40. Cybercrime Newsletter

28.02.2024

1) Neue Betrugsmasche Paypal warnt vor Betrugsanruf: Diese Anrufe sind nicht echt

So funktioniert die Masche

Betrüger haben sich eine neue Masche ausgedacht. Sie überraschen derzeit mit gefälschten Anrufen des Bezahldienstes Paypal. Darin werden die Angerufenen darüber informiert, dass Paypal eine hohe Summe von mehreren hundert Euro abbuchen wird. Um dies zu verhindern, soll eine Taste auf dem Telefon gedrückt werden.
Die Verbraucherzentrale warnt vor diesen Anrufen. Sie würden an andere Betrugsanrufe erinnern. Wer bei diesen nach der Ansage tatsächlich eine Taste gedrückt hat, wurde mit einer Person verbunden und im Gespräch dazu gedrängt, Geld auf ein ausländisches Konto zu überweisen oder in Kryptowährungen zu investieren.
Auch PayPal selbst kennt diese Betrugsmasche. "Wir erhalten derzeit vermehrt Anrufe von Kund:innen zu diesem Thema, darunter leider auch einige, die Opfer dieser Form des Betrugs geworden sind", bestätigt das Unternehmen auf Nachfrage von BRISANT. Betrüger würden dabei mit dem Vertrauen der Menschen spielen. "Häufig werden die Angerufenen unter Zeitdruck gesetzt, um so die Herausgabe von Informationen zu erreichen."

Das sollten Sie tun

Wer einen solchen Anruf bekommt, sollte unbedingt auflegen und keine Taste drücken. Dazu rät auch der Bezahldienst selbst. Das Unternehmen ruft seine Kunden in der Regel nicht an, "– und schon gar nicht mit der Aufforderung, Zahlungen zu leisten." Um sicher zu gehen, dass es keine ungewöhnlichen Zahlungen auf dem Paypal-Konto gibt, sollte man sich das Konto genauer ansehen. Wichtig dabei: Direkt auf die echte Webseite oder in die App gehen.

Auf seiner Webseite warnt der Bezahldienst Paypal vor den häufigsten Betrugsmaschen und listet diese auf. Zudem weist der Dienstleister darauf hin, dass er seine Kunden in der Regel per E-Mail kontaktiert. Ein erster Hinweis auf einen Betrug ist also bereits der Anruf.

Allerdings berichten laut Verbraucherzentrale bislang alle Betroffenen der neuen Betrugsmasche, dass sie noch während der Bandansage aufgelegt haben. Was passiert, wenn man tatsächlich eine Taste drückt oder einfach in der Leitung bleibt, ist also unklar. Keiner der Angerufenen konnte ungewöhnliche Zahlungen oder Abbuchungen feststellen. Sollte Ihnen doch ein hoher Betrag abgebucht worden sein oder Sie andere Ungereimtheiten feststellen, kontaktieren Sie unbedingt den Kundenservice - ebenfalls über die App oder die echte Webseite.

Wenn Sie doch getippt haben

Wenden Sie sich unbedingt an den Kundendienst des Bezahldienstes und behalten Sie Ihr Konto im Auge. Lassen Sie sich auf keinen Fall zu einer Zahlung drängen. Unternehmen wie Paypal weisen darauf hin, dass "seriöse Unternehmen ihre Kund:innen nicht anrufen, um persönliche Informationen abzufragen oder mit der Aufforderung, Zahlungen auszulösen." Außerdem sollten Sie den Betrugsversuch oder den Betrug bei der Polizei anzeigen. Wichtig dabei: die Telefonnummer, von der Sie angerufen wurden. Eine Anzeige kann für Entschädigungszahlungen wichtig sein.

Quelle: https://www.brisant.de/haushalt/sicherheit/paypal-betrug-anruf-172.html

2) Kriminelle kennen oft persönliche Details – Wenn der „Bankmitarbeiter“ anruft: Betrug mit Onlinebanking

Es klingt alles so glaubwürdig, was der angebliche Bankberater am Telefon sagt. Am Schluss ist das Konto leer.

Die Methoden werden immer perfider, zunehmend auch mithilfe von Künstlicher Intelligenz (KI): Kriminelle verschaffen sich Zugang zu sensiblen Daten, erwecken am Telefon Vertrauen bei ihren Opfern, um diese dann online auszuplündern.

Betrug: Fake-Anrufe mit KI

Sie rufen mit gefälschter Telefonnummer, gefälschter Stimme – und Wissen um vertrauliche Konto- und Einkaufsdaten an. Die neuen Maschen treffen immer mehr Menschen, auch jüngere. Längst sind nicht mehr nur Rentner betroffen.

Betrug mit angeblichem Bankmitarbeiter

Ralf Schorn (Name geändert) aus der Nähe von Stuttgart wurde so um sein gesamtes Erspartes betrogen:

Im Oktober klingelt sein Telefon. Auf dem Display: die **Nummer seiner Bank**. Der Anrufer habe gesagt, er sei ein Sicherheitsbeauftragter der Bank, erinnert er sich: „Die Stimme am Telefon sagte, dass auf mein Onlinebanking ein Zugriff erfolgt sei”, das Sicherheitssystem sei angesprungen, weil es mehrere Abbuchungsversuche aus dem Ausland gegeben habe.

Abzocke über die bankeigene Authentifizierungs-App

Der vermeintliche Bankmitarbeiter schlägt vor, das **Onlinebanking zu sperren** und ihm innerhalb von zwei Tagen neue Zugangsdaten zukommen zu lassen. Um diesen Vorgang zu legitimieren, solle er in die Santander-App, die ja für die **zwei Stufen Authentifizierung** mit dem Onlinebanking zuständig ist, sein Passwort eingeben.

Da **alles in der bankeigenen App** passiert, hat Schorn keine Bedenken. Was er nicht ahnt: damit gibt er die Kontrolle über sein Konto komplett an die Betrüger ab. Und die **räumen alles ab**, was geht. Insgesamt 21.000 Euro!

Wie kommen die die Betrüger an sensible Daten?

Voice + Phishing: Eine Kombination aus **Phishing (englisch für: Abfischen)**, also vorhergehendem Datenklau, und **Voice, also der (vertrauenerweckenden) Stimme** am Telefon, die die Opfer überzeugt. Ziel solcher Anrufe ist es, den Opfern sensible Daten zu entlocken oder sie zur Authentifizierung einer Aktion im Onlinebanking zu bringen, wenn die Verbrecher darauf schon Zugriff haben.

Wenn die Stimme mit KI imitiert wird

Damit keine Zeit bleibt, kritisch nachzufragen, erzeugen die Betrüger **Druck**: Es drohen Verluste auf dem Konto.

„Die Täter fangen an, bewusst eine **leichte Panik** zu generieren. In dieser Phase ist man natürlich geneigt, dem Bankmitarbeiter zu glauben: Ja, der hilft mir jetzt schon aus dieser Sache raus!“, erklärt Michael Lerch, Polizeihauptkommissar vom Polizeipräsidium Rheinpfalz in Ludwigshafen.

Solche Vishing- Betrügereien nehmen nicht nur zu, sondern werden immer **ausgefeilter**. Seitdem sich mithilfe von **KI** mit relativ wenig Aufwand **die Stimme nahezu jeder Person imitieren** lässt (es genügen schon wenige Sekunden Sound-Schnipsel), tätigen Betrüger immer öfter **Fake-Anrufe**, bei denen die Opfer vermeintlich die Stimme eines Familienangehörigen in Not hören – oder einen Vorgesetzten oder Mitarbeiter einer Bank.

Anrufer unter falscher Nummer: Caller ID Spoofing

Betrüger können heute zudem mittels krimineller Softeware schnell und einfach ihre Rufnummer verschleiern: Im Telefon-Display erscheint dann **die echte Rufnummer einer Behörde, der Polizei, eines Familienmitglieds oder eben einer Bank**.

Phishing-Daten werden im Internet frei zum Kauf angeboten

Die Betrüger haben sich in den verschiedenen Schritten des Verbrechens spezialisiert. Die einen erbeuten zum Beispiel mit Phishing oder auch mit Hilfe von Schadsoftware Bankzugangsdaten, die anderen nutzen diese dann für den Betrug via Anruf:

Leonard Bunjaku ist Experte für Computersicherheit in Freiburg. Er zeigt eine Webseite: Für alle frei zugänglich im Internet. Dort werden **Bankkunden-Daten** ganz offen zum **Kauf** angeboten: Commerzbank, Volksbank, Deutsche Bank – 20 Euro pro Onlinezugang. Offenbar stammen die Daten aus **Phishing-Angriffen**.

„Es ist natürlich hoch kritisch anzusehen – für jeden zugänglich, das ist schon sehr erschreckend!“ sagt der IT-Sicherheitsexperte.

Leonard Bunjaku zeigt ein Beispiel für eine Phishing-Seite: Durch Spam-Mails werden die Kunden auf falsche Bank-Seiten gelockt und geben dort nichtsahnend ihre Logindaten ein. Mit diesen Daten können Telefonbetrüger dann ihre Anrufe tätigen.

Unsicheres Online-Banking?

Einige Banken würden es den Betrügern auch sehr einfach machen, sich in fremde Konten einzuloggen, meint Experte Bunjaku. So reichen beispielsweise bei der Deutschen Bank immer noch Nutzername und Passwort aus, um ins Onlinebanking zu gelangen. Andere Banken, wie die Volksbank, sichern schon den Login mit einem verpflichtenden zweiten Faktor, wie einer Handy-App, ab.

Hinter solchen Anruf-Abzocken durch falsche Bankangestellte stecken professionelle Banden. Oft aus dem Ausland, sagt Polizeihauptkommissar Michael Lerch. Diese zu fassen und das Geld wiederzubekommen sei nahezu unmöglich.

Phishing und Online-Betrug: Wie kann ich mich schützen?

Michael Lerch, Polizeihauptkommissar: „Grundsätzlich: bei unerwarteten Anrufen misstrauisch zu sein, insbesondere wenn man die Person, die da anruft, einfach nicht kennt. Also die Identität zu verifizieren, macht natürlich immer Sinn. Also nicht einfach blindes Vertrauen zu haben, sondern zu überprüfen, zu hinterfragen.“

Eine echte Bank würde telefonisch niemals ein Onlinebanking-Passwort verlangen, sagt er. Auch kritische Rückfragen helfen, vor allem zu Details, die die Kriminellen vermutlich nicht wissen, wie zweite Vornamen, Aussehen oder ähnliches. Ganz wichtig: **nicht unter Druck setzen lassen**!

Was tun, wenn Geld von meinem Konto abgebucht ist?

- Erster Schritt: Sofort die Bank kontaktieren, um das Konto sperren zu lassen. Dadurch kann nicht noch mehr Geld abfließen. Wenn eine Obergrenze für Abbuchungen besteht - beispielsweise 1.000 Euro - könnten Kriminelle jeden Tag 1.000 Euro abziehen, bis das Konto leer ist.
- Zusätzlich zur Konto-Sperrung am besten auch alle dazugehörigen Karten sperren lassen. Meist ist im ersten Moment unklar, wie Kriminelle an ein Konto gekommen sind. Dafür hat jede Bank eine Sperr-Hotline.
- Wer mehrere Konten hat, sollte auch diese unbedingt auf verdächtige Aktivitäten checken. Außerdem alle Passwörter und Sicherheitsmaßnahmen ändern, die mit Finanzen zu tun haben.
- Zweiter Schritt: Anzeige bei der Polizei erstatten. Mit allen Informationen, die vorliegen. Das ist nicht nur wichtig, um den oder die Täter verfolgen zu können, sondern später vor allem, um Ansprüche gegenüber der Bank geltend machen zu können.

Haftet die Bank?

Grundsätzlich ist die Bank verpflichtet, bei einem nicht autorisierten Zahlungsvorgang den Betrag zu erstattet.

ABER: Der geschädigte Bankkunde muss nachweisen, dass es sich tatsächlich um einen Betrug handelt, den er nicht grob fahrlässig verschuldet hat. Und das ist oft nicht einfach. Ein Beispiel: Wenn mit einer EC-Karte Geld an einem Automaten abgehoben wird, muss ein Betrüger irgendwie an die dazugehörige PIN gelangt sein. Möglicherweise, weil die Nummer mit der Karte zusammen im Geldbeutel aufbewahrt wurde. Wie kann da ein Konto-Inhaber das Gegenteil beweisen?

Ist der PC, der für Online-Banking genutzt wird, geschützt? Durch einen Virenscanner, eine Firewall, die neuesten Updates - oder war es für Kriminelle ganz einfach, sich ins System zu hacken, weil kein ausreichender oder überhaupt kein Schutz bestand? Das könnte dann als grobe Fahrlässigkeit ausgelegt werden, und ein betrogener Bankkunde bekommt sein Geld nicht zurück. Verbraucherschützer sagen, dass viele Banken sich erstmal genau darauf berufen.

