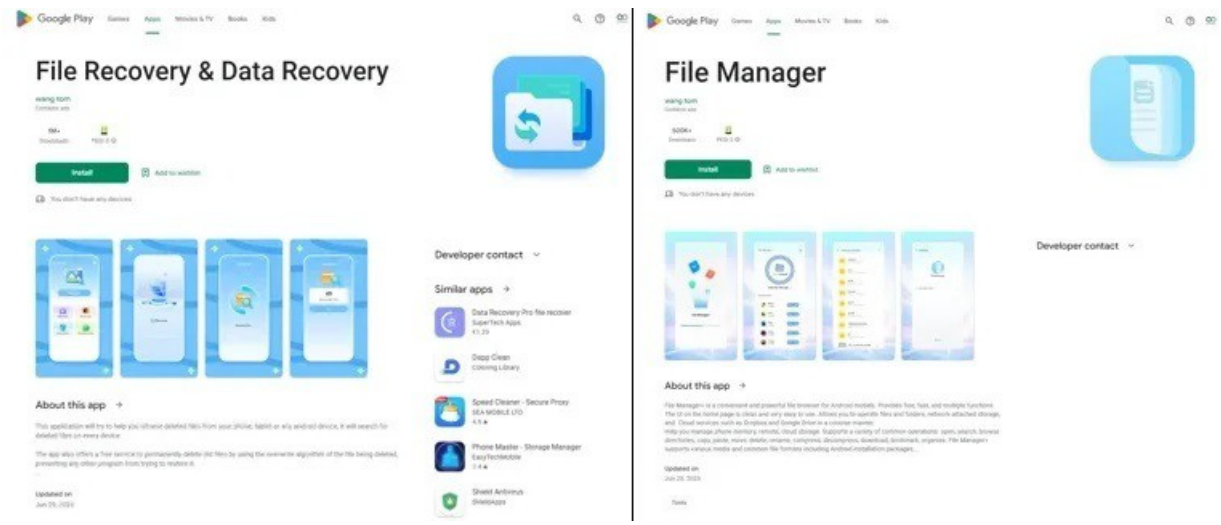
13) Sofort entfernen: Diese App verschickt deine Bilder & Videos an Kriminelle

Was man üblicherweise nicht erwartet, wenn man eine App mit Millionen Downloads installiert, ist, dass diese persönliche Nutzerdaten entwendet und an Dritte schickt. Und zwar in rauen Mengen. Doch genau das ist aktuell bei zwei Android-Anwendungen aus dem Google Play Store der Fall.

Infizierte Android-Apps stellen keine Seltenheit dar. Immer wieder entdecken Sicherheitsforscher Anwendungen mit versteckten Trojanern. Allerdings verzeichnen diese normalerweise kaum Downloads. Nicht so in diesem Fall. So wurde eine infizierte App über 500.000 Mal heruntergeladen und eine weitere sogar über 1 Million Mal. Beide Anwendungen bergen ein hohes Sicherheits- und Datenschutz-Risiko und sollten unmittelbar von dem Handy gelöscht werden. Doch das kann sich als schwieriger gestalten, als es den Anschein hat.

Zwei infizierte Android-Apps entdeckt

Sicherheitsforscher von Pradeo haben Malware in den beiden Dateimanager-Tools „File Recovery & Data Recovery“ und „File Manager“ entdeckt. Beide Anwendungen erfreuen sich hoher Download-Zahlen und beide stammen von dem gleichen Anbieter – wang tom. Im Rahmen ihrer primären Funktion sollen die Apps äußerst aggressiv vorgehen und hunderte Datenübertragungen durchführen. Zu den verschickten Informationen gehören unter anderem Bilder, Videos, Audio und Echtzeit-Standorte. Darüber hinaus auch noch Kontaktdaten aus der Kontaktliste sowie verknüpften Konten, der Netzwerkprovider, die Gerätemarke, das Modell und die Versionsnummer des Betriebssystems. Letztere können die Cyberkriminellen dazu benutzen, um im weiteren Verlauf die Schwachstellen der einzelnen Systeme zielgerichtet angreifen.



In diesen Apps versteckt sich ein Trojaner Bild: www.inside-digital.de

Bemerkenswert ist auch, dass die gestohlenen Daten nicht an einen Server, sondern an eine „große Anzahl“ von Servern verschickt werden sollen. Wobei sich die meisten der Ziele auf chinesischem Territorium befinden sollen.

So müssen Betroffene vorgehen

Die Sicherheitsexperten von Pradeo haben ihre Entdeckung mittlerweile an Google gemeldet – dem Unternehmen hinter Android. Daraufhin entfernte dieses beide Apps aus dem Play Store. Von deinem Smartphone musst du die Anwendungen indes manuell löschen. Doch das ist nicht ganz so einfach, denn die Cyberkriminellen hinter der Spyware scheinen sich unterschiedlicher Tricks bedient zu haben. So wurden die Apps zwar viele Male heruntergeladen, weisen jedoch keine Bewertungen auf. Daher gehen die Sicherheitsforscher davon aus, dass diese gefälscht seien und hier Installationsfarmen oder Emulatoren für mobile Geräte zum Einsatz kamen.

Ferner werden die Anwendungen nicht im App-Drawer oder auf dem Startbildschirm angezeigt. Einerseits, um die Existenz der Apps aus dem Gedächtnis des Nutzers zu tilgen. Und andererseits, um ihre Löschung zu erschweren. Wer die Anwendungen entfernen möchte, muss dies daher über die Einstellungen und die App-Übersicht erledigen.

Quelle: https://www.inside-digital.de/news/2-millionen-apps-schickt-deine-bilder-videos-an-dritte

14) News – Betrugsmasche: Vorsicht vor angeblichen Anrufen von Paypal

Das Landeskriminalamt Niedersachsen warnt vor einer neuen Telefon-Betrugsmasche, bei der Anrufer vorgeben, im Auftrag von Paypal zu handeln.

In dieser Woche warnt das Landeskriminalamt Niedersachen vor einer neuen Betrugsmasche, bei der sich Betrüger als Paypal-Mitarbeiter ausgeben. Wie mehrere Hinweisgeber gegenüber der Polizeibehörde bestätigten, klingelte bei ihnen das Telefon und am anderen Ende der Leitung meldete sich eine weibliche Stimme mit einer Ansage vom Tonband.

Angeblich 700 Euro an Basecoin gesendet

Die deutsch sprechende Frau behauptete in den der Polizei vorliegenden Fällen, eine Paypal-Mitarbeiterin zu sein. Sie behauptete weiterhin, dass der Angerufene gerade 700 Euro über den Bezahldienst an den Kryptowährungsanbieter Basecoin gesendet habe. Um die Transaktion rückgängig zu machen, solle der Angerufene auf seiner Telefon-Tastatur die “1“ drücken. Wie auch bei anderen Betrugsmaschen spielen die Kriminellen hier mit einer Einschüchterungstaktik, die den Angerufenen zum schnellen Handeln drängen soll, ohne allzu viel über den Anruf nachzudenken.

Kriminelle wollen möglicherweise Zugangsdaten erbeuten

Laut dem Landeskriminalamt Niedersachen hat keines der Opfer bislang eine Taste zur Weiterleitung gedrückt. Aus diesem Grund kann die Behörde nicht mit Sicherheit sagen, wie die Betrugsmasche weitergeht. Es sei jedoch denkbar, dass mit dem Drücken einer Ziffer eine reale Person am anderen Ende der Leitung den Anruf übernimmt. Diese könnte versuchen, Zugangsdaten und Kontaktinformationen des Angerufenen zu erbeuten. Es sei außerdem denkbar, dass das Opfer zum Tätigen einer echten Zahlung gedrängt werde, um die angebliche Überweisung von 700 Euro rückgängig zu machen.

Legen Sie sofort auf!

Derartige Anrufe werden meist per Call-ID-Spoofing verschleiert, indem entweder gar keine oder eine gefälschte Rufnummer angezeigt wird. Die Polizei rät allen Betroffenen, derartige Anrufe zu ignorieren und sofort aufzulegen. Sie sollten auf keinen Fall eine Taste zur

Weiterleitung drücken und während des Anrufs weder Login- noch Kontaktdaten preisgeben.

Prüfen Sie Ihre Transaktionen online

Wer sich um sein Paypal-Konto sorgt, sollte sich nach einem solchen Anruf einfach online in sein Konto einloggen und dort die getätigten Transaktionen überprüfen. Dort kann auch der echte Paypal-Support kontaktiert werden. Die Polizei rät außerdem, das Konto mit einer Zwei-Faktor-Authentifizierung zu schützen. Wer auf die Masche hereingefallen ist, und Daten von sich preisgegeben hat, sollte den Betrug umgehend bei Paypal melden und anschließend Anzeige bei Ihrer örtlichen Polizei erstatten.

Quelle: https://www.pcwelt.de/article/1991105/betrugsmasche-paypal.html

15) aktualisiert – Polizei warnt vor iCloud-Betrug per Mail

Eine Masche von Cyberbetrügern zielt recht hoch – so erkennen Sie den Phishing-Versuch und so schützen Sie sich.

Aktualisierung vom 13. Juli 2023:

Aktuell berichtet die Polizei Niedersachsen über gefälschte iCloud-Mails mit betrügerischer Absicht, über die bereits Mitte Mai berichteten. Dabei handelt es sich um eine bekannte Masche: Die Nutzerin oder der Nutzer wird regelrecht erpresst, sich angeblich kostenlosen Speicherplatz in Apples iCloud zu holen, ansonsten würden die Daten im iCloud-Drive gelöscht.

Die aktuellen Phishing-Versuche stammen offenbar aus dem gleichen oder vergleichbaren Netzwerk wie die im Mai, denn sogar recht offensichtliche Fehler bei der Rechtschreibung (das Verb „erhalten“ großgeschrieben) wurden beibehalten. Die Polizei berichtet über mehrere Abwandlungen der gleichen Mail. Nach dem Klick auf das vermeintlich kostenlose iCloud-Angebot werden die Kunden und Kundinnen aufgefordert, sich mit der aktuellen Kreditkarte zu „verifizieren“, wovon natürlich strikt abzuraten ist.

Um Apple dabei zu helfen, die Quelle solcher Phishing-Mails besser zu identifizieren und den Empfang durch den eigenen Spamfilter zu hindern, schicken Sie von Ihnen erhaltene Betrugs-Mails als Anhang an die Adresse reportphishing@apple.com. Falls Sie Ihre Apple-ID-Daten auf einer Phishing-Seite eingegeben haben, rufen Sie in Ihrem Browser appleid.apple.com auf und ändern Sie dort das Passwort Ihrer Apple-ID.