Wie lässt sich der Betrug nachweisen?

Das ist tatsächlich oft extrem schwierig. Ein Beispiel: Durch einen Phishing-Angriff, also eine gefälschte E-Mail, die angeblich von der eigenen Bank kommt, wird ein Bankkunde auf eine Betrüger-Seite geleitet und gibt dort sensible Daten ein. Mithilfe dieser Daten wird dann Geld vom Konto abgehoben. Der Vorgang wird am Ende jedoch kaum noch aufzuklären sein, denn diese Seiten verschwinden in der Regel sehr schnell wieder.

Hier selbst Beweise zu sichern, ist schwierig – es handelt sich dabei um Logdateien aus dem Internetrouter oder Telefondaten. Wenn ein Bankkunde etwa von einer manipulierten Nummer angerufen wurde, die bei ihm oder ihr aussah wie die von der eigenen Bank, ist externe Hilfe nötig. Entweder unterstützt die Polizei, wenn Anzeige erstattet wird. Oder es muss ein Fachanwalt eingeschaltet werden, wenn es um größere Summen geht und ein juristischer Streit mit der Bank ansteht. Auf jeden Fall sollte ein Phishing-Opfer seine elektronischen Geräte nicht wesentlich verändern, also zum Beispiel nicht neu aufsetzen, damit mögliche Beweise noch gesichert werden können.

Einigung mit der Bank auch ohne Streit möglich?

Verbraucherschützer sagen, dass Banken sehr oft die Schuld beim Kunden oder bei der Kundin sehen und auf grobe Fahrlässigkeit verweisen. Ein Kulanz-Angebot, dass dann manchmal kommt, sieht vor, dass ein kleinerer Teilbetrag des Schadens erstattet wird. Wer sich wirklich sicher ist, dass er nichts falsch gemacht hat, sollte sich darauf nicht einlassen und sich Hilfe holen.

Abbuchungen oder Überweisungen selbst wieder zurückholen?

Gerade bei Überweisungen ist das am schwierigsten. Eine Überweisung, die ein Kontoinhaber oder eine Kontoinhaberin "aktiv getätigt" hat, kann nicht mehr zurückgeholt werden. Dabei ist es erstmal egal, ob es das Opfer war oder ein Betrüger, denn das muss das Opfer ja nachweisen. Am einfachsten geht eine Rückbuchung bei Lastschriften. Lastschriften können beim Online-Banking selbst zurückholt werden, acht Wochen lang. Kreditkarten-Abbuchungen können reklamiert werden. Dafür gibt es bei der Bank ein Formular. Es ist etwas aufwändig, in der Regel hat man aber bis zu 120 Tage Zeit.

Phishing-Radar: Aktuelle Warnungen vor Betrug

Und noch Hinweis: Wer eine verdächtige E-Mail erhält, kann diese an die Verbraucherzentrale weiterleiten. Auf dieser Basis informieren die Verbraucherschützer auf ihren Internetseiten ständig über neue Betrugsvarianten. Personenbezogene Daten werden dabei anonymisiert. Die E-Mail-Adresse lautet: **phishing@verbraucherzentrale.nrw**

Quelle: https://www.swrfernsehen.de/marktcheck/betrug-im-online-banking-was-tun-wer-haftet-fuer-schaden-100.html

3) Lufthansa und Co. – Airlines: Verbraucherschützer warnen vor Betrugsmasche

Streiks, Verspätungen, Ausfälle: Internetkriminelle nutzen die Unsicherheit Reisender bei Problemen mit Flügen aus. Was vor Betrug schützt.

Damit es auf Reisen nicht stressig wird oder man sogar in die Falle von Betrügern gerät, ist eine gute Vorbereitung wichtig. Vor Antritt eines Fluges oder einer Reise sollte man sich in Ruhe die offizielle Service-Telefonnummer der Airline, des Buchungsportals oder des Reiseveranstalters heraussuchen und notieren.

Denn wer unterwegs oder bei plötzlich auftauchenden Fragen oder Problemen dringend mit einem der Unternehmen sprechen muss und die jeweiligen Kontakte googelt, läuft Gefahr, auf gefälschten Webseiten zu landen oder unwissentlich Betrüger anzurufen. Davor warnt das Europäische Verbraucherschutzzentrum Deutschland (EVZ).

Die Betrüger fordern Reisende dann etwa auf, persönliche Daten einzugeben und Programme oder Apps herunterzuladen. Das alles sollte man genauso wenig tun, wie Bank- oder Kreditkartendaten preiszugeben.

Lufthansa warnt vor betrügerischen Seiten

Auch die Lufthansa warnt beispielsweise in ihren aktuellen Fluginformationen davor, Lufthansa-Kontakte per Suchmaschine zu suchen: So laufe man Gefahr, auf betrügerischen Seiten mit falschen Kontakten zu landen.

Diese Websites zielten darauf ab, Daten von Kundinnen und Kunden abzugreifen. Das Unternehmen rät, nur die auf der offiziellen "Lufthansa.com"-Seite aufgeführten Kanäle für die Kontaktaufnahme zu nutzen und auch nur auf "Lufthansa.com" Daten einzugeben.

Fake-Seiten haben oft abwegige Domains

Wer ad hoc doch einmal die Hotline-Nummer eines Unternehmens benötigt und nicht umhinkommt, eine Internet-Suchmaschine zu verwenden, sollte dem EVZ zufolge genau auf die Adresse der Webseite schauen: Fake-Seiten hätten oft abwegige Domains.

Ein weiterer Tipp für den Anruf bei einer Servicenummer: Bei seriösen Hotlines laufe in aller Regel zunächst eine Ansage vom Band, dann komme man in eine Warteschleife. Bei Betrugsversuchen hat man den Angaben zufolge meist direkt einen Menschen an der Strippe.

Nichts installieren und nichts bestätigen

Im Gespräch sollte man allerspätestens dann misstrauisch werden und auflegen, wenn Software-Installationen oder Bestätigungen in der eigenen Banking-App verlangt werden. Denn kommt es danach tatsächlich zu Abbuchungen von Konto oder Kreditkarte, haben es Verbraucherinnen und Verbraucher den Erfahrungen des EVZ nach schwer, ihr Geld zurückzubekommen.

Betrugsopfer sollten es dennoch versuchen und so schnell wie möglich die eigene Bank kontaktieren und eine Rückerstattung ("Chargeback") fordern. Zudem sollten sie Anzeige bei der Polizei erstatten.

Quelle: https://www.t-online.de/digital/aktuelles/id_100348794/betrugsmasche-bei-airlines-kriminelle-nehmen-reisende-ins-visier.html

4) Betrugs-Ticker – Edeka, DPD und Google: Phishing-Mails fluten Posteingänge

Betrüger denken sich immer wieder neue Maschen aus, um Menschen um ihr Geld zu bringen. Wir zeigen Ihnen, wie gegenwärtig abgezockt wird.

Es ist eine regelrechte Abzockwelle, die derzeit über Konsumenten hereinbricht. Betrüger versuchen vor allem über digitale Kanäle, Zugang zu sensiblen Daten, Kreditkarten und Konten zu bekommen. Mit welcher Masche sie gerade unterwegs sind, lesen Sie immer aktuell hier.

++ Falscher Edeka-Gutschein über 500 Euro (20. Februar 2024) ++

Anfang dieser Woche wurden wieder viele deutsche Posteingänge mit betrügerischen E-Mails überflutet. Innerhalb weniger Stunden kamen gefälschte Schreiben von Edeka, Google, dem Paketdienstleister DPD und vielen anderen angeblichen Absendern an. Hinter den E-Mails stecken Betrüger, die Verbraucher mit falschen Versprechungen auf ihre Webseiten locken, sensible Daten erbeuten und dann die Konten leerräumen wollen.

So wird in dem falschen Edeka-Schreiben ein Geschenkgutschein im Wert von 500 Euro versprochen ("100% kostenlos und ohne Bedingungen"). Die Fake-Google-Mail verspricht 50 GB zusätzlichen, kostenlosen Speicherplatz und der DPD-Brief berichtet, dass eine Paketzustellung fehlgeschlagen sei und eine Unterschrift benötigt werde.

Die Verbraucherschutzzentrale NRW mahnt Empfänger, vor allem auf die Absender-Adressen zu achten. Beim Klick darauf entfaltet sich der wahre Absender – Beispiel DPD: fatmaavcioglu@fetisch.de. "Wir empfehlen wie immer, die Mail unbeantwortet in den Spam-Ordner zu verschieben", schreiben die Verbraucherschützer.

Diese Phishing-Mail verspricht einen Edeka-Gutschein in Höhe von 500 Euro. (Quelle: t-online)

++ Verbraucherschützer warnen ING-Kunden (19. Februar 2024) ++

Die Verbraucherzentrale NRW warnt Kunden der ING-Bank (früher ING-DiBa) davor, auf die abgebildete Phishing-Mail hereinzufallen. Die gefälschte E-Mail beginnt mit einer indirekten Anrede, anschließend wird für das Vertrauen der Kundschaft gedankt. In der Mail heißt es weiterhin, dass Sicherheit und Funktionalität der App gesteigert werden sollen, weshalb eine Überprüfung der Kundendaten vonnöten sei.

"So weit ist der Ton der Mail noch recht freundlich. Am Ende wird aber doch noch Druck ausgeübt, um die Chance einer Datenpreisgabe zu erhöhen", warnen die Verbraucherschützer. So heißt es in der Betrugsmail, sollte man seine Daten nicht bis zum 25.2.2024 überprüft haben, werde man zu einem persönlichen Gespräch vorgeladen.

Eine leere Drohung, da die ING in Deutschland keinen Kundenservice vor Ort hat. "Spätestens hieran lässt sich der Betrugsversuch erkennen. Wir empfehlen wie immer, die Mail unbeantwortet in den Spam-Ordner zu verschieben", schreiben die Verbraucherschützer.

Die falsche ING-E-Mail: Schon bei der indirekten Anrede sollten Kunden stutzig werden. verbraucherzentrale.de

++ Betrüger geben sich als Finanzberater aus (17. Februar 2024) ++

Betrüger haben einen Senior in Panketal bei Berlin um eine fünfstellige Summe Bargeld gebracht. Wie die Polizei am Freitag mitteilte, hatten sich die Täter in den vergangenen Monaten als vermeintliche Finanzberater ausgegeben und bei dem Mann um Investments mit Aussicht auf Dividenden geworben. Dafür forderten sie jedoch eine fünfstellige Summe Bargeld. Der ältere Herr habe das Bargeld per Post versandt. Nach Angaben eines Polizeisprechers lag der Betrag unter 20.000 Euro.

Als der Mann am Donnerstag keinen Gewinn von der scheinbaren Investition erhielt, erkannte er den Betrug. Die Kriminalpolizei hat den Angaben zufolge die Ermittlungen aufgenommen. "Das Geld des Opfers scheint jedoch vorerst verloren", schreiben die Beamten in einer Pressemitteilung.

++ Kriminelle kapern Handynummer (16. Februar 2024) ++

Totalschaden für Opfer: Die Polizei warnt vor einer Betrugsmasche, die SIM-Swapping genannt wird. So heißt es, wenn Betrüger in Ihrem Namen eine neue SIM-Karte bestellen und Sie von ihrer eigenen Nummer aussperren. Das passiere nun auch mit eSIMs und habe weitreichenden Folgen, berichtet das Landeskriminalamt (LKA) Niedersachsen.

Die Beamten erklären: "Erst übernehmen die Täter das Internet-Kundenkonto beim Mobilfunkprovider, dann bestellen sie dort eine eSIM für den Handyvertrag. Und zwar mithilfe des überrumpelten Opfers."

Das Perfide an der Masche ist, dass die Kriminellen ihre Opfer auf eine ganz falsche Fährte locken, um den geplanten Identitätsdiebstahl zu verschleiern. Sie rufen über eine

Mobilfunknummer an und geben sich etwa als Paketbote aus: Es befinde sich eine Sendung in Zustellung. Dieses könne aber aus Sicherheitsgründen oder wegen einer angeblich falschen Adresse nur ausgeliefert werde, wenn ein Code genannt wird, der per Kurznachricht kommt. Tatsächlich erhalten die Opfer dann eine SMS.

Doch der Code in der SMS kommt nicht von einem Paketdienst, sondern vom Mobilfunkanbieter, was die Opfer im Eifer des Gefechts übersehen. Denn es gibt Provider, die den Log-in beim Online-Kundenkonto nicht nur per Passwort, sondern auch per Einmal-SMS-Code anbieten, den jeder anfordern kann, der die Mobilfunknummer kennt.

Nennt nun das Opfer den Code am Telefon, können die Betrüger das Kundenkonto übernehmen und dann im Zweifel auch eine eSIM bestellen, die sie auf einem eigenen Gerät installieren, um Rufnummer und Vertrag des Opfers missbräuchlich zu nutzen.

++Gefälschte Bahn-Mail verspricht Jahreskarte (30. Januar 2024) ++

Wer würde nicht gerne ein Jahr gratis mit der Bahn fahren können – und in Zeiten von Streiks und Verspätungen scheint dieses Gewinnspiel eine freundliche Wiedergutmachung der Bahn zu sein. Angeblicher Preis: Eine Jahreskarte der Bahn für die Reise in der 1. Klasse bei Teilnahme am Gewinnspiel.

Aber Vorsicht. Sollten Sie dieses Angebot im Namen der Bahn erhalten haben (siehe Bild), dann verschieben Sie die E-Mail am besten sofort unbeantwortet in den Spam-Ordner, rät die Verbraucherzentrale. Klicken Sie auch auf keinen Fall auf die beiden angezeigten Links. Die Verbraucherschützer gehen davon aus, dass Opfer hier ihre Daten, zum Beispiel Kreditkartendaten, preisgeben sollen – und später das Konto leer geräumt wird.

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

Quelle: https://www.t-online.de/digital/aktuelles/id_100346104/betrugsmaschen-aktuell-edeka-dpd-google-flut-an-phishing-mails.html

5) Android-App sofort löschen: sonst leeren Kriminelle gnadenlos das Bankkonto

Mit nur einem Klick holen sich Android-Nutzer eine Gefahr auf ihr Handy: Schadprogramme. So entgeht man der Masche der Cyberkriminellen.

Dortmund – Mit jedem Download steigt die Gefahr, dass gefährliche Programme sich auf dem Smartphone ausbreiten. Unwissende bemerken den Schaden oft erst, wenn es bereits zu spät ist. In einem aktuellen Fall könnte das Geld auf dem Konto verschwunden sein (mehr zu Digitales auf RUHR24).

Android-App sofort löschen: Sonst leeren Kriminelle gnadenlos das Bankkonto

Davor warnt die Informationsplattform Watchlist Internet, die über Betrugsmaschen im Internet informiert. Im Umlauf ist derzeit ein Banking-Trojaner namens Anatsa.

Android-Nutzer können sich das Schadprogramm einfangen, sobald sie Apps wie PDF-Reader oder PDF-Viewer downloaden. Dass die Android-App verseucht ist, ist auf den ersten Blick nicht ersichtlich. Doch sobald Verbraucher dazu aufgefordert werden, ein zusätzliches Add-on herunterzuladen, ist Vorsicht geboten. Auf diese Weise gelangt der Virus auf das Handy, der Tastatureingaben des Nutzers mittels eines Keyloggers aufzeichnet.

Die Folgen können denkbar fatal sein, denn dadurch erhalten Kriminelle die Möglichkeit, an

persönliche Daten zu gelangen. Erspähen sie die Zugangsdaten für das Online-Banking, können sie problemlos Überweisungen tätigen, heißt es weiter.

Android-App sofort löschen – wie sich Verbraucher schützen können

Eine Schadsoftware kann sich nicht auf einem Handy ausbreiten, wenn Verbraucher frühzeitig erkennen, dass es sich um eine solche handelt. Watchlist Internet zufolge ist man auf der sicheren Seite, wenn man nur Apps aus dem offiziellen Google Play Store herunterlädt. Für iOS-Nutzer empfiehlt sich der Apple Store.

Liegen Warnungen zu einer Anwendung in den Bewertungen vor? Falls ja, sollte dies als weiteres Alarmsignal dienen, um die App nicht herunterzuladen. Und wenn es zudem erforderlich ist, Drittanbietern Zugriff zu gewähren, sollte man äußerst aufmerksam sein.

Android-App sofort löschen – weitere Schutzmaßnahmen ergreifen

Überall dort, wo es Internet gibt, kann eine potenzielle Gefahr lauern. Nicht nur im Posteingang, sondern auch in internetfähigen Geräten wie ferngesteuerten Sicherheitskameras und smarten Türschlössern. Dem Einfallsreichtum der Cyber-Kriminellen sind keine Grenzen gesetzt. Um ihnen einen Riegel vorzuschieben, sind einige Schutzmaßnahmen durchzuführen:

- **Virenschutzprogramm, Internetbrowser und Betriebssystem** up to date halten.
- Regelmäßige **Backups** für die Daten durchführen.
- **IT-Sicherheit** vor dem Kauf internetfähiger Geräte prüfen.

Neue Angriffswelle mit Banking-Trojaner

Anatsa ist eine bereits gut bekannte Schadsoftware, die die Sicherheitsforscher der Firma ThreatFabric kontinuierlich überwachen. Der Banking-Trojaner erscheint in Angriffswellen, die verschiedene geografische Regionen anvisieren. Im jüngsten Fall sind Länder in Europa betroffen. Dem aktuellen Bericht von ThreatFabric zufolge haben die Forscher erhöhte Aktivität des Trojaners in Deutschland, Slowakei, Slowenien, Spanien, Tschechien und UK festgestellt. Dort wurden mindestens 150.000 infizierte Geräte verzeichnet, wie ThreatFabric gegenüber „*Bleeping Computer*“ angegeben hat.

Die Hacker benutzen sogenannte „Dropper“-Apps, um den Banking-Trojaner auf Smartphones einzuschleusen. Diese Apps wirken nach außen hin wie legitime Apps, die in der Regel kostenlos zur Verfügung stehen. Die Angreifer konzentrieren sich dabei auf Genres, die eine hohe Nachfrage haben – wie im aktuellen Fall Cleaner-Apps, PDF-Reader und Datei-Manager. Damit gelingt es ihnen oft, im Play Store in der Top-Liste der kostenlosen Apps zu erscheinen. Das verleiht den Droppern mehr Sichtbarkeit und führt zu mehr Installationen. Die Apps lassen sich oft wie beschrieben nutzen – „droppen“ jedoch im Hintergrund die eigentliche Malware.

Infizierte Apps können Entdeckung entgehen

Dem ThreatFabric-Bericht zufolge nutzen die Angreifer einen mehrstufigen Prozess, um den Banking-Trojaner Anatsa einzuschleusen. Damit können sie Sicherheitsvorkehrungen im Android-Betriebssystem bis Version 13 umgehen. Die entscheidende Rolle spielen dabei die Bedienungshilfen in Android, die Benutzern mit Einschränkungen die Bedienung ihres Smartphones vereinfachen sollen.

Direkt nach der Installation kommunizieren die Dropper-Apps mit einem Command-and-Control-Server (C2), um die erfolgte Installation zu registrieren. Der C2-Server konfiguriert eine sogenannte DEX-Datei, die den Download der Malware vorbereitet. Die Hacker können

den Link auf die Malware dynamisch anpassen, sollte ein erster Versuch entdeckt werden. Erst dann sendet der Server den eigentlichen Banking-Trojaner an die App, um das Gerät zu infizieren. Anatsa bedient sich dabei der Programmierschnittstelle AccessibilityService, mit der die Installation Malware ohne Nutzereinwirken stattfindet. Die Apps erlangen Zugriff auf AccessibilityService, indem sie legitim wirkende Anfragen stellen. Laut ThreatFabric fordern Anatsa-Dropper etwa den Zugriff, um Apps mit hohem Akku-Verbrauch einzufrieren.

Ist der Banking-Trojaner einmal installiert, kann er das Smartphone übernehmen und finanzielle Transaktionen anstelle der Nutzer ausführen.

Diese Apps sollten Nutzer sofort löschen

Bislang hat ThreatFabric laut „*Bleeping Computer*“ fünf Apps identifiziert, die Teil der aktuellen Angriffswelle mit dem Banking-Trojaner Anatsa sind. Die Apps wurden insgesamt mehr als 150.000-mal installiert. Die Firma hat Google über ihre Ergebnisse informiert, das sie mittlerweile aus dem Play Store gelöscht hat. Alle betroffenen Apps stehen möglicherweise weiterhin in App-Archiven und Drittanbieter-Stores zur Verfügung.

Wer untenstehende Apps bereits installiert hat, sollte diese umgehend löschen.

- **Phone Cleaner – File Explorer** (com.volabs.androidcleaner)
- **PDF Viewer – File Explorer** (com.xolab.fileexplorer)
- **PDF Reader – Viewer & Editor** (com.jumbodub.fileexplorerpdfviewer)
- **Phone Cleaner: File Explorer** (com.appiclouds.phonecleaner)
- **PDF Reader: File Manager** (com.tragisoap.fileandpdfmanager)

Tipp: Lesen Sie weiter: Diese Malware-Kampagnen bedrohen derzeit Android-Geräte und iPhones

Quelle: https://www.ruhr24.de/service/gefahr-loeschen-handy-kriminelle-bankkonto-schadsoftware-internet-virus-digitales-android-app-92829743.html
und
https://www.techbook.de/mobile-lifestyle/apps/banking-trojaner-anatsa?utm_source=flipboard&utm_content=topic%2Fde-digital

6) Vorsicht vor Ping-Call-Betrug via WhatsApp: Dubiose Anrufe aus Indien, Iran und Mexiko

Nutzer von WhatsApp melden vermehrt unerwünschte Anrufe von unbekannten ausländischen Nummern. Die dubiosen Anrufer nutzen dabei sogenannte Vorwahlen aus Ländern wie Indien, dem Iran oder Mexiko. Experten vermuten einen Betrugsversuch hinter dieser Entwicklung.

In den letzten Tagen beklagen immer mehr WhatsApp-Nutzer anonyme Anrufe, die insbesondere Vorwahlen aus Indien, dem Iran und Mexiko aufweisen. Die Motive hinter diesen Anrufen sind noch nicht vollständig geklärt, doch es besteht der Verdacht auf betrügerische Absichten.

Wie das Landeskriminalamt Rheinland-Pfalz mitteilt, bedienen sich die Anrufer offenbar einer als "Ping-Call" bekannten Technik. Dabei wird das Telefon des Empfängers nur kurz zum Klingeln gebracht, bevor der Anrufer wieder auflegt. Das Ziel ist es, den Empfänger dazu zu bringen, zurückzurufen. Oft sind diese Anrufer nicht im digitalen Adressbuch des Empfängers gespeichert. Besonders auffällig sind Nummern mit der indischen Ländervorwahl +91.

Versteckte Codes in der Nummer?

Im Gegensatz zu herkömmlichen Betrugsmethoden geht es bei diesen Anrufen jedoch nicht darum, über kostenpflichtige Nummern Geld einzutreiben. Vielmehr wird vermutet, dass die Anrufer ihre Opfer dazu bewegen wollen, Geld zu überweisen oder persönliche Daten preiszugeben. Eine weitere Theorie besagt, dass die Betrüger versuchen könnten, mithilfe von in der Nummer verborgenen Steuercodes fremde WhatsApp-Konten zu übernehmen.

Wie man sich schützen kann

Um sich vor diesen dubiosen Anrufen zu schützen, sollten Nutzer unbedingt vermeiden, Anrufe von unbekannten ausländischen Nummern entgegenzunehmen oder zurückzurufen. Dies gilt unabhängig davon, ob die Kontaktaufnahme über WhatsApp oder einem anderen Messenger erfolgt.

In den Einstellungen von WhatsApp gibt es zudem die Möglichkeit, Anrufe von unbekannten Nummern stummzuschalten. Hierzu muss man den Bereich "Datenschutz" ansteuern und dort den Punkt "Anrufe" finden. Dort kann die Option "Anrufe von Unbekannt stummschalten" aktiviert werden. Damit werden keine Telefonate mehr durchgestellt, wenn die Nummer nicht als Kontakt gespeichert ist.

Quelle: https://www.ak-kurier.de/akkurier/www/artikel/139648-vorsicht-vor-ping-call-betrug-via-whatsapp--dubiose-anrufe-aus-indien--iran-und-mexiko

7) Betrügerische Webportale – Experten warnen vor Betrugsmasche: Opfer um 700.000 Euro erleichtert

Betrüger haben auch in den Landkreisen Ravensburg, Sigmaringen und Bodensee Geldanlagen im Visier. Sie versprechen traumhafte Renditen beim Festgeld. Wie Sie sich schützen.

Die Polizei Ravensburg warnt vor einer neuen Betrugsmasche, die derzeit auch in den Landkreisen Ravensburg, Sigmaringen und Bodensee die Runde macht.

Laut Polizeibericht geht es um Geldanlagen, die traumhafte Renditen bei einer Laufzeit von nur zwei Jahren garantieren - angelegt als Festgeld. Bei solchen Angeboten sei Vorsicht geboten, warnt die Polizei.

Betrügerische Webportale für Festgeld seien nur schwer von seriösen Angeboten zu unterscheiden. Und so gehen die Betrüger laut Polizei vor: Der Kunde legt sein Erspartes für einen bestimmten Zeitraum fest an. Zunächst wirkt die Anlage seriös, die Kontoauszüge machen was her, und das Opfer hat ein gutes Gefühl.