Ursprünglicher Bericht vom 16. Mai 2023:

Betrüger versuchen derzeit im deutschsprachigen Internet mit einer vorgeblich von Apple stammenden Mail an Ihre Identität und die Kreditkarte zu kommen. Der Betrugsversuch lässt sich aber relativ leicht erkennen, obwohl die Kriminellen eine Falle stellen, die ein Manko Apples ausnutzt.

Denn den Text hat man so oder so ähnlich schon gelesen: “Lieber Kunde, Dein iCloud-Speicher ist voll”. Apple gibt für jede Apple-ID, die für Nutzung von iPhone, iPad und Mac praktisch unerlässlich ist, nur ein Gratisvolumen von 5 GB, seit dem Start des Dienstes im Spätsommer 2011. Wer mehr will, muss zahlen, und wer nicht nur Gelegenheitsnutzer ist, wird bald mehr brauchen, allein um Fotos in der iCloud zu sichern.

Klingt erst nach Apple – dann aber gar nicht mehr

Der Ton kommt auch bekannt vor, Apple duzt seine Kund:innen gerne. Aber – hier sollte man stutzig werden – spricht Apple die Kundschaft in solchen Fällen auch persönlich an, niemals

als “Lieber Kunde” – eher noch als “Liebe(r) Kund:in”, aber das ist ein anderes Thema. Zudem wurde man im Betreff noch gesiezt: “Ihr iCloud-Speicher ist voll” – es folgte dann noch eine siebenstellige Nummer.

Weiter im Text klingt das gar nicht mehr nach Apple: “Aber als Teil deines Treueprogramms kannst du jetzt zusätzliche 50 GB kostenlos erhalten, bevor deine Daten auf dem iCloud Drive gelöscht werden”. Welches Treueprogramm? Kostenlose 50 GB bei Apple, die es sonst für 0,99 Euro pro Monat verkauft? Die Erpressung, das iCloud Drive zu löschen, traut man Apple nur dann zu, wenn man eine ganz schlechte Meinung von Cupertino hat.

iCloud-Speicher bei Apple kaufen? Ja, aber bitte sicher!

Richtig ist: Reduziert man sein iCloud-Speichervolumen, etwa von 200 GB auf 50 GB, bekommt man eine Warnung, falls nicht alle Daten auf die reduzierte Größe passen. Apple nennt dann aber eine Frist und zeigt Lösungen auf. Hier geht es aber um den umgekehrten Weg: Kauft man bei Apple wirklich 50 GB oder mehr, weil die 5 GB nicht ausreichen, bleibt auf dem iCloud Drive alles erhalten. Ist der Speicher voll, schreiben Systeme und Anwendungen einfach keine neuen Daten mehr auf den Speicher.

Das Kleingedruckte unter dem im schicken Apple-Blau gehaltenen Button “50 GB Erhalten” sollte noch mehr stutzig machen. Wäre ja beinahe komisch, wenn es nicht so ernst wäre, denn die Fälschung ist auf den ersten Blick nicht schlecht: “Nach der Anmeldung musst du deine Kreditkartendaten zur Validierung deiner Apple-ID eingeben. Wir werden keinen Betrag einziehen”.

Es gibt noch ein weiteres, klares Indiz, warum es sich um eine Fälschung handelt: Die Absenderadresse, in dem uns berichteten Fall **reminder-0ti@gilt.com**. Hier haben sich die Betrüger die geringste Mühe gemacht, ihre Absicht zu verschleiern.

Der Leser, der uns von der Mail berichtete, musste sich zudem mit einem Screenshot behelfen, um uns zu informieren. Denn den Versuch der Weiterleitung per E-Mail unterband offenbar sein Provider GMX – der aber die Mail zuvor korrekt zugestellt hatte.

Weder der Leser noch wir haben klugerweise auf den Button “50 GB Erhalten” geklickt, laut Verbraucherzentrale wird man dann zu einer gefälschten Website geschickt, mit einem Eingabefenster für die vertraulichen Daten.

So erkennen Sie Phishing-Mails – die wichtigsten Erkenntnisse

1. **Seien Sie skeptisch:** Gratis gibt es von Apple nichts
2. **Prüfen Sie die Anrede:** Werden Sie durchgehend geduzt und namentlich angesprochen?
3. **Prüfen Sie die Rechtschreibung:** Korrekt sollte es “50 GB erhalten” heißen, der Großbuchstabe bei einem Verb ist selbst in einer Überschrift falsch. Sonst ist die Rechtschreibung in dieser konkreten Phishing-Mail fast schon unauffällig, “Du” würde Apple jedoch konsequent groß schreiben. Viele Phisher erkennt man aber an derartigen Fehlern.
4. **Prüfen Sie Ihre Apple-ID:** Vielleicht haben Sie ja schon ein Abo bei Apple gelöst, ist der Speicher wirklich so voll? Sehen Sie nach in den Einstellungen Ihrer Apple-ID, finden Sie auf iPhone, iPad und Mac jeweils ganz oben in den Einstellungen.
5. **Prüfen Sie die Absendemail:** Stammt die wirklich von Apple? Das ist jedoch kein zu 100 Prozent sicheres Indiz, raffinierte Betrüger können den Absender fälschen (Spoofing)
6. **Klicken Sie nie auf einen Link in einer verdächtigen Mail!** Und falls Sie es doch tun: Auf welcher URL landen Sie? Das Ziel des Links finden Sie auch heraus, ohne darauf zu klicken, fahren Sie einfach mit der Maus über den Button oder halten Sie auf iPhone

oder iPad den Finger auf dem Link, bis Sie ein Popup für verschiedene Optionen bekommen – darin ist auch der Link zu sehen.

Gegen Phishing helfen Maßnahmen wie diese am Besten, nicht jede Sicherheitssoftware filtert Betrugsversuche zuverlässig aus. Die besten Sicherheitsprogramme gegen Bedrohungen anderer Art für den Mac testen wir regelmäßig für Sie.

Quelle: https://www.macwelt.de/article/1918169/polizei-warnt-betrug-icloud-mail.html?utm_date=20230727141844&utm_campaign=Macwelt%20Daily&utm_content=Title%3A%20Polizei%20warnt%20vor%20iCloud-Betrug%20per%20Mail&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

16) Apps – Diese iOS-App ist in den Top 10 der Charts – und eine fiese Falle

Hüte dich vor dieser iOS-App. Sie scheint zwar unfassbar beliebt, doch nur, weil sie sich für etwas ausgibt, das sie nicht ist.

Im App Store für iPhones befindet sich eine **iOS-App** in den Top 10, die dort eigentlich gar nichts zu suchen hat. Anstatt das zu bieten, was sie suggeriert, handelt es sich um einen potentiell gefährlichen Fake.

iOS-App imitiert neue Twitter-Alternative

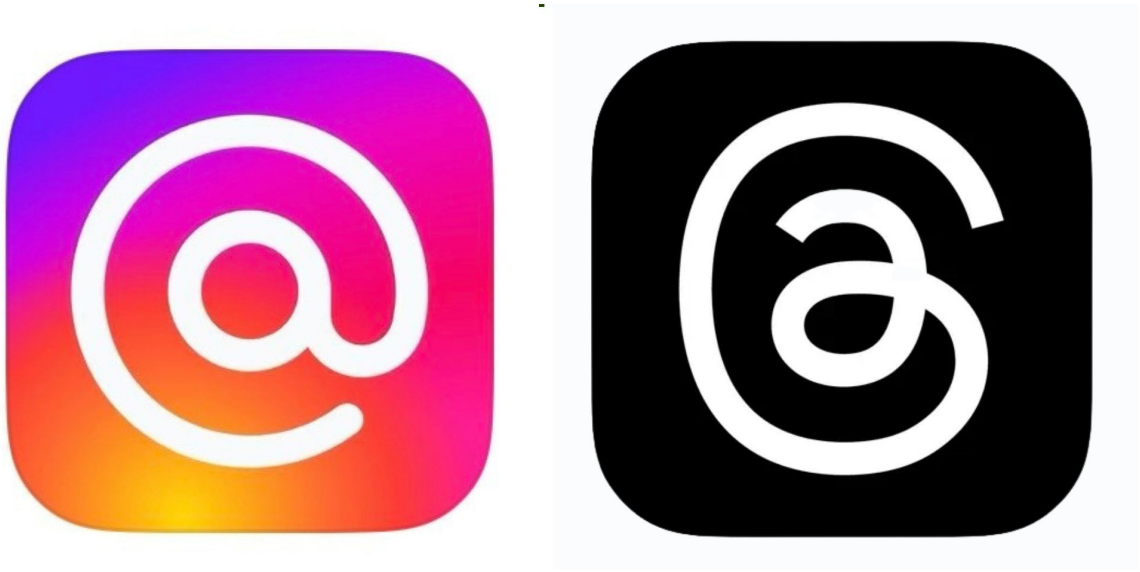
Und zwar handelt es sich um eine Nachahmung der neuen Twitter-Alternative Threads. Die App, die aus dem Hause Meta und damit aus den selben vier Wänden wie Instagram und WhatsApp stammt, ist erst vor kurzem gelauncht. Allerdings ist sie, Stand jetzt, weder als Android- noch als iOS-App in Europa verfügbar.

Die Anwendung „Threads for Insta“ ist also lediglich ein Fake des neuen sozialen Netzwerks aus dem Zuckerberg-Unternehmen. Nichtsdestotrotz befindet sich die Anwendung aktuell auf Platz 6 der App Store-Charts.

So erkennst du den Fake sofort

Damit du nicht auf den Schwindel hineinfällst, solltest du Herausgeber und das Logo der iOS-App beachten:

1. Bei dem Fake „Threads for Insta“ entdeckst du den Herausgeber „SocialKit LTD“. Tippst du auf diesen Namen findest du nur Fotobearbeitungsprogramme mit wenig bis gar keinen Bewertungen. Nach einer iOS-App aus dem Meta-Universum sieht das also nicht aus.
2. Das Logo lässt den Schwindel ebenfalls auffliegen. Anstelle des offiziellen, leicht verschnörkelten und weißen @-Zeichens auf schwarzen Grund sieht man hier ein herkömmliches @ mit den typischen Instagram-Farben im Hintergrund:



Achtung Fake – links siehst du die Nachahmer-App „Threads for Insta“. Rechts hingegen ist die richtige iOS-App zu sehen.
Quelle: appfollow.io

Quelle: https://www.futurezone.de/digital-life/apps/article471588/diese-ios-app-ist-in-den-top-10-der-charts-und-eine-fiese-falle.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

17) Betrugsmasche per Knopfdruck bringt Frau um fast 24.000 Euro

Ein falscher Klick, und schon räumen Kriminelle das Konto leer. Wie leicht man Opfer von Internetbetrug werden kann, erfuhr nun eine Frau im Norden.