Die Anleger werden zunächst auch engmaschig telefonisch von vermeintlichen Bankberatern betreut. Das böse Erwachen kommt dann am Ende der Anlagezeit, wenn es um die Auszahlung geht. Dann sind die Betrüger mit dem Geld bereits verschwunden.

Überweisung geht direkt an die Betrüger

Denn oft überweisen die Opfer im Glauben, ihr Geld auf ein festes Anlagekonto zu überweisen, direkt an die Betrüger im Ausland, erklärt die Polizei. Dabei machen sich die Täter den sogenannten IBAN-Trick zunutze: Die Opfer überweisen ihr Erspartes an ihren eigenen Namen mit einer ausländischen Kontoverbindung und glauben so, ein Konto im

Ausland zu besitzen. Da die Empfängerbanken jedoch nicht verpflichtet sind, den Namen des Kontoinhabers in Verbindung mit der IBAN zu überprüfen, bleibt der Geldfluss für diese meist unentdeckt.

Die Kriminalpolizeidirektion Friedrichshafen hat bereits mehrere Ermittlungsverfahren mit dieser Betrugsform bei der Staatsanwaltschaft zur Anzeige gebracht. Die Aussichten auf einen Ermittlungserfolg sehen jedoch düster aus. Laut Polizeibericht hat ein Opfer rund 700.000 Euro „investiert“ - das Geld konnten aber auch die Ermittler nicht mehr zurückholen.

Ausschließlich zu seriösen Banken gehen

Die Kriminalbeamten warnen daher: „Legen Sie Ihr Geld ausschließlich bei seriösen Banken und Kreditinstituten an. Prüfen Sie verlockend klingende Angebote akribisch, und lassen Sie sich weitere Angebote machen. Überweisen Sie kein Geld auf ein ausländisches Konto! Sollten Sie dennoch Opfer eines Betrugs geworden sein, erstatten Sie umgehend Anzeige bei der Polizei.“

Quelle: https://www.schwaebische.de/regional/oberschwaben/ravensburg/neue-betrugsmasche-um-700-000-euro-erleichtert-2278250

8) Vorsicht, Telefonbetrug: Bei diesen Telefon-Nummern auf keinen Fall ans Handy gehen

Betrügerische Telefonanrufe können nicht nur nerven, sondern auch teuer werden. Bei diesen Rufnummern sollten Sie nicht rangehen und am besten direkt blocken.

Ob perfider Enkeltrick, fiese Schockanrufe oder diverse andere Abzockmethoden über Handy –für Kriminelle ist die Betrugsmasche über Telefon immer noch ein lukratives Geschäft.

Zwar nehmen Betrüger häufig insbesondere ältere Menschen ins Visier, doch das Bundeskriminalamt warnt auf seiner Internetseite regelmäßig alle Bürger zur besonderen Vorsicht. Denn betrügerische Spam-E-Mails oder Betrugsmaschen am Telefon können jeden treffen. Dass Kriminelle die Gutgläubigkeit ihrer Opfer schamlos ausnutzt, hat im vergangenen Jahr für viel Frust bei den Betroffenen gesorgt. 2023 sind nach Angaben der Bundesnetzagentur rund 60.000 Beschwerden eingegangen. Aktuell geht eine neue Betrugsmasche um, die Kunden der ING-Bank ins Visier nimmt.

Bei Anruf Abzocke: Bei diesen Telefonnummern handelt es sich um Betrüger

Leider reißen die Betrugsversuche über Telefon nicht ab. Im Gegenteil. Sie nehmen weiter zu, so die Erkenntnisse der App-Betreiber von *Clever Dialer*. Jeden Monat geben die Experten für Spam-Schutz und Anruferkennung die von Verbrauchern am häufigsten gemeldeten, verdächtigen Telefonnummern heraus. In ihrem aktuellen Bericht für Januar 2024 konnten die Fachleute sogar einen Zuwachs an Spam-Anrufen von 4,8 Prozent im Vergleich zum Vormonat Dezember registrieren.

Im Top-10-Ranking belegt Großbritannien die drei Spitzenplatzierungen. Bei allen Telefonnummern im Ranking handelt es sich um Kostenfallen. Die reichen von falschen, verführerischen Gewinnversprechen bis hin zu Angeboten für Zahnersatz oder Krankenversicherungen und telefonischen Belästigungen in Dauerschleife. Das Erfreuliche hingegen ist, dass die gemeldeten Blockierungen immerhin um 26,6 Prozent gestiegen sind. „Verbraucher wissen sich zu wehren, sind aufgeklärter und nutzen zunehmend Lösungen wie Anti-Spam-Apps“, gibt *Clever Dialer* an.

Von diesen Telefonnummern gab es im Januar 2024 am meisten Spam-Anrufe © Clever Dialer

Betrugsversuche: Auch im Internet scheuen Cyberkriminelle keinen Aufwand

Welche Abzocke sich hinter den jeweiligen Nummern aus Deutschland versteckt, lesen Sie nachfolgend im Überblick:

Spam-Mobilfunknummern aus Deutschland:	Art des Betrugsversuchs:
015258439631	Angeblicher Gewinn
01632392810	Tägliche Anrufe: Mehrfache Versuche, den Angerufenen auszufragen
01744366754	Betrügerischer Anruf (Bei Rückruf ist die Nummer nicht vergeben)
01629529625	Teilnahme an einem angeblichen Gewinnspiel
015213560964	Vermeintliches Angebot für Zahnpflege und Krankenkasse
015258438437	Gewinnversprechen mit Abfrage von persönlichen Daten
01629529841	Verdacht auf Spam-Anruf

Doch leider lauern die Gefahren, von Kriminellen abgezockt zu werden, nicht nur am Telefon. Auch im Internet scheuen Cyberkriminelle keine Mühen und versuchen mit Fake-Shops oder Phishing-Versuchen ihre ahnungslosen Opfer abzuzocken. Zum Teil setzen sie sogar auch Künstliche Intelligenz für ihre Betrügereien ein. Bei einer neuen Betrugsmasche namens Social Engineering erschleichen sich Betrüger das Vertrauen ihrer Opfer, um sie zu manipulieren.

Quelle: https://www.merkur.de/verbraucher/telefon-betrug-spam-nummern-kostenfalle-warnung-handy-92833708.html

9) Online-Ausweisfunktion: Kritische Schwachstelle erlaubt Übernahme der Identität

Die Umsetzung der Online-Ausweisfunktion auf Smartphones reißt eine immense Lücke in das Identifizierungsverfahren. Wirklich schließen lässt sich die nicht.

Ein anonymer Hacker hat eine Schwachstelle in der Online-Ausweis-Funktion des Personalausweises gefunden, die es Unbefugten ermöglicht, fremde Identitäten vollständig zu übernehmen. Damit könnten beispielsweise in fremdem Namen Konten eröffnet oder Behördengänge erledigt werden. Benötigt wird dafür zwar ein Zugriff auf das Smartphone der angegriffenen Person, der ließe sich aber bereits über eine manipulierte App erlangen. Damit ließe sich demnach der eigentlich für Identifizierung über die offizielle AusweisApp übertragene PIN abfangen und an den Angreifer weiterleiten. Der kann sich damit und mit weiteren einsehbaren Informationen als die angegriffene Person ausgeben und in derem Namen aktiv werden.

Sicherheitslücke nur schwer zu schließen

Mit der Methode lasse sich das schwächste Glied in der Sicherheitskette der Online-Ausweis-Funktion ausnutzen, erklärt der nur unter dem Pseudonym "CtrlAlt" auftretende Entdecker der Schwachstelle in einem ausführlichen Blogeintrag. Dort erklärt er, wie beispielsweise beim Besuch der Seite der Arbeitsagentur mit dem Smartphone eine Weiterleitung zur AusweisApp erfolgt. Genau dieser Deeplink kann demnach mit einer bösartigen App gekapert werden, ohne dass das auf dem Gerät ersichtlich ist. Wie leicht Nutzern und Nutzerinnen solch eine App untergejubelt werden kann, hat erst vor wenigen Tagen die Verfügbarkeit einer irreführenden Kopie des Passwort-Generators LastPass gezeigt. Der Angriff über solch eine App wäre auch auf einem Smartphone möglich, das alle Updates installiert hat.

"CtrlAlt" hat dem Bundesamt für Sicherheit in der Informationstechnik nach eigenen Angaben eine umfangreiche Dokumentation zukommen lassen und anderthalb Monate Zeit eingeräumt. Das BSI habe der Beschreibung auch zugestimmt, die sei "technisch in nahezu jedem Aspekt korrekt". Trotzdem hält man es dort nicht für notwendig, in irgendeiner Weise zu reagieren, weil die kritische Schwachstelle mit der CVE-ID CVE-2024–23674 nicht direkt in der Software oder Hardware zu finden ist. Stattdessen werde darauf verwiesen, dass es an den Nutzern und Nutzerinnen liege, für die Sicherheit auf ihren Geräten zu sorgen. Das sei unverantwortlich, kritisiert "CtrlAlt", auch weil die dafür gemachten Vorschläge im konkreten Fall überhaupt nichts helfen würden.

"Die Behauptung, dass User solch einen Angriff verhindern können, indem sie Sicherheitsratschlägen folgen, ist nicht korrekt", meint "CtrlAlt". Er habe mehrere mögliche Angriffswege dokumentiert, nur gegen einen würden die BSI-Vorschläge überhaupt helfen. Er schlägt stattdessen vor, als erste Gegenmaßnahme eine offizielle Liste aller sicheren Apps mit eID-Funktion öffentlich zu machen. Das würde es zumindest leichter machen, potenziell betrügerische Software zu erkennen. Das BSI hat laut dem Spiegel angekündigt, das zumindest zu prüfen. Potentiell verschärft wird das Problem durch die erzwungene Öffnung der App-Stores für Android und iOS, was die Einschleusung gefährlicher Apps erleichtern könnte. Empfehlungen für eine wirkliche Entschärfung hat "CtrlAlt" nicht.

Das BSI hat seine Reaktion nun ebenfalls veröffentlicht und wiederholt die Aussagen, die gegenüber dem Hacker gemacht wurden. Auch gegenüber heise online hat das Bundesamt inzwischen noch einmal beteuert: "Aus Sicht des BSI besteht keine Schwachstelle in der AusweisApp."

Quelle: https://www.heise.de/news/AusweisApp-Kritische-Schwachstelle-erlaubt-Uebernahme-fremder-Identitaeten-9630452.html

10) Online-Banking: Betrüger stehlen 50.000 Euro – Bank muss Schaden nicht ersetzen

Betrüger haben einem Mann beim Online-Banking 50.000 Euro gestohlen. Das Betrugsopfer wollte das Geld von seiner Bank erstattet bekommen. Doch ein Gericht entschied anders: Die Bank muss den Schaden nicht ersetzen.

Ein Rechtsanwalt und Steuerberater bleibt vorerst auf einem Schaden von 50.000 Euro sitzen. Seine Bank muss ihm das verlorene Geld nicht erstatten, entschied jetzt das Oberlandesgericht Frankfurt (Urteil vom 06.12.2023 – Az. 3 U 3/23). Das berichtet Spiegel Online. Der Fall stellt sich folgendermaßen dar.

Der Mann sagt, dass er im September 2021 eine SMS erhalten habe, die dem Anschein nach von einer Telefonnummer kam, die sonst seine Bank für die Kundenkommunikation verwendet. In der Kurznachricht stand, dass das Online-Konto des Mannes eingeschränkt worden sei. Um das zu ändern, solle er sich für ein neues Verfahren anmelden und hierzu auf einen Link tippen, der in der SMS enthalten war.

Der Rechtsanwalt tat das. Daraufhin rief ihn ein Mann an. Im Lauf des nun folgenden Gesprächs bestätigte der Rechtsanwalt eigenen Angaben zufolge auf Anweisung des Anrufers “etwas” in der Push-TAN-App seiner Bank. Noch am selben Tag wurden vom Konto des Mannes 49.999,99 Euro abgebucht.

Der Rechtsanwalt war auf einen Betrüger hereingefallen und wollte daraufhin, dass ihm seine Bank den Schaden erstattet. Die Bank lehnte das aber ab. Deshalb verklagte das Betrugsopfer seine Bank.

Die Bank widerspricht jedoch der Darstellung des Opfers. Denn laut Bank machte ihr Kunde sogar zwei Freigaben: Zunächst habe er per Push-TAN-Freigabe das Tageslimit für Überweisungen für einen Tag auf 50.000 Euro hochsetzen lassen. Diese Freigabe erfolgte laut Bank per Gesichtserkennung. Danach überwies der Mann noch die 49.999,99 Euro mit einer zweiten Freigabe.