Eine 46-jährige Hohenlockstedterin aus dem Kreis Steinburg ist Opfer einer raffinierten Betrugsmasche geworden. Wie die Polizei am Donnerstag mitteilt, hat sie dadurch fast 24.000 Euro verloren.

Am Dienstag hatte die Frau von ihrer Bank eine SMS-Nachricht erhalten, in der sie aufgefordert wurde, ihre "Best Sign App" der Postbank zu aktualisieren. Um dies zu tun, sollte sie einen Button klicken und ihre Bankverbindung eingeben.

Doch dabei handelte es sich um eine gefälschte Nachricht von Kriminellen: Die Postbank fordert ihre Kunden niemals auf diese Weise zur Eingabe ihrer Bankverbindung auf.

Am nächsten Tag musste die Frau feststellen, dass fast 24.000 Euro von ihrem Konto abgebucht worden waren. Ob der Schaden durch Stornierungen noch begrenzt werden kann, bleibt laut Polizei unklar.

Quelle: https://www.t-online.de/region/hamburg/id_100214900/online-banking-bei-postbank-ein-knopfdruck-bringt-frau-um-24000-euro.html

18) Smartphones und Tablets – Hackerangriffe im Urlaub: So können Sie sich schützen

Mal abschalten und an nichts denken: Dass Urlauber oft sorglos unterwegs sind, machen sich Betrüger zunutze. So schützen Sie Ihre Technik vor Angreifern.

Für viele ist die Urlaubszeit die schönste Zeit im Jahr. Doch nicht nur Erholungssuchende freuen sich auf die Reisezeit, auch für Kriminelle sind die Sommermonate lukrativ. Warum? Weil fast jeder Urlauber ein wertvolles Smartphone, Tablet oder Notebook bei sich hat. Und diese Geräte bieten Betrügern eine Möglichkeit, an wertvolle Daten von Touristen zu kommen.

Wie die Kriminellen das machen, teilt das Sicherheitsunternehmen Eset mit: "Vermeintliche Reiseschnäppchen, gefälschte Online-Reiseportale, angezapfte WLAN-Hotspots oder abgeräumte Bankkonten: Hacker haben verschiedene Tricks in der Hinterhand, um die Unbedarftheit vieler Touristen für ihre Zwecke auszunutzen."

Das Betrugsmeldezentrum "Action Fraud" schätze den Schaden durch Urlaubsschwindel im Jahr 2022 allein für Großbritannien auf rund 17,5 Millionen Euro, berichtet Eset.

Offene WLAN-Hotspots sind eine Gefahrenquelle

Auch F-Secure, ein Unternehmen, das sich auf IT-Sicherheit spezialisiert hat, macht auf die Gefahren von Angriffen in Urlaubsregionen aufmerksam. Vor allem das Verbinden mit offenen WLAN-Hotspots sei gefährlich, weil Nutzer dabei Daten wie Cookies ungeschützt übertragen.

"Cookies sind die Generalschlüssel der digitalen Welt. Wer in einem Urlaubshotel ungeschützt ein Netzwerk nutzt, lässt diesen Schlüssel quasi am Hotelbüfett offen herumliegen", warnt F-Secure.

Um nicht auf Betrugsmaschen während des Urlaubs reinzufallen, sollten Reisende sich bereits vor der Ferienzeit Gedanken zur Absicherung ihrer Geräte machen und einige simple Tipps befolgen.

Was Sie vor dem Urlaub beachten sollten:

"Buchen Sie Ferienobjekte nur auf seriösen Portalen, die einen Schutz vor gefälschten Angeboten bieten", rät Eset. Zudem sollten die Bewertungen anderer Urlauber zu den Unterkünften genau geprüft werden.

Denn immer mehr Betrüger platzieren ihre eigenen gefälschten Einträge auf diesen seriösen Seiten. Die Ferienobjekte existierten entweder nicht, seien gar nicht zu mieten oder von anderen Angeboten kopiert.

Was Sie während des Urlaubs beachten sollten:

Sie sollten sich nicht an öffentlichen Plätzen, Flughäfen oder in Cafés über das kostenlose WLAN in ihr Bankkonto oder andere wertvolle Konten einloggen, rät Eset.

Bei dem WiFi-Dienst könne es sich "um einen gefälschten Hotspot handeln, der von Cyberkriminellen eingerichtet wurde, um den Datenverkehr abzufangen oder Passwörter und persönliche Informationen zu stehlen".

So schützen Sie Ihre Geräte zusätzlich vor fremdem Zugriff:

- Installieren Sie eine Internet Security, um sich vor Schadsoftware wie Trojanern und Ransomware zu schützen.

- Machen Sie vor dem Urlaub Back-ups Ihrer Daten.
- Stellen Sie sicher, dass Betriebssystem, Sicherheitssoftware und Apps auf dem aktuellen Stand sind.
- Machen Sie auch Updates auf Reisen, um zwischenzeitlich entstandene Schwachstellen schließen zu können.
- Lassen Sie Ihre Geräte nie aus den Augen. Wo viele Touristen sind, sind auch Diebe nicht weit, die nur auf eine Gelegenheit warten.
- Schützen Sie Ihre Geräte mit einem Passwort oder Fingerabdruck und verwenden Sie eine Zwei-Faktor-Authentifizierung für genutzte Online-Dienste.
- Im Urlaub sollten Sie auf digitale Einkaufsbummel oder Online-Banking möglichst verzichten. Legen Sie bei Ihrer Bank besser ein Limit für tägliche Geldbewegungen fest. Behalten Sie zudem nach Ihrer Reise Kredit- und Kartenabrechnungen im Auge.
- Schalten Sie die Bluetooth- und WLAN-Funktionen aus, wenn Sie sie nicht brauchen.
- Teilen Sie während der Ferien keine Urlaubsbilder in sozialen Medien wie Facebook und Instagram. Reale und digitale Diebe warten nur auf solche "Einladungen".

VPN als sicherste Lösung

Wie F-Secure schreibt, sei ein VPN-Zugang eine Lösung, um sich vor Angreifern zu schützen. "Eine VPN-Verbindung weist der eigenen Internetverbindung einen sicheren Weg wie durch einen Tunnel. Das eigene Signal wird über verschlüsselte Server weitergeleitet, so dass die Daten für die Betrüger nicht erreichbar sind", heißt es.

Was VPN ist und wie Sie einen Anbieter dieser Sicherheitslösung aussuchen, haben wir hier für Sie zusammengefasst. Mit dieser Lösung können Sie Ihren Urlaub genießen und brauchen sich um die Sicherheit Ihrer Technik weniger Sorgen zu machen.

Quelle: https://www.t-online.de/digital/sicherheit/id_100201528/hacker-angriffe-im-urlaub-so-koennen-sie-sich-schuetzen.html

Anwenderinformationen:

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

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

Nicht nur am PC, auch auf Android-Smartphones machen sich Schadprogramme (so genannte Malware) breit. Sie zeigt unerwünschte Werbung an, errechnet virtuelle Münzen in Währungen wie Monero oder überträgt vertrauliche Daten an Kriminelle. Wird Ihr Handy ständig heiß (auch wenn Sie es gar nicht benutzen), leert sich der Akku rasch oder steigt der Datenverbrauch rapide an, dann ist Ihr Gerät mit hoher Wahrscheinlichkeit infiziert. Grundsätzlich gilt die Empfehlung, dass Sie ein von Malware infiziertes Gerät auf die Werkseinstellungen zurücksetzen und ganz neu einrichten sollten.

Muss ich meine Passwörter ändern?

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

Alternativ können Sie die Malware mit der folgenden Anleitung gezielt **deinstallieren**. Der Vorteil: alle anderen Apps, Daten und Einstellungen bleiben erhalten. Gerade bei „einfacher“ Malware, die zum Beispiel nur Werbung einblendet, kann diese Methode ratsam sein. Perfekte Sicherheit bietet sie aber ausdrücklich nicht. Und das Ändern der Passwörter ist in jedem Fall sinnvoll. Schließlich könnte die Malware sensible Daten gestohlen haben.

Schritt 1: Im abgesicherten Modus neu starten

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

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

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

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

Schritt 2: Werbung gezielt ausblenden

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

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

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

Schritt 3: App deinstallieren

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

Manche Apps wehren sich allerdings gegen die Deinstallation. Sie fragen schon bei der

Installation nach Administratorrechten (auch „Geräte-Administrator“ oder „Geräte-Verwaltung“ genannt). Gerade wenn sich Malware als Virenscanner oder Diebstahlschutz tarnt scheint das auch nachvollziehbar, wird bei der Deinstallation aber zum Problem.

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

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

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

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

2) WhatsApp: Neue Funktion lässt Sprachnachrichten alt aussehen

Sprachnachrichten sind jetzt offiziell von gestern: WhatsApp erlaubt nun auch kurze Videobotschaften, die direkt in der App erstellt werden. Sie dürfen bis zu 60 Sekunden lang sein und erscheinen beim Empfänger in kreisrunder Form. Die Funktion wird gerade in der Android-Beta verteilt, bei iOS müssen sich Nutzer noch gedulden.

WhatsApp schaltet Videonachrichten frei

Schon etwas länger ist bekannt, dass die Entwickler von WhatsApp an **einer neuen Funktion für Videobotschaften arbeiten**. Erstmals wurde sie Mitte Juni entdeckt. Jetzt hat WhatsApp damit begonnen, die Betaversion der Android-App flächendeckend mit den neuen Videonachrichten auszustatten.

Die Videobotschaften selbst sind schnell erklärt: Es handelt sich im Grunde um eine **Video-Variante der allseits bekannten Sprachnachrichten**. Sie können direkt im Messenger aufgenommen und anschließend verschickt werden. Eine wichtige Einschränkung betrifft die Länge, denn Videos dürfen nur maximal 60 Sekunden lang sein.

Beim Empfänger werden Videonachrichten nicht wie sonst bei Videos üblich in einem Rechteck dargestellt, sondern als Kreis angezeigt. Beim Erstellen der Videos sollten Nutzer entsprechend darauf achten, **sich möglichst mittig zu filmen**. Wie lang die Videos sind, lässt sich an einem Fortschrittsbalken erkennen, der um das Video selbst platziert ist.

Um eine Videobotschaft aufzunehmen, wird das Mikrofon-Symbol im Chat etwas länger gedrückt. Wie bei Sprachnachrichten können Nutzer das Video ansehen, bevor sie es versenden.

WhatsApp: Wann erscheinen Videonachrichten für alle?

Bislang ist die Funktion **nur in der Betaversion der Android-App aufgetaucht** (Quelle: Caschys Blog). Lange dürfte es jetzt nicht mehr dauern, bis sie auch in der finalen Variante zu finden sein wird. Unter iOS könnte hingegen noch etwas Zeit vergehen, bis sich auch hier Videobotschaften erstellen und versenden lassen.

Tipps und Tricks zu Sprachnachrichten seht ihr im Video unter dem u.g. Link

Quelle: https://www.giga.de/news/whatsapp-neue-funktion-laesst-sprachnachrichten-alt-aussehen/

3) Sowohl Navi als auch Dashcam: Geniale Autofahrer-App runderneuert

Die völlig kostenlos angebotene Navi-App "Magic Earth" ist ein echter Geheimtipp. Neben der Routenführung übernimmt sie auf Wunsch auch gleich die Funktion einer Dashcam. iOS-Nutzer können die App jetzt in einer runderneuerten Fassung herunterladen.

Fahrassistenzsysteme können nicht nur direkt im Auto stecken. Es gibt auch Navigations-Apps, die solche Dienste anbieten. Dazu gehört etwa die Anwendung "Magic Earth", die kostenlos für iOS und Android zu haben ist.
Die Assistenzfunktionen von "Magic Earth" können aktiviert werden, wenn sich das Smartphone im Querformat in einer Halterung befindet und die Kamera freie Sicht auf die Straße hat. So warnt die App etwa, wenn man die Spur verlässt, der Abstand zum voraus fahrenden Auto zu gering wird oder Fußgänger die Straße queren. Und es gibt eine Dashcam-Funktion zum Aufzeichnen der Fahrt, damit man bei Unfällen einen Videobeweis hat.
Mit der jetzt veröffentlichten **Version 7.8.0** lässt sich "Magic Earth für iOS" in einem runderneuerten Release herunterladen. Die Entwickler betonen im Change-log, die App von Grund auf neu geschrieben zu haben.

3D-, Sat- und Live-Ansicht

Für die Darstellung und Routenplanung mit Verkehrsinformationen in Echtzeit nutzt die App ansonsten Kartenmaterial, das auf dem Open-Street-Map-Projekt basiert. Es sind aber auch 3D- und Satellitenansichten verfügbar. Bei kniffligen Spurwechseln oder Abbiege-Situationen kann die App auch das Live-Bild der Smartphone-Kamera aufs Display bringen und mit Pfeilen verdeutlichen, wo es lang geht.
Mithilfe von Offline-Karten ist man in 233 Ländern und Regionen im Zweifel auch unabhängig vom mobilen Internet. Die Turn-by-turn-Navigation ist nicht nur für Autos verfügbar, sie kann auch auf Radfahren, Fußgänger und Nahverkehr umgestellt werden.

Unterstützung für Carplay

"Magic Earth" unterstützt auch Apple Carplay, allerdings noch kein Android Auto. Wer die App im Carplay-Modus nutzt, sieht die Navi-Karte auf dem Display des Auto-Entertainmentsystems.
Das iPhone in der Windschutzscheibenhalterung dient dann als "Augen und Ohren" für die Assistenz-Features von "Magic Earth" und zeigt auf seinem Display nur Warnungen an, wenn man etwa die Spur verlässt oder ein Fußgänger auf die Straße läuft.

Kein Tracking, keine Werbung

Ein Vorteil für alle, die nicht gerne ihre Daten preisgeben: Magic Earth verspricht, trackingfrei zu sein, also die Nutzung nicht zu verfolgen, und auch keine persönlichen Daten von Nutzerinnen und Nutzern zu speichern. Werbung gibt es in der App auch nicht.
Was es dagegen gibt, ist eine Fülle potenziell interessanter Orte (POI) samt zugehöriger Wikipedia-Einträge für weitergehende Informationen. Auch das Wetter fehlt nicht: "Magic Earth" zeigt die Temperatur an einem Ort an und wie das Wetter dort in den nächsten 14 Tagen werden soll. Und es lassen sich nicht zuletzt Parkplätze, Tankstellen und Ladesäulen oder Restaurants entlang der Strecke auswählen.

Quelle: https://www.chip.de/news/Sowohl-Navi-als-auch-Dashcam-Geniale-Autofahrer-App-runderneuert_184642750.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=25-07-2023%2B17%253A00%253A07&utm_content=nl_chipmob&utm_term=

4) 10 unbekannte Funktionen der Apple Watch, die Sie kennen müssen

Die Apple Watch ist so vielseitig, dass einige Funktionen selbst eingefleischten Fans unbekannt sind. Hier ist eine Liste mit zehn etwas versteckten Features.

Als Apple 2014 seine allererste Smartwatch vorstellte, war sich die Welt nicht ganz sicher, wofür sie gut sein sollte… und Apple auch nicht. In jenen frühen Tagen sprach das Unternehmen neben den bis heute beliebten Fitness-Funktionen enthusiastisch über Digital Touch, das selbst wir vergessen haben. Es dauerte einige Zeit, bis die Nutzer und Drittentwickler Apple ihre Wünsche an eine Smartwatch mitteilten und das Unternehmen diese aufgriff.

Heute ist die Apple Watch ein ausgereiftes und vielseitiges Produkt. Sie ist sogar so vielseitig, dass Sie vielleicht einige ihrer nützlichsten Funktionen gar nicht kennen. Hier eine kurze Liste mit zehn davon.

Bessere iPhone-Fotos machen

Schön um die Ecke gedacht: Es gab schon immer Situationen, in denen es schwierig oder unmöglich ist, eine Kamera auszulösen, weil sie außer Reichweite oder außer Sichtweite der Person sein muss, die das Foto macht: etwa, wenn Sie versuchen, die Anschlüsse an der Rückseite Ihres Macs zu fotografieren oder wenn Sie ein Gruppenfoto aufstellen, bei dem alle dabei sein wollen. Früher waren Timer die Hauptlösung, aber das führte oft zu enormer Hektik, die Kamera richtig zu platzieren und rechtzeitig zurück zu sein, bevor die Zeit abgelaufen ist. Abhilfe schafft die Apple Watch.

Wenn Sie die Kamera-App auf Ihrer Uhr starten, wird gleichzeitig die entsprechende App auf dem gekoppelten iPhone geöffnet. Was auch immer die Kamera des iPhones abbildet, können Sie auf dem Uhr-Display sehen. Sie können zwischen der vorderen und hinteren Kamera umschalten, indem Sie die Optionstaste unten rechts drücken. Bei einem zufriedenstellenden Bild drücken Sie den Drei-Sekunden-Timer, schauen nach oben, lächeln und genießen Ihr perfektes Foto.

Andere Apple-Geräte freischalten

Eine mit dem Passwort gesicherte Apple Watch bleibt entsperrt, solange Sie sie am Handgelenk tragen. Sie kann also als praktischer digitaler Schlüssel fungieren, mit dem Sie Ihren Mac und Ihr iPhone allein dadurch entsperren können, dass Sie sich in der Nähe befinden.

Öffnen Sie auf dem iPhone die App *„Einstellungen“* und gehen Sie zu „*Face ID & Code“* (bzw. *„Touch ID & Code“* auf älteren Geräten), scrollen Sie dann nach unten und tippen Sie auf den Schalter unter „*Mit Apple Watch entsperren*“. Auf dem Mac öffnen Sie die Systemeinstellungen, gehen zu „*Touch ID & Passwort*“ und klicken auf das Kästchen neben Ihrer Apple Watch.

Spiele spielen

So klein der Bildschirm der Apple Watch auch sein mag, bietet er dennoch genug Platz für ein paar lustige Spiele. Wir empfehlen Deep Golf und Lifeline, die beide perfekt für dieses Format geeignet sind, weitere hervorragende Vorschläge finden Sie hier.

Sprechen Sie mit Chat-GPT

Wahrscheinlich haben Sie Ihre eigene Meinung über die Ethik von KI, aber es ist schwer zu

leugnen, dass es Spaß macht, mit Chat-GPT zu spielen. Dank der Petey-App können Sie diese Gespräche jetzt auch auf der Apple Watch führen. Tippen Sie auf die Schaltfläche „Frag mich alles“ und geben Sie dann eine Frage ein (oder noch besser, verwenden Sie die Diktat-Schaltfläche und schonen Sie Ihren Finger), und schon bald werden Sie hören, was unser zukünftiger KI-Overlord über das Thema denkt. Es gibt sogar eine Komplikation, bei der Petey nie weiter als einen Fingertipp entfernt ist.

Navigation mit Handgesten steuern

Die Standardmethode zur Steuerung der Apple Watch besteht darin, das Gerät an einem Handgelenk zu tragen und dann mit der anderen Hand auf den Bildschirm zu tippen und die Tasten und Drehknöpfe zu drücken und zu drehen. Aber es gibt Situationen, in denen man die Uhr mit der gleichen Hand steuern muss, die sie trägt. Und das ist dank Assistive Touch möglich, einer der praktischen Bedienungshilfefunktionen von Apple.

Öffnen Sie die Watch-App auf dem gekoppelten iPhone. (Alternativ können Sie die Funktion auch in der App „Einstellungen“ der Apple Watch einrichten, aber das ist auf dem kleinen Bildschirm etwas umständlich.) Wählen Sie im Reiter „Meine Uhr“ die Option „Bedienungshilfen“ und scrollen Sie nach unten, bis Sie „*Assistive Touch*“ sehen. Tippen Sie darauf und dann auf den Schalter oben im nächsten Bildschirm, um die Funktion zu aktivieren.

Das einmalige Zusammentippen mit zwei Fingern blättert im Menü nach vorn, zweimaliges – zurück. Das Ganze ist etwas gewöhnungsbedürftig, aber Übung macht den Meister. Sie können zudem jeder Geste eine andere Aktion zuweisen.