Grobe Fahrlässigkeit und atypischer Ablauf

Dieser Unterschied in den Angaben zwischen dem Betrugsopfer und seiner Bank ist wichtig. Denn damit sei die Angabe des Mannes, dass er nur einmal “etwas” in seiner App per Gesichtserkennung bestätigt habe, nicht glaubhaft, wie das Gericht feststellt. Sondern es liege grobe Fahrlässigkeit vor, weil er gleich zweimal die entsprechende Freigabe erteilt habe.

Das Gericht stellte zudem fest, dass das Betrugsopfer aufgrund seiner beruflichen Qualifikation – der Mann ist wie erwähnt Rechtsanwalt und Steuerberater – grundsätzlich erfahren sei mit geschäftlichen Dingen wie eben dem Online-Banking. Der Mann habe zugegeben, dass er Online- und Telefonbanking bei mehreren Instituten nutze und mit den grundlegenden Funktionen der dazu notwendigen Apps vertraut sei. Der Kläger habe aber laut Gericht durch die (mehrmalige) Bestätigung der Push-TAN gegen seine Verpflichtung verstoßen, Sicherheitsmerkmale vor unbefugten Zugriff zu schützen. Zudem habe der Mann erkennen müssen, dass ein “atypischer Ablauf” vorliegen würde – damit ist der Tipp auf den Link in der SMS und der Anruf gemeint.

Das Urteil ist noch nicht rechtskräftig, weil der Mann Nichtzulassungsbeschwerde eingereicht habe und vor dem Bundesgerichtshof in Revision gehen wolle.

Quelle: https://www.pcwelt.de/article/2236858/online-banking-betruger-stehlen-50000-euro-bank-muss-schaden-nicht-ersetzen.html?utm_source=flipboard&utm_content=markuxx077%2Fmagazine%2FSecurity

11) Vorsicht: Raffinierter Betrug mit Samsung Galaxy S24 – so läuft die fiese Masche

Betrüger haben sich einen schlauen Weg ausgedacht, um Kaufinteressenten eines Samsung Galaxy S24, S24+ oder S24 Ultra um ihr Geld zu bringen. So geht der Betrug.

Das österreichische Sicherheitsportal Watchlist Internet warnt vor Betrügereien mit dem Samsung Galaxy S24, S24 plus und S24 Ultra (ausführlicher Testbericht). Demnach bieten Betrüger das Top-Smartphone der Südkoreaner zu extrem niedrigen Preisen in Fake-Onlineshops an. Für schlappe 149 Euro bis maximal 269 Euro zuzüglich Nachnahmegebühr würde man die hochpreisigen Smartphones dort angeblich bekommen. Doch die dort bestellten Smartphones werden nie geliefert, das Geld ist verloren.

Die Betrüger bauen in ihren Webshops – Watchlist Internet nennt konkret shop.mgmmgme.shop als Beispiel für die Adresse eines solchen betrügerischen Webshops – die offiziellen Samsung-Seiten zum S24 nach, um ihren Shop möglichst authentisch erscheinen zu lassen. Nur bei den Preisen unterscheiden sich die nachgebauten Shops von Samsungs Onlineshop. Das Galaxy S24 Ultra mit 1 TB bekommt man dort für gerade einmal 269 Euro, für ein Galaxy S24 plus mit 512 GB muss man nur 209 Euro zahlen und das günstigste S24 mit 128 GB gibt es in diesem Fakeshop für sage und schreibe 149 Euro.

Für solch niedrige Preise bekommen man allenfalls Einsteiger-Smartphones, aber ganz sicher nicht die Flaggschiffe von Samsung, die dem Apple iPhone Paroli bieten.

Das ist der fiese Trick: Nachnahme und leere Päckchen

Um misstrauische Käufer zu überzeugen, verkaufen die Betrüger nur per Nachnahme. Die Käufer müssen also nicht vorab überweisen! Erst bei Übergabe der Lieferung durch den Postboten muss man bezahlen. Das sollte doch Betrug unmöglich machen …

Macht es aber nicht. Denn die per Nachnahme zugestellten Päckchen sind **leer**. Und der Briefträger ist mit der Nachnahme bereits weg.

Tipp: Falls Sie den Betrug noch **vor** Empfang des Päckchens durchschauen, können Sie sich leicht schützen: Verweigern Sie einfach den Empfang der Nachnahmesendung und zahlen Sie nichts. Dann geht die (leere) Lieferung an die Betrüger zurück.

Sie haben bereits die Nachnahme bezahlt?

Dann ist das Geld wohl weg, denn die Post ist **nicht** Ihr Ansprechpartner. Ihre einzige Möglichkeit: Erstatten Sie sofort Anzeige bei der Polizei. Vielleicht besteht dann noch eine Möglichkeit, dass diese die Weitergabe des Geldes von der Post an die Betrüger stoppt.

So erkennen Sie Fakeshops

Typisch für betrügerischen Shops sind die niedrigen Lockvogelpreise und meist Vorkasse (im oben geschilderten Fall allerdings nicht) als einzige tatsächlich mögliche Zahlart. Viele dieser Fakeshops bieten zwar anfangs auch andere Bezahlmöglichkeiten an, unterbinden dann aber letztlich jede andere Möglichkeit und bestehen auf Vorkasse. Mitunter schalten derartige Fakeshops sogar Werbung auf Plattformen wie Facebook. Seien Sie also misstrauisch.

Überprüfen Sie immer das Impressum. Zahlen Sie nie per Vorkasse. Suchen Sie im Internet nach Bewertungen für den infrage kommen Onlineshop. Kann man die Gütesiegel auf der Webseite anklicken und führen diese dann zu dem Aussteller des Siegels – oder ist das

Gütesiegel einfach nur ein Bild?

Mehr zu Fakeshops lesen Sie hier:

- Vorsicht: Fakeshops tarnen sich mit echten Personenangaben
- Fakeshop-Finder: So entlarven Sie sofort betrügerische Online-Shops
- Fakeshop-Finder: Gratis-Tool prüft Webshops und warnt vor Betrügern
- Polizei: So erkennen Sie betrügerische Fakeshops

Quelle: https://www.pcwelt.de/article/2236067/betrug-samsung-galaxy-s24.html

12) Betrug: Verbraucherzentrale warnt vor neuer Masche mit Fakeshops

Gefälscht Online-Shops sind eine beliebte Masche bei Kriminellen im Netz. Die Verbraucherzentrale Niedersachsen hat nun eine neue Variante für den Betrug in Fakeshops aufgedeckt und warnt vor ganz bestimmten Webadressen.

Die Verbraucherzentrale Niedersachsen hat in den vergangenen Tagen vermehrt Beschwerden über Fakeshops erhalten, die einem ganz bestimmten Muster folgen. Denn deren Webadresse ist immer gleich aufgebaut und daran ist der Betrug bereits zu erkennen.

Dabei ist es offenbar vollkommen unerheblich, um welche Produkte es sich in dem Online-Shop handelt. Denn hier sei von Spielwaren über Technik bis hin zu Tierbedarf alles dabei, teilt die Verbraucherzentrale mit.

Betrug in Fakeshops: Vorsicht bei diesen Webadressen

Die Verbraucherzentrale Niedersachsen weist darauf hin, dass die Adressen der Shops immer dem gleichen Muster folgen. Diese seien immer mit einem Vornamen und einem Nachnamen wie folgt aufgebaut: „Vorname-Nachname.Shop“.

Bereits mehrere solcher Kombinationen seien bereits aufgetreten, darunter „monika-jung.shop“, „peter-schneider.shop“ oder „frank-hildebrandt.shop“. Verbraucher:innen sollten auch deshalb bereits bei einer solchen URL aufhorchen, da den Shops der kriminelle Hintergrund oft nicht anzusehen ist.

Denn die Seiten an sich sehen laut der Verbraucherzentrale professionell aus und verfügen sogar über ein Impressum. Diese Angaben seien jedoch von woanders geklaut.

„Zurzeit fallen Fakeshops auf, die einem bestimmten Muster folgen“, erklärt Kathrin Bartsch von der Verbraucherzentrale Niedersachsen. Die Rechtsexpertin weist außerdem darauf hin: „Die Shops sind bei Google-Shopping gelistet. Auf den ersten Blick sehen sie professionell aus. Meist werben große Bilder für die angebotenen Produkte.“

> Wer das Muster kennt, kann sie jedoch recht einfach entlarven, zumal eine Umsatzsteuer-Identifikationsnummer fehlt und die Allgemeinen Geschäftsbedingungen immer im gleichen Stil geschrieben sind.

Dabei würden die Kriminellen manche Fakeshops schnell wieder offline nehmen. Andere wiederum seien länger im Netz verfügbar.

So kannst du dich vor dem Betrug schützen

Doch die fehlende Umsatzsteuer-ID oder die auffälligen AGBs sind nicht die einzigen Mittel,

um den Betrug in den Fakeshops zu entlarven. Die Verbraucherzentrale weist ausdrücklich noch einmal auf ihren Fakeshop-Finder hin.

Hier kannst du eine URL einfach eingeben, diese wird dann vom Fakeshop-Finder geprüft. Über ein Ampelsystem erhältst du dann eine Einschätzung zu dem jeweiligen Shop.

Bei der URL zu dem Fakeshop „monika-jung.shop“ beispielsweise erhältst du eine rote Ampel und den Hinweis, dass die URL Anzeichen für einen Fakeshop aufweist. Außerdem bekommst du diverse Gründe für diese Entscheidung mitgeteilt.

Tipp: https://www.verbraucherzentrale.de/fakeshopfinder-71560

Quelle: https://www.basicthinking.de/blog/2024/02/14/fakeshops-betrug/

13) Betrug per Fake-Support – LKA warnt vor neuem Betrug bei Kleinanzeigen

Immer wieder nutzen Betrüger das Verkaufsportal Kleinanzeigen für ihre Machenschaften. Nun warnt das LKA Niedersachsen vor einer besonders gefährlichen Masche.

Ob Smartphone, alte Kommode oder "Teilchenbeschleuniger" – auf Kleinanzeigen (ehemals Ebay Kleinanzeigen) verkaufen und kaufen Menschen allerhand Gegenstände, die sie nicht mehr brauchen oder schon immer wollten. Doch beliebt ist die Verkaufsplattform nicht nur bei ehrlichen Usern. Auch Betrüger treiben auf Kleinanzeigen ihr Unwesen und versuchen Nutzerinnen und Nutzer um ihr Erspartes zu bringen oder sensible Nutzerdaten zu erbeuten. Regelmäßig warnen Verbraucherschützer und Ermittlungsbehörden deshalb vor den neusten Maschen der Kriminellen – so auch jetzt. Denn nun teilt das Landeskriminalamt Niedersachsen mit, dass Betrüger User des Dienstes derzeit durch eine besonders listige Methode zu Überweisungen verleiten wollen. Gefährdet ist demnach, wer auf Kleinanzeigen ein Angebot inseriert.

Betrug mit mehreren Stufen

Denn bei ihrem mehrschichtigen Vorgehen geben sich die Kriminellen zunächst als Interessent aus und kontaktieren Verkäufer über die Chatfunktion des Kleinanzeigen-Portals. Im Verkaufsgespräch geben sie an, die angebotene Ware kaufen und bezahlen zu wollen. Dazu benötigten sie lediglich die E-Mail-Adresse des Verkäufers. Teilt der Verkäufer die mit, behaupten die Betrüger im nächsten Schritt, die Zahlung sei getätigt worden, müsse aber noch durch den Verkäufer bestätigt werden. Dazu erhalte dieser in Kürze eine E-Mail des Kleinanzeigen-Supports. Tatsächlich trifft die schon kurz darauf ein – dahinter stecken in Wahrheit jedoch weiterhin die Betrüger. In der täuschend echt wirkenden Nachricht soll das Opfer über einen Link bestätigen, auf welches Konto der gezahlte Betrag überwiesen werden soll. Doch, Sie ahnen es schon, auch dieser Link ist gezinkt und führt das Opfer auf eine gefälschte Kleinanzeigen-Webseite.

Geld überwiesen, ohne es zu wissen

Dort wendet sich ein vermeintlicher Kleinanzeigen-Mitarbeiter samt falschem Namen und Foto per Live-Chat an User, um sie zur Eingabe ihrer Bankdaten zu verleiten. Dazu behaupten die Betrüger im Chat, dass zum Abschluss der Transaktion nur noch die Bankdaten über einen weiteren Link einzugeben seien und der Vorgang anschließend per TAN-Code bestätigt werden müsse. Leistet das Opfer dem Folge, heißt es, dass es ein Problem bei der Verifizierung der Bankkarte gegeben hätte. Der Vorgang sei zu wiederholen.