Die Zeit ablesen, ohne hinzusehen

Wenn Sie aus irgendeinem Grund nicht auf die Apple Watch schauen können, aber trotzdem die Zeit wissen möchten, ist die Zeitansage eine weniger bekannte Funktion für Sie. Um sie einzurichten, öffnen Sie auf der Apple Watch die App „Einstellungen“ suchen Sie „Uhr“, scrollen zu „Zeitansage“ und tippen dann auf „Ein“, um sie zu aktivieren. (Dies kann auch in der Watch-App auf einem gekoppelten iPhone erfolgen; auch hier gehen Sie zu „Uhr“ und tippen auf „Zeitansage“). Jetzt müssen Sie nur noch zwei Finger für etwa eine Sekunde auf das Zifferblatt der Uhr halten, und sie sagt Ihnen die Zeit laut vor.

Wenn Sie hingegen die Uhrzeit lautlos wissen möchten, ohne auf das Display zu schauen, sollten Sie „Taptische Zeit“ in Betracht ziehen. (Sie können diese Funktion in der Watch-App unter „*Uhr*“ > „*Taptische Zeit*“ aktivieren oder auf ähnliche Weise in der „Einstellungen“-App der Apple Watch). Es gibt verschiedene Optionen, doch wir finden das Ziffernformat am einfachsten: Eine lange Vibration, gefolgt von vier kurzen Vibrationen, gefolgt von drei langen Vibrationen, gefolgt von sechs kurzen Vibrationen zeigt so die Zeit 14:36 an.

Schnelles Beantworten von Nachrichten

Die Apple Watch scheint wahrscheinlich nicht das optimale Gerät zum Schreiben von Nachrichten zu sein, doch watchOS wurde so entwickelt, um dabei zu helfen. Tippen Sie auf die Benachrichtigung einer eingehenden Nachricht (oder öffnen Sie die Nachrichten-App auf Ihrer Apple Watch und tippen Sie dort auf eine Nachricht) und Sie sehen die Option zum Antworten. Das ist einfacher, als es klingt.

Am einfachsten ist es, eine der vorgefertigten Antworten auszuwählen, z. B. „Ja“, „Nein“ und „Kann ich dich später anrufen?“ Ein Fingertipp, und schon ist die vorgefertigte Antwort auf dem Weg zum Empfänger: ganz einfach. Und wenn Ihnen diese Antworten zu begrenzt erscheinen, können Sie Ihre eigenen einpflegen, indem Sie die Watch-App auf Ihrem gekoppelten iPhone öffnen und zu „Nachrichten“ > „Standardantworten“ gehen.

So hält der Akku viel länger

Kaum jemand scheint zu wissen, dass die Apple Watch jetzt einen Energiesparmodus hat – vielleicht, weil es bereits einen Stromsparmodus gab, der viel drastischer war und die Uhr im Grunde unbrauchbar machte. Der Energiesparmodus, der mit watchOS 9 im Jahr 2022 eingeführt wurde, ist jedoch viel näher an der entsprechenden Funktion des iPhones und reduziert einfach Funktionen und Einstellungen, um die Akkulaufzeit zu verlängern.

Um den Energiesparmodus zu aktivieren, öffnen Sie das Kontrollzentrum, indem Sie vom Ziffernblatt nach oben wischen und tippen Sie auf den Akkuprozentsatz. Direkt unter der Zahl für die verbleibende Akkulaufzeit sehen Sie einen Schalter mit der Aufschrift „Energiesparmodus“. (Beachten Sie, dass das Kontrollzentrum in watchOS 10 stattdessen durch Drücken der Seitentaste aufgerufen wird.)

Bewahren Sie Ihre Privatsphäre

Der Always-On-Bildschirm der Series 5 und neuer hat viele gute Eigenschaften, doch dadurch werden persönliche Daten für andere sichtbar. Glücklicherweise können Sie die Einstellungen so anpassen, dass sensible Komplikationen und Benachrichtigungen nur angezeigt werden, wenn Sie Ihr Handgelenk hochhalten.

Beginnen wir mit den Komplikationen, die persönliche Daten wie Kalendertermine oder Gesundheitsinformationen anzeigen können. Öffnen Sie die Watch-App auf Ihrem gekoppelten iPhone. Gehen Sie im Reiter „Meine Uhr“ zu „Anzeige & Helligkeit“ > „Immer eingeschaltet“ > „Komplikationsdaten anzeigen“. Hier können Sie auswählen, welche Komplikationen ihre Daten anzeigen dürfen, wenn der Always-On-Bildschirm im abgedunkelten Modus ist.

Ähnlich können Sie unter „Anzeige & Helligkeit > Immer eingeschaltet > Mitteilungen einblenden“ die Benachrichtigungen feintunen, die im gedimmten Modus angezeigt werden und deren Informationen nur dann zu sehen sind, wenn Sie Ihr Handgelenk anheben.

Diskrete Wegbeschreibung

Vor dem Start öffnen Sie Karten auf Ihrem iPhone und wählen Sie ein Ziel und die Art der gewünschten Wegbeschreibung aus. Starten Sie die Route und stellen Sie sicher, dass Sie die akustischen Warnsignale ausschalten, indem Sie auf die Taste zum Stummschalten bzw. Aufheben der Stummschaltung auf der rechten Seite tippen. Stecken Sie das iPhone in eine Tasche.

Während Sie gehen, weist Sie die Apple Watch mit drei Summtönen darauf hin, links abzubiegen und mit einer schnellen und gleichmäßigen Folge von 10 bis 12 haptischen Berührungen nach rechts. (Sie brauchen sie nicht zu zählen, der Rhythmus verrät es.) Wenn Sie Ihr Ziel erreichen, spüren Sie eine lange Vibration.

Quelle: https://www.macwelt.de/article/1988809/unbekannte-apple-watch-funktionen.html?utm_date=20230727112406&utm_campaign=Macwelt%20Daily&utm_content=Title%3A%2010%20unbekannte%20Funktionen%20der%20Apple%20Watch%2C%20die%20Sie%20kennen%20m%C3%BCssen&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Smartphone-Tipps – Die schlimmsten Handy-Sünden: Das sollten Sie vermeiden

Viele „liebe Gewohnheiten“ sind den teuren Mobilgeräten wenig zuträglich. Um zu verhindern, dass Ihr wertvolles Smartphones durch eigenes Verschulden beschädigt wird, zählen wir hier die häufigsten Handy-Sünden auf.

Aus unserem Alltag sind Smartphones längst nicht mehr wegzudenken; es gibt kaum Gelegenheiten, bei denen der digitale Begleiter fehlt. Doch wie das so ist mit Alltagsdingen: Man wird im Umgang mit ihnen oft unaufmerksam.

Sünde 1: Extreme Temperaturen

Auch wenn der Winter sich gerade verabschiedet, sind Temperaturschwankungen und extreme Temperaturen rund ums Jahr gefährlich für die empfindlichen Smartphones. So gibt etwa Apple als vorgesehene Betriebstemperatur für iPhones einen Temperaturbereich zwischen Null und 35 Grad Celsius an.

Bei Minusgraden arbeiten Akkus und beispielsweise Flüssigkristalle des LC-Displays nicht mehr zuverlässig. Das kann dazu führen, dass der Bildschirm nicht mehr auf Eingaben reagiert oder dass sich das Mobiltelefon ganz ausschaltet. Im Winter hilft es, das Mobiltelefon nahe am Körper zu tragen und bei extremer Kälte möglichst nicht aus der Tasche zu nehmen. Auch eine Hülle hilft, Kälteschäden zu vermeiden.

Wird es heißer als 35 Grad Celsius, laufen die elektrochemischen Prozesse im Inneren der Akkus schneller ab, was dazu führen kann, dass die Akkus schneller altern. Als Schutz vor Hitze empfiehlt es sich, das Smartphone vor direkter Sonneneinstrahlung zu schützen und möglichst in einer Tasche zu tragen.

Sünde 2: Starke Temperaturschwankungen

Was ebenfalls zu schwerwiegenden Schäden am Smartphone führen kann, sind starke Temperaturschwankungen. Wer also mit seinem Smartphone in der Hand von der Skipiste in eine mollig warme Hütte einkehrt, riskiert, dass sich im Inneren des Mobiltelefons Kondenswasser bildet.

Das kann Korrosionen an elektronischen Bauteilen begünstigen. Allerdings sind Smartphones, die über einen Staub- und Wasserschutz verfügen, weniger anfällig als Geräte ohne besondere Zertifizierungen. Um mögliche Schäden durch Kondenswasser zu verhindern, sollten Smartphones bei Kälte in einer Hülle nahe am Körper transportiert werden.

Telefonate sollten möglichst mit einem Headset geführt und auf eine längere Exposition des Geräts in der Kälte (oder Hitze und sehr hoher Luftfeuchtigkeit) nach Möglichkeit verzichtet werden.

Sünde 3: Billige Netzteile und Ladekabel von Drittanbietern

Ist das Original-Ladekabel oder das Netzteil Ihres Smartphones beschädigt oder verloren gegangen, sollten Sie keinesfalls zu einem günstigen No-Name-Ersatz greifen. Denn häufig sind diese Ladekabel und Netzteile nicht zertifiziert und fälschlicherweise mit dem obligatorischen CE-Zeichen versehen. Schlecht verarbeitete Netzteile können sehr heiß werden und unter Umständen sogar anfangen zu brennen.

Bekannt geworden sind darüber hinaus Fälle, bei denen es durch einen Kurzschluss bei minderwertig verarbeiteten elektronischen Bauteilen zu Stromschlägen und schwerwiegenden Verletzungen gekommen ist. Wer also sein Netzteil oder Ladekabel ersetzen muss, sollte Ersatzteile direkt vom Hersteller kaufen.

Sünde 4: Mit dem Handy in der Hosentasche zur Toilette gehen

Wenn das teure Smartphone locker in der Hosentasche steckt, passiert es nicht selten, dass es herausfällt. Oft geschieht das beim Umziehen oder eben beim Gang auf die Toilette. Fällt das Mobiltelefon beim Umziehen aus der Tasche, kann das Display kaputt gehen. Mit einer

sogenannten „Spider-App“ könnte man notfalls leben; im schlimmsten Fall reagiert das Gerät aber nicht mehr auf Fingereingaben. Dann muss der Bildschirm in einer Handy-Reparaturwerkstatt getauscht werden.

Nicht selten landet der mobile Kleincomputer aber auch in der Toilette. Jetzt müssen Sie schnell handeln, denn eintretendes Wasser kann großen Schaden am Handy anrichten. Das Smartphone muss schnell aus der Toilette gefischt und ausgeschaltet werden – falls es überhaupt noch läuft.

Keinesfalls sollte es mit dem Fön oder auf der Heizung getrocknet werden. Vielmehr empfiehlt sich ein schnelles, oberflächliches Trocknen mit einem Lappen. Anschließend sollten Sie das Gerät an einem trockenen Ort liegen lassen. Nach ungefähr zwei Tagen können Sie dann versuchen, das Gerät wieder einzuschalten. Funktioniert das nicht, hilft nur noch der Gang zur Handy-Reparaturwerkstatt.

Übrigens sind selbst "wassergeschützte" Smartphones nicht vor Wasserschäden nach einem längeren Bad im Pool oder der Badewanne gefeit – abhängig ist das nämlich von der jeweiligen Schutzklasse. Der Wasserschutz bezieht sich außerdem meist auf Leitungswasser - Seifenlauge, Chlor oder Salzwasser kann die Dichtungen angreifen und schließlich Wasser eindringen lassen.

Sünde 5: Smartphone ohne Hülle an den Sandstrand mitnehmen

Ebenso gefährlich wie eintretende Feuchtigkeit sind Staub und Sand für ein Smartphone. Wer also auf sein Mobiltelefon auch am Sandstrand keinesfalls verzichten möchte oder kann, sollte es zumindest in eine wasserdichte Hülle packen. Wichtig: Achten Sie dabei unbedingt auf die Zertifizierung! Ein wasserdichtes Case ist in der Regel so gebaut, dass auch Kopfhörer- und Lade-Anschlüsse sowie Tasten gesondert geschützt sind.

Alternativ zu einem festen Smartphone-Case bieten sich als Schutz für das teure Mobiltelefon auch wasserfeste Hüllen an. Sie sind leicht, und es gibt sie schon für unter 10 Euro. Damit lässt sich das Handy auch in der Badetasche so transportieren, dass weder die nasse Badehose noch das Sandspielzeug Kratzer und Wasserschäden verursachen können.

Sünde 6: Das Smartphone offen auf den Tisch legen

Das Smartphone im Restaurant offen auf den Tisch zu legen ist eine weit verbreitete (Un)Sitte und schlicht unhöflich; zeigt es dem Gegenüber doch deutlich, dass einem das Handy wichtiger ist als das ungestörte Gespräch mit ihm.

Abgesehen davon kann es aber auch ganz schnell passieren, dass mal das Cola- oder Bierglas umkippt und sich die klebrige Flüssigkeit über das Smartphone ergießt. Und während leichte Wasserschäden meist behebbar sind, verkleben zuckerhaltige Getränke die Anschlüsse und Tasten.

Zum anderen ist es auch eine Aufforderung an Langfinger, das kostbare Gerät in einem kurzen Moment der Unaufmerksamkeit des Besitzers einzustecken.

Sünde 7: Apps abschießen

Der angerichtete Schaden wird nicht sofort offensichtlich, doch zu vernachlässigen ist er nicht: Die Rede ist vom "Abschießen" von Apps, d.h. des systematischen Schließens über den Taskmanager des Betriebssystems.

Historisch gesehen hat der gelegentliche "Hausputz" tatsächlich einmal einen Sinn gehabt. Als Android und iOS noch in den Kinderschuhen steckten waren im Hintergrund laufende Apps berüchtigt dafür, dass sie Smartphones regelmäßig ausbremsten und Akkus leerten. Durch das Ritual im Taskmanager ließ sich der Effekt zumindest eingrenzen.

Diese Zeiten sind zum Glück vorbei. Heute managen beide Betriebssysteme Hintergrund-Apps nahezu störungsfrei. Sie legen Anwendungen schlafen, sobald Sie sie verlassen und wecken sie erst bei der Rückkehr wieder auf, oder wenn ein wichtiges Ereignis eintritt. Das kann zum Beispiel die Standortänderung sein, von der die Navi-App erfahren muss.

Wer Apps trotzdem noch routinemäßig abschießt, der greift in die ausgereiften Automatismen von Android und iOS ein. Das führt vor allem zu erhöhtem Leistungsbedarf, denn das Betriebssystem muss die zwangsbeendeten Apps wieder starten, statt sie nur aufzuwecken. Damit geht unnötiger Stromverbrauch einher. Der Akku ist entsprechend früher leer und verschleißt schneller. Schießen Sie Apps deshalb nur noch dann ab, wenn sie tatsächlich abgestürzt sind oder anderweitig Probleme bereiten.

Sünde 8: Scharfe Putzmittel

Handys sind fast ständig im Einsatz, drinnen, draußen und in allen möglichen Lebenssituationen. Daher ist es kein Wunder, dass sie Fingerabdrücke, Staub und Schmutz sammeln. Eine unsaubere Oberfläche ist aber nicht nur optisch unangenehm, sondern auch unhygienisch.

Andererseits sollten Sie aufpassen, dass Sie ein schmutziges Smartphone nicht "kaputt putzen". Scharfe oder scheuernde Reinigungsmittel können das Display und die Oberfläche des Smartphones beschädigen. Das ist mindestens hässlich und möglicherweise sogar schädlich für die Funktionsfähigkeit Ihres Handys.

Sehen Sie insbesondere vom Einsatz von alkohol- beziehungsweise lösungsmittelhaltigen Reinigungsmitteln ab. Propylalkohol verbietet sich also genauso wie die meisten Glasreiniger, denn beide können die Beschichtung des Displays angreifen oder dessen Verklebung lösen. Auch die schiere Menge an Reinigungsmittel kann zum Problem werden, wenn es in das Handy gerät. Zwar sind viele aktuelle Modelle zumindest einigermaßen gegen eindringende Flüssigkeit geschützt. In Putzmittel "ertränken" sollte man sie trotzdem nicht. Vermeiden Sie auch, zu viel Druck beim Reinigen auszuüben.

Für die Reinigung von Smartphones empfehlen wir ein weiches, fusselfreies Tuch, das leicht angefeuchtet ist. Alternativen sind spezielle Reinigungstücher und Sprays, die für den Gebrauch mit elektronischen Geräten entwickelt wurden.

Insgesamt sollte man also vorsichtig sein, wenn man das Smartphone reinigt, um Kratzer oder Beschädigungen zu vermeiden. Ein gelegentliches Reinigen des Geräts ist jedoch wichtig, um es hygienisch und in einem ansprechenden Zustand zu halten.

Sünde 9: Display-Poliermittel

Im Handel gibt es zahlreiche Poliermittel, die versprechen, Displaykratzer von Smartphones und anderen elektronischen Geräten zu entfernen. Meistens werden sie als die einfache und kostengünstige Alternative zum Tausch des Displays beworben.

In der Praxis taugt die Methode nach unserer Erfahrung wenig. Sie mag Kratzer reduzieren oder sogar beseitigen. Doch häufig kann man das gar nicht wirklich erkennen, weil anstelle des Kratzers ein großer blinder Fleck entsteht, der noch viel mehr stört. Das liegt daran, dass Poliermittel - ähnlich wie Zahnpasta - schleifende Substanzen enthalten. Beim Verreiben glätten diese Mittel die Oberfläche des Displays, nehmen Kratzern die Tiefe und reduzieren damit deren Sichtbarkeit. Doch dabei wird auch ein Teil der Displaybeschichtung entfernt.

Deshalb ist es besser, wenn Sie das Smartphone-Display schon im Vorfeld durch eine Schutzfolie oder ein Schutzglas vor Kratzern bewahren. Das setzt aber voraus, dass Sie sich weder am optischen Effekt noch an der etwas schwergängigeren Touch-Bedienung stören. Entsteht doch ein Kratzer, dann heißt es entweder, damit zu leben, oder das Display gegen

ein neues auszutauschen. Letzteres übernimmt ein professioneller Reparaturbetrieb. Für viele Modelle finden Sie aber auch Anleitungen und Bezugsquellen für Ersatzteile im Netz.

Sünde 10: Handy trifft Mikrowelle

Smartphones bestehen aus einer Vielzahl elektronischer Bauteile, die nicht nur empfindlich auf Hitze, Schmutz und Feuchtigkeit reagieren, sondern auch auf magnetische Felder. Starke Magnetfelder können Transistoren, Magnetfeldsensoren und Speichermedien beschädigen. Handys können dadurch komplett zerstört werden oder zumindest wichtige Daten verlieren.

Zwar entstehen auch rund um Lautsprecher, Elektromotoren und Hochspannungsleitungen Magnetfelder. Doch in den meisten Haushalten dürfte die Mikrowelle die größte magnetische Gefahr für das Handy sein. Diese Geräte erzeugen starke magnetische Felder, um elektromagnetische Wellen zu generieren, die Essen und Getränke erwärmen. Legen Sie Ihr Handy möglichst nicht in die Nähe einer laufenden Mikrowelle, sondern lieber ein paar Meter weit weg.