Ohne es zu wissen, löst das Opfer damit jedoch jedes Mal aufs neue eine Überweisung an die Betrüger aus, statt selbst Geld zu erhalten. Mehrere beispielhafte Screenshots, die das LKA Niedersachsen in seiner Warnung veröffentlicht, zeigen das mehrschichtige Vorgehen.

Das ist im Betrugsfall zu tun

Geschädigten dieses Betrugs empfiehlt das LKA Niedersachsen, sich umgehend bei ihrer Bank zu melden, um die ungewollten Abbuchungen bestenfalls noch zu stoppen. Zudem sind Beweise gefragt: Sammeln Sie Screenshots, den Chatverlauf, Mails und Kontoauszüge mit den Betrügerkonten und erstatten Sie Anzeige. Das ist sowohl bei der örtlichen Polizeidienststelle als auch über die zuständige Online-Wache der Polizei möglich. Darüber hinaus erläutert das LKA, dass ein seriöser Kundensupport User niemals zur Eingabe von Passwörtern, PIN- oder TAN-Codes auffordern würde, um eine Aktion zu bestätigen. Außerdem sei es hilfreich, Zahlungsoptionen bereits vorab und direkt über die offizielle Webseite der jeweiligen Verkaufsplattform zu definieren. Sollten Sie hingegen per Chat oder E-Mail zur Einrichtung ihrer Kontodaten aufgefordert werden, sollten Sie die Transaktion umgehend abbrechen. Mit welchen Methoden Betrüger außerdem Jagd auf sensible Daten machen und wie Sie sich effektiv davor schützen, erfahren Sie in unserem umfassenden Phishing-Ratgeber. Tipps und Tricks rund ums Inserieren und Kaufen bei Kleinanzeigen finden Sie in diesem Ratgeber.

Quelle: https://www.computerbild.de/artikel/cb-News-Sicherheit-LKA-warnt-vor-neuem-Betrug-bei-Kleinanzeigen-37975819.html

14) Offline-Trick funktioniert noch immer: So sichern Sie Ihr Konto ab

Ein einfacher Trick erlaubt es Betrügern seit vielen Jahren, Geld von fremden Konten ins Ausland zu überweisen. Verhindern lässt sich dies mit einer simplen Sperre bei der Bank.

Geht es um Betrug beim Bankkonto, denken viele heute zuerst ans Online-Banking. Doch obwohl Cyberkriminalität weiterhin ein großes Risiko bleibt, sollten auch Offline-Betrugsmaschen nicht unterschätzt werden.

So können Kriminelle mit einer altmodischen Methode auch heute noch Ihre Ersparnisse recht einfach ins Ausland überweisen. Wir zeigen Ihnen, wie Sie sich **davor absichern** können und ob Sie im Ernstfall Ihr Geld zurückbekommen.

Überweisung per Beleg: So einfach geht das

Hacking, Phishing, Social Engineering – nichts davon ist beim Betrug mit der **beleghaften Überweisung** notwendig. Hier werfen die Täter einfach einen Überweisungsträger in Papierform bei der Bank ein.

So überweisen diese sich einfach selbst Geld von Ihrem Konto auf das eigene. Das liegt oft im Ausland, um die Spuren leichter zu verwischen. Für diese Masche brauchen die Betrüger also keinen ausgefeilten Plan, sondern **nur drei Dinge**:

- Ihren Namen
- IBAN und BIC
- Eine Unterschrift

Am schwierigsten nachzumachen ist wohl die Unterschrift, aber die Betrüger müssen diese noch **nicht einmal fälschen**. Aber warum fällt so etwas nicht auf?

Ein Grund dafür könnte sein, dass die Banken nicht genügend Personal haben, um die Unterschriften zu prüfen – der Verbraucherschutz behauptet sogar:

"Bei kleinen Beträgen können Sie mit Micky Maus unterschreiben und kommen damit durch."

So schützen Sie sich vor dieser Betrugsmasche

Um sich vor dieser Betrugsmethode zu schützen, sollten Sie Ihre **Bankdaten äußerst sparsam herausgeben**. Dazu zählt auch, dass Sie Ihre Geldbörse immer an der Person tragen – zwei Fotos von Vorder- und Rückseite Ihrer EC-Karte liefern den Dieben alle nötigen Informationen.

Wenn Sie ohnehin Ihre Überweisungen nur noch Online oder an einem Schalter in der Bank tätigen, dann sollten Sie die **beleghaften Überweisungen sperren** lassen. Dadurch werden Überweisungsaufträge in Papierform von der Bank gar nicht erst bearbeitet.

Rufen Sie dazu bei Ihrem Geldinstitut an und informieren Sie sich über die Möglichkeiten. Die Sparkassen bieten diesen Schritt sogar direkt im Kundenkonto beim Online-Banking an. Überweisungen am Terminal in der Filiale sind dennoch weiterhin möglich.

Wenn das keine Option für Sie ist, **prüfen Sie Ihre Kontoauszüge** engmaschig, damit Ihnen der Betrug im Ernstfall schnell auffällt. Am besten schauen Sie mindestens einmal wöchtenlich danach.

So bekommen Sie Ihr Geld zurück

Es gibt eine gute Nachricht: Sollte so ein Betrugsversuch stattfinden, dann bekommen Sie in aller Regel **Ihr Geld zurück**. Die Banken sind dazu verpflichtet und dürfen auch keine Bearbeitungsgebühren dafür erheben – die Banken sind über einen Haftungsfonds versichert.

Lediglich bei unverwechselbar gefälschter Unterschrift können Sie auf den Kosten sitzen bleiben, wie das Landgericht Dessau 2014 urteilte.

Nicht nur Privatpersonen sind betroffen, sondern auch mittelständische und größere Unternehmen. Hier setzen die Betrüger darauf, dass diese zusätzliche Überweisung in der Buchhaltung nicht auffällt – hier müssen die Mitarbeiter entsprechend sorgfältig auf kleine Beträge schauen, die sich nicht zuordnen lassen. Sonst ist das Geld futsch.

Was tun Banken gegen diesen Betrug?

Einige Banken haben Maßnahmen gegen diese Betrugsform ergriffen. Unter anderem gibt es bei vielen Geldhäusern gar **keine Außenbriefkästen** mehr für Überweisungsträger.

Außerdem gibt es an einigen Standorten die Belege **nur noch am Schalter** von einem Mitarbeiter, sodass diese nicht mehr frei verfügbar in der Filiale herumliegen.

Bei größeren Summen prüfen die Mitarbeiter in Banken die Überweisungsträger zudem genauer, in manchen Instituten kommt auch Software zum Einsatz, die die Unterschriften prüft.

Darüber hinaus stellen Banken aber nur höchst selten Anzeige gegen die Betrüger. Oftmals werden nur kleine Beträge überwiesen, die dann in der Summe lukrativ sind – die Strafverfolgung wäre allerdings zu aufwändig.

Laut der Deutschen Kreditwirtschaft werden in Deutschland rund 6,7 Milliarden Überweisungen beleglos durchgeführt – dagegen nur rund **370 Millionen mit Beleg**, Tendenz sinkend. Zur Häufigkeit der Betrugsfälle mit Belegen wollte sich keine der von uns angefragten Banken äußern.

Quelle: https://www.chip.de/news/Offline-Trick-funktioniert-noch-immer-So-sichern-Sie-Ihr-Konto-ab_184693795.html

15) Ransomware-Bande Lockbit zerschlagen – oder auch nicht

Unter der Leitung von Europol haben internationale Ermittlungsbehörden Server der Ransomware-Gruppe Lockbit beschlagnahmt und verdächtige Personen verhaftet. Weitere Täter werden noch per Haftbefehl gesucht. Unklar bleibt, ob dies wirklich das Ende für Lockbit bedeutet.

Am Anfang dieser Woche haben zehn internationale Strafverfolgungsbehörden, darunter auch solche aus Deutschland, die Kontrolle über die Darknet-Seiten der Ransomware-Bande Lockbit übernommen. Diese mutmaßlich russische Bande bietet Ransomware-as-a-Service an, also Software und Infrastruktur als kostenpflichtige Dienstleistung für andere Online-Kriminelle. In Polen und der Ukraine wurden Verdächtige verhaftet.

Die Ermittler haben bei der „Operation Cronos“ offenbar die seit November 2023 bekannte PHP-Schwachstelle CVE-2023-3824 ausgenutzt, um letztlich 34 Lockbit-Server in Europa, Australien und den USA zu übernehmen. Dabei sind ihnen auch Tools und Schlüsseldaten in die Hände gefallen, mit denen verschlüsselte Dateien auf den Rechnern der Opfer wieder entschlüsselt werden können. Auch etliche Krypto-Wallets der Kriminellen haben die Strafverfolger dabei beschlagnahmt.

In Polen und in der Ukraine sind zwei Personen verhaftet worden, die wahrscheinlich Lockbit-Kunden sind. Diese sogenannten Affiliates betätigen sich als Erpresser und nutzen dazu die bereitgestellten Tools und Dienste der Lockbit-Bande. Zudem ist in den USA Anklage gegen zwei Russen erhoben worden, die noch nicht gefasst wurden. Weitere Informationen aus der Operation Cronos wollen die Behörden in den nächsten Tagen schrittweise veröffentlichen, auch die Identitäten mutmaßlicher Lockbit-Köpfe, die noch auf freiem Fuß sind.

Während dieser Schlag gegen die weltweit produktivste Ransomware-Bande fraglos ein großer Erfolg ist, kommen doch Zweifel auf, ob dies wirklich das Ende der Lockbit-Gruppe bedeutet. Mitglieder der Gruppe behaupten, sie verfügten noch immer über Backup-Server, die den Behörden nicht in die Hände gefallen seien. Chester Wisniewski, Global Field CTO bei Sophos, schätzt, dass ein erheblicher Teil der Lockbit-Infrastruktur noch immer unter der Kontrolle der Kriminellen ist. Doch jeder behördliche Erfolg, der die Handlungen der Täter störe und das Misstrauen unter ihren Partnern erhöhe, sei ein großer Gewinn.

Die japanische Polizei hat inzwischen ein Entschlüsselungsprogramm (Decryptor) erstellt, mit dem die Opfer der Lockbit-Ransomware ihre verschlüsselten Dateien wieder entschlüsseln können. Es steht auf der Website „No More Ransom“ unter dem Eintrag „Lockbit 3.0 Ransom“ zum Download bereit.

Tipp: Erpresser-Viren: Wie Sie sich schützen
Die gefährlichste Malware des Jahres 2023

Quelle: https://www.pcwelt.de/article/2242917/ransomware-bande-lockbit-zerschlagen-oder-auch-nicht.html?utm_date=20240227141623&utm_campaign=Security&utm_content=Title%3A%20Ransomware-Bande%20Lockbit%20zerschlagen%20%E2%80%93%20oder%20auch%20nicht&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

Anwenderinformationen:

1) Apps unbrauchbar gemacht: Amazon blockiert heimlich Fire-TV-Funktion

Einige Apps für Fire TV funktionieren nicht mehr. Der Grund: Amazon blockiert Grundfunktionen des Betriebssystems.

Amazon hat mit einem Update für mehrere Fire-TV-Modelle das Betriebssystem geändert und macht damit einige Apps unbrauchbar, wie das Fire-TV-Blog AFTVNews berichtet. In Fire OS wurde die Möglichkeit für Apps blockiert, lokale ADB-Verbindungen aufbauen und dann ADB-Befehle ausführen zu können.

Damit werden alle Fire-TV-Apps unbrauchbar gemacht, die ADB-Funktionen lokal auf Fire-TV-Geräten nutzen. ADB steht für Android Debug Bridge und ist ein Hilfsprogramm zum Debugging und wird aber auch für Funktionen verwendet, die sonst nicht ohne weiteres zur Verfügung stehen. Für die Nutzung von ADB müssen die Entwickleroptionen auf dem Gerät aktiviert werden.

Das Blog kritisiert, dass Entwickler solcher Apps von Amazon nicht im Vorfeld informiert wurden. Selbst nach der Abschaltung der Betriebssystemfunktionen wurden App-Entwickler nicht über diesen Schritt informiert.

Auswirkungen auf Apps für Fire TV

Nach Informationen des Blogs wurden Geräte mit Fire OS 7 und Fire OS 8 bereits aktualisiert, so dass die Geräte Fire TV Stick, Fire TV Stick 4K, Fire TV Stick 4K Max sowie Fire TV Cube von diesen Änderungen betroffen sind. Es ist nicht bekannt, ob auch ältere Fire-TV-Modelle mit Fire OS 6 oder Fire OS 5 ein solches Update erhalten werden – das Blog geht davon aus, dass dies noch passieren werde. Fire-TV-Updates lassen sich nicht ohne weiteres verhindern, sondern werden automatisch installiert.