Quelle: https://www.connect.de/ratgeber/die-6-schlimmsten-handy-suenden-3199451.html?utm_source=connect-NL&utm_medium=newsletter

6) So löschen Sie sämtliche Aktivitäten in Ihrem Google-Konto

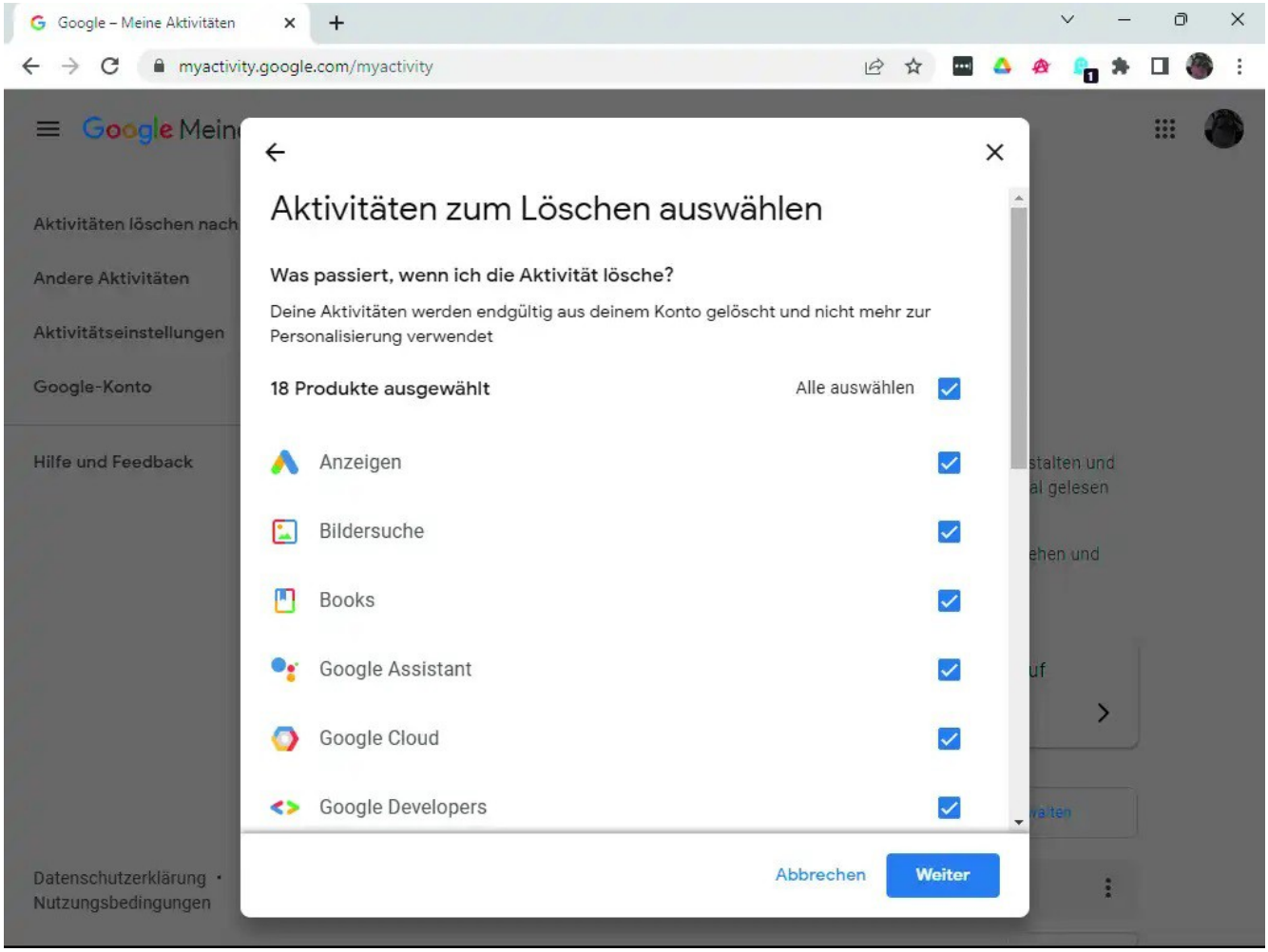
Google sammelt umfangreiche Daten über Sie, darunter Suchanfragen, besuchte Websites, genutzte Apps, Standortdaten, Kontakte und persönliche Informationen. So löschen Sie Ihre Aktivitätsdaten.

Google sammelt so viele Daten über Sie wie nur möglich. Der Konzern merkt sich unter anderem Ihre Eingaben bei seiner Suchmaschine, registriert die Websites, die Sie besuchen, und die Anwendungen, die Sie im Einsatz haben. Hinzu kommen Standortdaten, die Liste Ihrer Kontakte, persönliche Daten wie zum Beispiel Adresse, Alter und Geschlecht und vieles mehr.

All diese Informationen bezieht Google über alle Ihre Geräte hinweg und speichert sie zentral in Ihrem Nutzerkonto. Zumindest die Daten zu Ihren Aktivitäten können Sie dort löschen. Loggen Sie sich dazu über den Browser bei Ihrem Google-Konto ein und rufen Sie die Website https://myactivity.google.com auf.

Dort können Sie über die Buttons „Web- & App-Aktivitäten“, „Standortverlauf“ wie auch „YouTube-Verlauf“ einstellen, welche Daten Google von Ihnen sammeln darf. Um die bereits vorhandenen Daten zu löschen, klicken Sie auf der linken Seite auf „Aktivitäten löschen nach“ und im folgenden Fenster auf „Gesamte Zeit“.

Achten Sie im nächsten Fenster darauf, dass bei „Alle auswählen“ ein Häkchen steht, und klicken Sie unten auf „Weiter“. Es erscheint nun eine Sicherheitsabfrage, die Sie mit „Löschen“ bestätigen.



Quelle: IDG Google sammelt so viele Daten über Sie wie möglich. In den Einstellungen Ihres Kontos können Sie diese Sammelwut begrenzen und alte Einträge löschen.

Tipp: Jetzt prüfen: Fünf schnelle Sicherheits-Maßnahmen

Quelle: https://www.pcwelt.de/article/1977152/aktivitaeten-in-google-konto-loeschen.html

7) Amazon-Konto gesperrt: So bekommen Sie trotzdem Zugriff auf gekaufte Inhalte

Auch wenn Ihr Konto gesperrt wurde, muss Ihnen Amazon Zugriff auf gekaufte Filme, Musik, E-Books und Hörbücher gewähren. Mit diesem Musterbrief geht das.

Bislang war es für Online-Händler Amazon möglich, Nutzerkonten zu sperren, wenn sie gegen Nutzungsrichtlinien verstoßen hatten. Durch diese Sperre konnten Kunden keine Einkäufe mehr über ihr Konto bei Amazon tätigen und hatten keinen Zugriff mehr auf digitale Inhalte, die sie in der Vergangenheit über dieses Konto gekauft haben.

Oberlandesgericht Köln kippt Amazon-Klausel

Diese Klausel in den Amazon-Nutzungsbedingungen hat das Oberlandesgericht Köln nun in einem aktuellen Urteil (AZ: OLG Köln 6 U 90/15) gekippt. *“Jeder Händler kann zwar ohne Angabe von Gründen entscheiden, mit wem er Geschäfte macht. Dies darf aber nicht dazu führen, dass Verbraucher in ihren Rechten eingeschränkt werden,“* erklärt das Oberlandesgericht. Das Urteil ist rechtskräftig und Amazon darf Kunden, deren Konto gesperrt wird, künftig nicht mehr den Zugang zu bereits gekauften Inhalten verwehren.

Amazon darf keine gekauften Inhalte zurückbehalten

Folgende Klausel in den Amazon-AGBs ist damit ab sofort unwirksam: *“Wir behalten uns das Recht vor, Ihnen Services auf der Website vorzuenthalten, Mitgliedskonten zu schließen oder Inhalte zu entfernen oder zu verändern, wenn Sie gegen anwendbare Gesetze, diese Nutzungsbedingungen oder andere anwendbare Vertragsbedingungen oder Richtlinien verstoßen.“*

Kunden können ihr Recht mit einem Musterbrief durchsetzen

Die Verbraucherzentrale empfiehlt Kunden, denen ein Zugriff auf erworbene digitale Inhalte verwehrt wird, gegenüber Amazon auf einen Zugang darauf zu bestehen. Ihr Recht können Amazon-Kunden etwa mit einem an Amazon gerichteten Musterbrief durchsetzen, den die Verbraucherzentrale auf ihrer Website als PDF-Datei bereitstellt. Hier müssen lediglich die Absenderadresse und das Datum sowie eine Unterschrift eingesetzt werden.

Quelle: https://www.pcwelt.de/article/2001735/amazon-konto-gesperrt-mit-diesem-musterbrief-bekommen-sie-trotzdem-zugriff-auf-gekaufte-inhalte.html?utm_date=20230727125618&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Amazon-Konto%20gesperrt%3A%20So%20bekommen%20Sie%20trotzdem%20Zugriff%20auf%20gekaufte%20Inhalte&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

8) Statt auf Post zu warten: Schufa-Auskunft sofort per App einholen

Bei vielen Menschen hat die Schufa einen eher schlechten Ruf. Dennoch geht es oft nicht ohne, wenn Sie einen Kredit wollen. Wie Ihr Schufa-Score ausschaut, prüfen Sie ab sofort per App.

Die Schufa will transparenter werden und bietet jetzt die Möglichkeit, den sogenannten Basisscore über die Web-App Bonify kostenlos abzurufen.
Die Schufa möchte damit transparenter werden und künftig auch mehr Kontrolle über Daten gewähren. Der Basisscore ermöglicht laut Schufa eine Einschätzung der eigenen Bonität über alle Branchen hinweg. Er lässt sich ab sofort jederzeit kostenlos und digital einsehen.

Schufa-Score kostenlos abrufen

Um den Schufa-Score über die Web-App abrufen zu können, müssen Sie sich mit Ihrer Mail-Adresse bei Bonify registrieren. Vergeben Sie dazu ein starkes Passwort, das sich am besten ein Passwortmanager ausdenkt. Sie erhalten danach eine Mail mit einem Aktivierungs-Link, über den Sie das neue Konto freischalten können.

Kniffliger als die Registrierung ist die Identifikation. Sie ist entweder per Personalausweis über IDnow oder per Bankkonto möglich. Vorsicht, mit den Kontodaten gewährt man Bonify umfangreichen Zugriff, um Kontobewegungen von bis zu zwei Jahren abzurufen.

Verbraucherschützer warnen: Auch Verbraucherschützer warnen, das Konto mit Bonify zu verbinden. Datensparsamer ist die Identifikation über den Personalausweis.
Hat man sich identifiziert, wird der Schufa-Basiscore als Prozentwert angezeigt. Je näher man an den 100 Prozent ist, desto besser. Unter den Details können Sie dann noch sehen, wie Sie im Vergleich zu anderen Menschen in Ihrem Bundesland bzw. deutschlandweit abschneiden.

Basisscore per Post erhalten

Die Schufa gibt an, dass die Macher der Bonify-App zwar in einem Tochterunternehmen arbeiten, beide Firmen aber rechtlich unabhängig sind. Ohne explizite Einwilligung sollen keine Daten von der Schufa zu Bonify und umgekehrt fließen.

Wer sich weder mit der Identifikation per Personalausweis noch mit der Angabe von Kontodaten wohlfühlt, kann immer noch auf dem Postweg den Basisscore anfordern. Das ist ebenfalls kostenlos möglich, jedoch mit einer Wartezeit von rund einer Woche verbunden.

Die Schufa weist darauf hin, dass die Bonify-App kein Ersatz für die die offizielle Bonitätsauskunft ist. Diese kostet nach wie vor rund 30 Euro.

Hinweis: Der Abruf des Basisscore steht bisher nur in der Web-App Bonifyzur Verfügung. In den nativen Apps für Android und iOS soll die Funktion noch im August 2023 nachgereicht werden.

Tipp: Schufa-Score verbessern mit einfachem Trick
Kein Handy-Vertrag wegen schlechter Bonität

Quelle: https://www.chip.de/news/Statt-auf-Post-zu-warten-Schufa-Auskunft-sofort-per-App-einholen_184876356.html?utm_source=nl_chipd-dy&utm_medium=chip-newsletter&utm_campaign=19-07-2023%2B17%253A00%253A03&utm_content=nl_chipmob&utm_term=

9) Mehr als 70.000 Router infiziert: Malware bleibt häufig unerkannt

Router von privaten Nutzern und kleinen Unternehmen fallen aktueller Schadsoftware zum Opfer. Das müssen Sie beachten.

Syke – Eine Malware hat Zehntausende SoHo-Router mit Linux-Betriebssystem infiziert – dazu zählen unter anderem Fritz!Box-Router. Da die Schadsoftware zumeist über einen langen Zeitraum unentdeckt bleibt, lohnt sich eine genauere Prüfung. Auch Präventivmaßnahmen können ergriffen werden.

Nutzer von SoHo-Routern aufgepasst: Über 70.000 Router sind infiziert

Erst kürzlich hat sich eine Warnung der Verbraucherzentrale an Telekom-Kunden gerichtet, nun sind linuxbasierte SoHo-Router betroffen. Laut dem Technologieportal *bleepingcomputer.de* ist die Schadsoftware mindestens seit Mai 2021 im Umlauf und somit zwei Jahre lang unentdeckt geblieben. Ziel der Malware: Infizierte Router zu einem Botnetz hinzuzufügen, um kriminelle Aktivitäten der Datengewinnung wie das Ausspähen von Passwörtern und digitaler Werbebetrug zu ermöglichen.

Dass SoHo-Router der Malware zum Opfer fallen und somit kleine Büros sowie private Haushalte betroffen sind, ist kein Zufall. Anders als in großen Unternehmen werden dort seltener Systemupdates durchgeführt – es ist mit größeren Sicherheitslücken zu rechnen. Es zeigt sich: Verbraucher sollten sich nicht nur damit auseinandersetzen, wie sie ihre Router noch schneller machen, sondern auch die Sicherheit der eigenen Daten mehr in den Blick nehmen.

Malware für Router entdeckt: Das müssen Sie nun beachten

Wenn Ihr Router von einer Malware wie dieser befallen wird, sind Ihre Daten in Gefahr. Schon

das Downloaden einer App kann böse Konsequenzen haben. Laut dem Verbraucherportal *Chip* und der Verbraucherzentrale können folgende Maßnahmen zum Schutz vor der Avrecon-Malware und anderen Schadprogrammen helfen:

1. Vor dem Kauf: IT-Sicherheit prüfen und gegebenenfalls beraten lassen
2. Router verschlüsseln, regelmäßig neu starten und aktuelle Sicherheits-Patches installieren
3. Vorsicht beim Herunterladen von Apps und Dateien: besonders bei Programmdateien mit den Endungen .exe, .bat, .com oder .vbs
4. Vorsicht im Umgang mit Mails: besonders bei auffälligen Betreffzeilen und bei unbekannten Links und Anhängen
5. Keine Makros aktivieren, d.h. eine Kette von Befehlen in einem Anwendungsprogramm

Um zu überprüfen, ob Sie bereits von der Schadsoftware betroffen sind, sollten Sie ausfindig machen, um welchen Router es sich handelt. Nutzen Sie einen SoHo-Router mit Linux-Betriebssystem? Dann könnten Sie von dieser Malware betroffen sein. Bei Verdacht oder wenn Sie unsicher sind, sollten Sie den Router zunächst nicht weiterzuverwenden und sich von Fachleuten beraten zu lassen, empfiehlt die Verbraucherzentrale.

Quelle: https://www.kreiszeitung.de/verbraucher/nutzer-homeoffice-update-email-internet-it-passwort-fritzbox-router-soho-linux-sicherheit-virus-92409587.html

Allgemeines:

1) Online-Finanzamt – Das ändert sich bald beim Steuerportal Elster

Wer schon länger nicht mehr in sein Elster-Postfach geschaut hat, sollte das schnell nachholen. Das Portal der Finanzämter ändert eine Regel.

Mit Elster, dem Onlineportal der Finanzämter, können Sie kostenlos Ihre Steuererklärung einreichen. Dabei fällt allerlei Kommunikation an, die bisher in Ihrem privaten Posteingang in "Mein Elster" gespeichert wurde. Doch damit ist bald Schluss.

Wie die Finanzverwaltung am Mittwoch in einer E-Mail an alle Elster-Nutzer mitteilte, werden künftig nur noch solche Nachrichten dauerhaft vorgehalten, die Sie später noch benötigen. Als Beispiele nennen die Behörden Übertragungsprotokolle, digitale Bescheide und Daten zu den Bescheiden.

Elster: Diese Nachrichten werden gelöscht

Alle anderen Nachrichten sollen in Zukunft nach einem Jahr automatisch gelöscht werden. Das betrifft insbesondere Mitteilungen darüber, wenn sich der Status einer Berechtigung oder Vollmacht geändert hat, sowie Informationen zu geänderten Zertifikatsdetails. Den aktuellen Status einer Berechtigung oder Vollmacht können Sie stattdessen schon jetzt jederzeit in den jeweiligen Verwaltungsoberflächen einsehen.

Beginn der Löschung ist der 18. September 2023. Dann verschwinden Nachrichten, bei denen die Speicherfrist bereits abgelaufen ist. "Falls Sie noch einen Teil dieser Dokumente benötigen, loggen Sie sich bitte vor diesem Termin in Ihr Benutzerkonto ein und laden die gewünschten Nachrichten herunter", heißt es in der Mitteilung weiter.

E-Mail statt Nachricht in "Mein Elster"

Künftig erhalten Sie auch keine Nachrichten mehr an Ihr Elster-Postfach, die Ihnen bestätigen, dass Sie ein Formular erfolgreich versendet und übermittelt haben. Stattdessen werden Sie darüber direkt per E-Mail informiert.

Im vergangenen Jahr wurden mehr als 62 Millionen Steuererklärungen mithilfe von Elster verschickt – Rekord. Die hohe Zahl ist allerdings auf die Pflicht zur Abgabe der Grundsteuererklärung zurückzuführen, die Eigentümer im Zuge der Grundsteuerreform einreichen mussten. 2023 sind bisher rund 34,5 Millionen Steuererklärungen via Elster eingegangen (Stand: 30. Juni).

Tipp: Kostenloses Programm: Steuererklärung mit Elster: So geht’s

Quelle: https://www.t-online.de/finanzen/ratgeber/steuern-recht/einkommenssteuer/id_100213986/elster-steuer-portal-aendert-diese-regel-was-sie-jetzt-tun-sollten.html

2) Gebrauchte Technik clever verwerten: So einfach funktioniert eBay Trade-In

Sie haben alte Technik zu Hause und wissen nicht, wohin damit? Mit eBay Trade-In haben Sie jetzt die Gelegenheit, Ihre gebrauchte Technik einzuschicken und den Wert als Gutschein oder Auszahlung zu erhalten. Entdecken Sie, wie einfach es ist, Ihre Technik einzutauschen und erfahren mehr über die smarte Lösung von eBay Trade-In.

Trade-In leicht gemacht: So einfach funktioniert's!

Sie haben alte Technik, die nicht mehr gebraucht wird? Mit eBay Trade-In bietet sich Ihnen die Chance, Ihre gebrauchte Technik einzuschicken, ihren Wert ermitteln zu lassen und Ihnen einen Gutschein über den festgestellten Wert ausstellen zu lassen. Das Beste daran: Sie können den Gutschein entweder als eBay-Guthaben direkt einlösen oder den Wert Ihres Altgeräts auf Ihr Bankkonto überweisen lassen. Aktuell gibt es einen **50-Euro-Gutschein on top**, wenn Sie sich für eBay Trade-In entscheiden. Doch beeilen Sie sich, denn die Aktion ist nur **bis Montag, den 7. August (08:59 Uhr)** gültig.
Das Prinzip von eBay Trade-In ist einfach und unkompliziert. Zuerst finden Sie Ihr Gerät in der Übersicht und machen Angaben zu Marke, Modell und Zustand. Anhand dieser Angaben ermittelt eBay in Kooperation mit dem Partner Foxway den Wert Ihres Altgeräts. Nun stehen Ihnen zwei Optionen zur Auswahl: Sie können sich entweder für eine **Sofort-Gutschrift in Form eines eBay-Gutscheins** entscheiden, der Ihnen beim Kauf eines Artikels Ihrer Wahl den ermittelten Wert vom Kaufpreis abzieht. Oder Sie wählen die **Auszahlung des ermittelten Wertes auf Ihr Bankkonto.**

Gute Gründe für Trade-In: Mehr als nur Smartphones eintauschen

Bei eBay Trade-In geht es nicht nur um Smartphones – Sie haben die Möglichkeit, zwischen 10 verschiedenen Gerätekategorien zu wählen und Ihre alte Technik einzutauschen. Egal ob Tablet, Laptop, Smartwatch oder mehr, mit Trade-In geben Sie Ihrer gebrauchten Technik einen neuen Sinn und sorgen dafür, dass sie ein neues Leben bekommt. Darüber hinaus brauchen Sie sich um Ihre persönlichen Daten keine Sorgen zu machen. Sie sollten lediglich vor Einsendung SIM- und Speicherkarten von Ihrem Altgerät entfernen. Nachdem Ihr Gerät bei den Expert*innen von Foxway eingegangen ist, werden alle Ihre Daten unwiderruflich gelöscht.
Greifen Sie jetzt zu und nutzen Sie die Gelegenheit, Ihre gebrauchte Technik gewinnbringend einzutauschen. Mit eBay Trade-In erhalten Sie nicht nur einen finanziellen Anreiz, sondern

tragen auch dazu bei, dass gebrauchte Technik weiterlebt und eine sinnvolle Verwendung findet. Weitere Informationen zur Aktion finden Sie auf der Website von eBay.

Quelle: https://www.chip.de/news/Gebrauchte-Technik-clever-verwerten-So-funktioniert-eBay-Trade-In_184879633.html?utm_source=nl_chipschnaeppchen&utm_medium=chip-newsletter&utm_campaign=25-07-2023%2B19%253A58%253A14&utm_content=nl_chipmob&utm_term=