Die gesperrten ADB-Funktionen werden wohl nur von wenigen Fire-TV-Apps genutzt, aber wer eine der Apps bisher verwendet hat, kann diese eben nicht länger nutzen. In dem Bericht werden die Apps TDUK APP Killer und TDUK APP Cache Cleaner von TechDoctorUK genannt, die durch das Update des Betriebssystems quasi deaktiviert wurden.

Beide Apps verwenden lokale ADB-Verbindungen, um mit einem Tastendruck das Beenden aller laufenden Apps zu erreichen oder den App-Cache aller Apps zu löschen. Die beiden Apps funktionieren bereits seit einigen Tagen nicht mehr, es gab aber keine Erklärung dafür. Der Entwickler wurde von Amazon im Vorfeld nicht darüber informiert, dass die Funktionen des Betriebssystems gesperrt wurden. Es ist derzeit nicht bekannt, welche weiteren Fire-TV-Apps von den Einschränkungen betroffen sind.

Amazon hielt Informationen zurück

Erst nachdem sich das Blog eingeschaltet und bei Amazon nachgefragt hatte, räumte das Unternehmen ein, dass diese ADB-Funktionen im Betriebssystem gesperrt wurden. Im Vorfeld wurden App-Entwickler nicht informiert; auch Besitzer von Fire-TV-Geräten erhalten von Amazon keine Informationen.

Der Betreiber des Blogs hat vor einigen Jahren bei Amazon für kurze Zeit als Produktmanager für Fire-TV-Geräte gearbeitet. Damals habe es bei Amazon klare Regeln gegeben, dass solche grundlegenden Änderungen am Betriebssystem nicht gemacht werden, ohne Entwickler frühzeitig darüber zu informieren und diesen auch Hilfe bei Problemen anzubieten, damit die Apps nicht einfach nicht mehr funktionieren.

Amazon nennt erhöhte Sicherheit als Grund

Die betreffenden Funktionen gab es seit zehn Jahren mit dem ersten Fire-TV-Gerät, das Amazon auf den Markt gebracht hatte. Die Streichung der Funktionen begründet das Unternehmen mit einer höheren Sicherheit. Nach Informationen des Blogs habe kein anderer Hersteller jemals die Notwendigkeit gesehen, die ADB-Funktionen blockieren zu müssen.

Das Blog hält die erhöhte Sicherheit für vorgeschoben und vermutet, dass Amazon damit stattdessen alternative Startbildschirm-Apps alias Launcher verhindern will. Er verweist darauf, dass bei allen ADB-Funktionen vorher ein deutlicher Warnhinweis auf dem Bildschirm erscheint, um diese Befehle ausführen zu lassen.

Nach den Updates soll es weiterhin möglich sein, ADB-Verbindungen von einem Computer oder Smartphone zu einem Fire-TV-Geräte herzustellen.

Quelle: https://www.golem.de/news/apps-unbrauchbar-gemacht-amazon-blockiert-heimlich-fire-tv-funktion-2402-182569.html?utm_source=flipboard&utm_content=topic%2Fde-digital

2) Systemschäden vermeiden – Malware entfernen: So klappt's unter Android

Viren sorgen nicht nur auf PCs für Probleme. Auch für Android ist inzwischen allerhand Malware in Umlauf, die Sie besser schnell beseitigen.

Um solche schädlichen Programme kostenlos zu erkennen und zu löschen, benötigen Sie nicht immer eine zusätzliche App. Google bietet mit Google Play Protect selber eine Sicherheitssoftware an, die auf modernen Android-Smartphones bereits vorinstalliert ist.

So entfernen Sie kostenfrei Malware in Android

Google Play Protect sucht im Hintergrund permanent nach mit Malware verseuchten Android-Apps, um diese zu beseitigen. Führen Sie die folgenden Schritte zur Installation des Programms aus:

1. Öffnen Sie auf Ihrem Mobiltelefon den "Google Play Store".
2. Tippen Sie oben rechts auf Ihr Profilbild und wählen Sie anschließend "Play Protect".
3. Das Zahnrad-Symbol auswählen, um die Einstellungen der Software zu öffnen.
4. Aktivieren Sie die Option "Apps mit Play Protect scannen".

Sofern Sie auch Apps verwenden, die nicht aus dem Google Play Store stammen, aktivieren Sie zusätzlich die Option "Erkennung schädlicher Apps verbessern". Damit erlauben Sie dem Dienst, die Apps für Analysezwecke an Google-Server zu übermitteln.

Virusinfektionen vorbeugen

Um Ihr Android-Smartphone grundsätzlich vor Viren zu schützen, empfiehlt es sich, die Systemsoftware stets auf dem neuesten Stand zu halten. Das funktioniert wie folgt:

1. Zuerst die "Systemeinstellungen" öffnen.
2. Navigieren Sie zu "Sicherheit & Datenschutz" > "System & Updates".
3. Prüfen Sie jeweils, ob unter "Sicherheitsupdates" oder "Google-Play-Systemupdate" neue Aktualisierungen verfügbar sind und installieren Sie diese gegebenenfalls.

Achten Sie außerdem darauf, dass Sie allgemein keine Links von unbekannten Absendern anklicken und keine Apps oder andere Dateien aus unseriösen Quellen herunterladen.

Alternative Möglichkeiten

Beachten Sie, dass Google Play Protect, ebenso wie jede andere Sicherheitssoftware, nicht sämtliche Android-Malware erkennt und entfernt. Haben Sie nach den obigen Maßnahmen noch immer das Gefühl, einen Virus auf Ihrem Smartphone zu haben, helfen diese Schritte weiter:

- Installieren Sie eine alternative Sicherheitssoftware und scannen Sie damit Ihr System. Lösungen gängiger Hersteller wie Avira, AVG oder Bitdefender finden Sie im Google Play Store.
- Das Mobiltelefon auf die Werkseinstellungen zurücksetzen. Beachten Sie jedoch, dass dabei sämtliche auf dem Gerät gespeicherten Daten verloren gehen. Legen Sie daher zuvor eine Datensicherung an.
- Kontaktieren Sie gegebenenfalls den Support des Herstellers Ihres Smartphones.

Ziehen Sie, wenn nötig, auch ausgebildetes IT-Fachpersonal zurate. Dieses kann Ihnen helfen, Schadsoftware auf dem Smartphone zu beseitigen.

Tipp:

- Smartphone-Sicherheit: Phishing: WhatsApp-Link geöffnet – was tun?
- Malware stoppen: iPhone vor Viren schützen: So geht's
- Stiftung Warentest: "Ein Muss für jeden Rechner": Antivirenprogramme im Test

Quelle: https://www.t-online.de/digital/smartphone/id_100332944/malware-entfernen-unter-android-so-klappt-s.html

3) Neuer Fotoschutz – WhatsApp: Das ändert sich beim Profilbild

WhatsApp-Nutzer können Profilfotos anderer Anwender nicht speichern. Jetzt verhindert der Dienst eine Möglichkeit, die Funktion zu umgehen.

Vor einigen Jahren hatte WhatsApp die Option entfernt, dass Nutzer die Profilbilder anderer Anwender herunterladen und speichern können. Jetzt gehen die Entwickler noch einen Schritt weiter. Wie das Portal "WABetainfo" berichtet, testet das Unternehmen derzeit eine Funktion, Screenshots – also Bildschirmaufnahmen – von Profilbildern zu unterbinden.

Nach der Installation der neuen Betaversion für Android (2.24.4.25) sei es nicht mehr möglich, Screenshots von Profilfotos zu machen, heißt es. Bei dem Versuch, eine Bildschirmaufnahme mit dem fremden Profilbild zu machen, erscheine ein Hinweis: "Can’t take a screenshot due to app restrictions" – ein Screenshot ist aufgrund von App-Einschränkungen nicht möglich.

Identitätsdiebstahl mit fremden Profilbildern

Mit der Funktion wolle WhatsApp das "unbefugte Teilen von Profilfotos verhindern" und die Privatsphäre seiner Nutzer schützen, schreibt "WABetainfo". Es seien Fälle bekannt, bei denen fremde Profilbilder für kriminelle Zwecke genutzt wurden. Zum Beispiel, um Nutzer zu belästigen oder Identitätsdiebstahl zu betreiben.

Eine Garantie, dass die Funktion im kommenden offiziellen Update für WhatsApp zur Verfügung steht, gibt es nicht. Da Funktionen aus den Betaversionen von WhatsApp normalerweise übernommen werden, ist es aber wahrscheinlich, dass die Funktion in den kommenden Wochen für alle Nutzer bereitgestellt wird. Ob die Option auch für iOS-Anwender kommt, ist nicht bekannt.

Seit Jahren ist WhatsApp der beliebteste Messenger hierzulande. Es gibt keine Werbung, die App ist statt an ein Profil an die Telefonnummer des Nutzers gebunden. Nachrichten sind mit Ende-zu-Ende-Verschlüsselung geschützt, was dafür sorgt, dass sie nur auf den Geräten der beteiligten Nutzer im Klartext sichtbar sind, aber nicht für den Dienst. Regelmäßig bringen die WhatsApp-Entwickler neuen Funktionen heraus.

Tipp:

- Messenger: WhatsApp hat eine neue Funktion
- Zweites Profil: Neue Funktion bei WhatsApp
- Erweiterter Trickbetrug: Warnung: Neue WhatsApp-Betrugsmasche

Quelle: https://www.t-online.de/digital/aktuelles/id_100349726/neue-whatsapp-funktion-das-aendert-sich-beim-profilbild.html

4) Fehlerhaftes Windows-Update verursacht Probleme: Nur eines hilft

Insgesamt hat Microsoft zwei fehlerhafte Windows-Updates herausgegeben. Sie sorgen für folgendes Problem.

Gleich zwei **Windows**-Updates machen aktuell Negativschlagzeilen. Nutzerinnen und Nutzer sehen sich mit mehreren Problemen konfrontiert. Zwar steht seitens Microsoft noch kein Update bereit, allerdings kannst du dir auf diese Weise selbst helfen.

Windows-Updates sorgen für Probleme

Mit den neuesten Updates KB5034763 für Windows 10 und KB5034765 für Windows 11 scheinen sich Probleme mit der Taskleiste zu häufen. Einige Nutzer*innen berichten von einer gänzlich verschwundenen Taskleiste, während andere feststellen, dass angeheftete Apps nicht mehr angezeigt werden oder Symbole im Infobereich (wie WLAN- oder Soundeinstellungen) fehlen.

Obwohl diese Fehler Microsoft bekannt sind, gibt es bisher keine offizielle Bestätigung oder Lösung seitens des Konzerns, wie Windows Latest berichtet.

Der einzige Lösungsansatz der aktuell für Betroffene bleibt, ist demnach die Deinstallation des Updates. Zwar berichten einige Nutzer*innen, dass eine Neuinstallation der Aktualisierung etwas gebracht habe, doch die sicherste und nachhaltigste Methode ist, das Update zu löschen, bis Microsoft einen Patch bereitstellt.

Update deinstallieren: So geht’s

Willst du das Update löschen, bis Microsoft mit einer Lösung aufwartet, befolge folgende Schritte:

- Rufe die Einstellungen deines PCs auf.
- Suche nach dem Punkt „Windows-Update“.
- Dort findest du die Option „Updateverlauf“.
- Hier kannst du nun das letzte Update löschen.
    - Stelle sicher, dass du das Update mit der Versionsnummer KB5034763 für Windows 10 oder KB5034765 für Windows 11 entfernst.
- Das System wird neu gestartet. Danach sollten die Probleme vorerst der Vergangenheit angehören.

Bist du bereits in der Update-Übersicht, solltest du prüfen, ob du das neuste Windows-Sicherheitsupdate geladen hast. Es schließt gleich 72 Sicherheitslücken.

Probleme mit dieser Aktualisierung scheint es obendrein keine zu geben.

Quelle: https://www.futurezone.de/digital-life/article529870/fehlerhaftes-windows-update-verursacht-probleme-nur-eines-hilft.html

5) WhatsApp: Ein neues Feature für alle

Viele haben sie noch nicht aktiviert. Wir erklären, warum jeder diese neue WhatsApp-Funktion aktivieren sollte.

WhatsApp bietet zwar immer mehr Möglichkeiten, die eigene Privatsphäre zu schützen, aber viele Optionen sind nicht von vornherein aktiviert und müssen manuell eingeschaltet werden.

Eine dieser Optionen steht seit kurzem Beta-Testern zur Verfügung und wird nun der breiten Öffentlichkeit zugänglich gemacht: Nutzer können nun ihren Online-Status vor anderen Nutzern verbergen, berichtet das Online-Magazin "SamaGame".

Ob Nutzer das komplette Datenschutzpaket aktivieren wollen, bleibt ihnen überlassen. Allerdings sollten Nutzer zumindest einstellen, dass nicht jeder WhatsApp-Nutzer auf das eigene Profil zugreifen kann, denn nur so können Überwachungsmethoden wie Stalker-Programme ausgehebelt werden.

So kann die neue WhatsApp-Funktion für mehr Datenschutz aktiviert werden:

Um die neue Funktion zu aktivieren, muss wie folgt vorgegangen werden:

- In WhatsApp oben rechts auf die drei Punkte gehen und Einstellungen öffnen.
- In der Rubrik Datenschutz auf "Zuletzt online/ Online" klicken.
- Unter "Wer kann sehen, ob ich online bin" "Wie Zuletzt online" auswählen.

Wenn in der Kategorie "Zuletzt online" die Option "Niemand" ausgewählt ist, kann niemand sehen, ob Sie gerade online sind.

Eine weitere Neuerung für den Datenschutz betrifft sich selbst löschende Nachrichten. Ab sofort ist es nicht mehr möglich, Screenshots von selbstlöschenden Nachrichten auf dem Handy zu machen, die Funktion ist gesperrt. Auf dem PC lässt sich diese Einschränkung nicht durchsetzen, daher hat WhatsApp die selbstlöschenden Nachrichten für die Desktop-Versionen einfach deaktiviert. Selbstlöschende Nachrichten sind also nur noch auf dem Handy-Postfach sichtbar.

Quelle: https://www.chip.de/news/Neue-Funktion-fuer-WhatsApp-Nutzer-die-Sie-auf-jeden-Fall-aktivieren-sollten_185135416.html

6) Nutzer müssen reagieren: Schwere Sicherheitslücken in vielen Druckern entdeckt

Canon-Nutzer sollten nun Sicherheitsvorkehrungen treffen, da in einigen Druckern Sicherheitslücken entdeckt wurden.

Bei den betroffenen Druckern handelt es sich um Multifunktions- und Laserdrucker von Canon, bei denen Sicherheitslücken entdeckt wurden. Einige Modelle sind anfällig für Denial-of-Service-Angriffe über das Internet, die dazu führen können, dass die SOHO-Drucker komplett lahmgelegt werden. Canon hat in einer Sicherheitsmitteilung seinen Kunden einige Hinweise gegeben, um das Risiko solcher Angriffe zu minimieren.

Die Sicherheitsmeldung von Canon ist recht knapp gehalten und enthält keine Angaben zur Risikoeinstufung. Es werden sieben Sicherheitslücken aufgeführt, jedoch wird kein CVSS-Wert angegeben. Die Schwachstellen sind jedoch mit CVE-Nummern aufgelistet, über die Details zu den Lücken sowie der CVSS-Wert ermittelt werden können. Der Wert beträgt für alle Lücken 9,8, was bedeutet, dass sie als "kritisch" eingestuft werden.

Betroffene Nutzer der Canon-Drucker sollten schnell handeln

Die betroffenen Geräte sind von Region zu Region unterschiedlich. In Europa sind die Serien i-SENSYS LBP673Cdw, C1333P, MF750C, MF754Cdw und C1333i und den Firmware-Versionen bis einschließlich v03.07 und älter betroffen.

Nutzer dieser Produkte sollten daher vorsichtig sein. Canon will auf seinen Support-Seiten aktualisierte Firmware-Versionen zur Verfügung stellen. Betroffene Kunden sollten diese installieren. Außerdem rät der Hersteller, den Druckern eine private IP-Adresse zuzuweisen. Zudem dazu empfiehlt er die Drucker mit einem Kabel- oder WLAN-Router zu betreiben. Diese Maßnahmen können helfen, da sie den Netzwerkzugriff einschränken.

Quelle: https://www.chip.de/news/In-vielen-Druckern-wurde-eine-schwere-Sicherheitsluecke-entdeckt-Nutzer-muessen-handeln_185139720.html

7) Samsung warnt vor schwerer Sicherheitslücke: Nutzer müssen jetzt dringend reagieren

Samsung-Nutzer müssen jetzt aufpassen. In einem beliebten Tool ist eine Sicherheitslücke aufgetaucht.

Samsung informiert aktuell über eine Sicherheitslücke in seinem Magician-Tool, das zur Verwaltung von internen und externen SSDs sowie anderen Speichermedien von Samsung dient. Die Gefahr wird als hoch eingestuft, da eine unzureichende Rechtekontrolle bei der Nutzung einer sogenannten Named Pipe festgestellt wurde.

Nutzer werden dringend dazu aufgefordert, die aktualisierte Version des Magician-Tools zu installieren, in der der Fehler behoben wurde. Das Unternehmen warnt offiziell in einer Sicherheitsmitteilung vor den Risiken. Betroffen ist die Version 8.0.0 für Windows.

Samsung Magician Tool: Diese Version sollten Nutzer jetzt installieren

Für Nutzer, die noch die Version 8.0.0 des Magician-Tools verwenden, steht die aktualisierte Version 8.0.1 zur Verfügung. Diese schließt die Sicherheitslücke und stellt die sichere Nutzung der Anwendung wieder her. Das Magician-Tool ermöglicht unter anderem das Aktualisieren der Firmware von Samsung SSDs und Speicherkarten, um wichtige Firmware-Updates zu installieren.

Um die Sicherheit des Systems zu gewährleisten, sollten Nutzer des Samsung Magician-Tools dringend das Update auf die Version 8.0.1 durchführen. Dies stellt sicher, dass die Sicherheitslücke geschlossen wird und das System vor potenziellen Angriffen geschützt ist. Nutzer sollten regelmäßig auf Updates prüfen und diese zeitnah installieren, um die Sicherheit ihrer Systeme zu gewährleisten.

Quelle: https://www.chip.de/news/Schwere-Sicherheitsluecke-bei-Samsung-Das-muessen-Nutzer-jetzt-beachten_185141483.html

8) iPhone-Trick: Sofort bessere Akku-Laufzeit – klappt bei jedem Modell

Viele wissen es gar nicht, aber mit nur einer Einstellung lässt sich das Durchhaltevermögen deines Apple-Smartphones deutlich optimieren. Probiere es selbst aus.

Egal wie leistungsfähig ein Smartphone ist, am Ende bleibt das Gerät immer abhängig von seinem Akku. Für Besitzer*innen eines **iPhones** ist immerhin ein **Trick** verfügbar, der schnell für Abhilfe sorgt, sollte sich die Batterie überraschend rasant entleert haben. Achtung: Er funktioniert nur bei Geräten, die über 5G-Technologie verfügen.

Praktischer iPhone-Trick: So hält die Batterie länger

Für den iPhone-Trick ist erstaunlich wenig nötig. In nur wenigen Schritten hilfst du damit deinem Akku auf die Sprünge. Und auch künftig sorgt die folgende Einstellung dafür, dass dein Smartphone länger durchhält. Alles, was du dafür tun musst, ist die folgende Einstellung vorzunehmen.

iPhone-Trick für längere Akku-Laufzeit

1. Öffne die Einstellungen-App.
2. Wähle „Mobilfunk“.
3. Gehe weiter zu den „Datenoptionen“.
4. Unter „Sprache & Daten“ findest du eine Auswahl verschiedener 5G-Einstellungen.
5. Setze dein Häkchen bei „5G automatisch“.

Hast du die entsprechende Option ausgewählt, wird 5G nur noch dann verwendet, „wenn die Batterielebensdauer dadurch nicht signifikant verringert wird“, wie es in den Einstellungen heißt. Alternativ kann du auch die Option „LTE“ wählen. Dann wird beim Verbindungsaufbau komplett auf die 5G-Technologie verzichtet.

Lesetipp: Von 2 iPhone-Einstellungen raten Experten ab

Weitere iPhone-Tricks

Willst du neben dem Akku auch dein Internetsignal stärken, kann eine andere Handy-Einstellung helfen. Sie funktioniert beim iPhone, aber auch bei anderen Geräten wie dem iPad. Apple selbst verrät übrigens von Zeit zu Zeit, welche iPhone-Tricks und versteckten Funktionen es noch gibt. Oft genug wissen Nutzer*innen gar nicht, was ihr Smartphone wirklich alles kann.

Quelle: https://www.futurezone.de/digital-life/article407813/iphone-trick-akku-batterie-laufzeit.html?utm_source=flipboard&utm_content=topic%2Fde-digital

9) Ihr Handy kann geortet werden: Diese 3 Methoden müssen Sie kennen

Fast jeder hat sein Smartphone immer in der Tasche dabei. Das ermöglicht es, dass Sie auf Schritt und Tritt verfolgt werden können – es sei denn, Sie stoppen das.

Wenn eine App nach Ihren Standortdaten fragt, mag das auf den ersten Blick normal erscheinen. Mit diesen Daten können Unbefugte Ihr Handy orten, und das sogar anonym.Auch wenn Ihr Handy geortet wurde, bedeutet das nicht unbedingt, dass Sie fahrlässig mit Ihren Daten umgegangen sind. Kriminelle nutzen verschiedene Methoden, um Mobiltelefone unbemerkt zu orten. Drei davon zeigen wir Ihnen hier.

Fremde orten Handys: Wie sie vorgehen

Smartphones sind heute ständige Begleiter. Hacker wissen, dass Sie persönliche und sensible Daten auf Ihren Geräten speichern. Um an diese Daten zu gelangen, kann die Handyortung hilfreich sein. Die anonyme Handyortung verrät vor allem Ihren ständigen Aufenthaltsort. Darüber hinaus können Hacker mithilfe von Spionagesoftware eine Vielzahl von Informationen aus Ihrem Smartphone auslesen.

Es gibt verschiedene Wege der anonymen Handyortung, um auf ein Telefon zuzugreifen:

1. Dienste zur Handyortung: Manche Dienste erlauben die Ortung von Handys nach Anmeldung. Dabei wird eine SMS an das zu ortende Smartphone gesendet, die von Ihnen beantwortet werden muss, um die Ortung zu aktivieren. Mobilfunkanbieter können auch über "stille SMS" Ihren Standort auf 100 Meter bestimmen, ohne Ihr Wissen.
2. Handyortung durch Apps: Dafür muss eine spezielle App installiert werden, die den Standort ermitteln kann.
3. Spionage-Apps: Diese Apps sind speziell zur Handyortung konzipiert, aber nicht als solche erkennbar und oft als andere Anwendungen getarnt. Sie sind schwer von Ihrem Smartphone zu entfernen. Achten Sie daher darauf, neue Apps nur aus vertrauenswürdigen Quellen zu installieren, am besten aus offiziellen App-Stores.

Wie funktioniert Handy-Ortung? Smartphones werden vor allem dann geortet, wenn Hacker Zugriff auf die GPS-Daten haben. Ihr Standort kann dann bis auf zehn Meter genau bestimmt werden.

Wissen Kriminelle zum Beispiel, dass Sie nicht zu Hause sind, dann könnten diese leichter bei Ihnen zu Hause einbrechen – das ist zwar kein sehr wahrscheinliches Szenario, aber durchaus möglich. Aber auch Ihnen nahestehende Personen könnten ein Motiv haben, Ihr Gerät zu orten.

Maßnahmen gegen Handy-Ortung

Beachten Sie, dass jede Handyortung ohne Zustimmung des Besitzers illegal ist und einen schweren Eingriff in die Privatsphäre darstellt. Nur die Polizei darf fremde Handys orten, und das auch nur in bestimmten Fällen, wie zum Beispiel bei der Aufklärung von Verbrechen oder bei der Suche nach gestohlenen Smartphones.

Es gibt verschiedene Maßnahmen, um sich vor Handyüberwachung zu schützen. Schon wenige Einstellungen können verhindern, dass jemand Ihr Handy ortet, etwa folgende:

- Standortfreigabe für jede App individuell bestimmen, keine Generalfreigabe erteilen
- Standortfreigabe nur dann erteilen, wenn das akut für die Nutzung einer App benötigt wird (zum Beispiel Google Maps)
- nutzen Sie unbedingt eine sichere Methode zum Entsperren des Handys, damit Fremde (oder Ihnen nahestehende Personen!) nicht einfach so Spionage-Apps auf Ihrem Gerät installieren können
- Möchten Sie gar nicht getrackt werden, hilft es nur, das Handy auszuschalten, dann wirken auch stille SMS vom Provider nicht

Achten Sie aber vor allem immer darauf, welche Berechtigungen die Apps verlangen, die Sie installieren wollen. Ist eine Standortfreigabe für die Funktion der Anwendung gar nicht nötig, dann sollten Sie skeptisch sein.

Quelle: https://www.chip.de/news/Ihr-Handy-kann-geortet-werden-Diese-3-Methoden-muessen-Sie-kennen_185121167.html

10) Einfach erklärt – WhatsApp-Trick: So finden Sie heraus, wer Ihre Telefonnummer gespeichert hat

Sie wollen herausfinden, wer Ihre Handynummer gespeichert hat? WhatsApp bietet eine Funktion, die eigentlich nicht dafür vorgesehen ist. So geht's.

WhatsApp ist der beliebteste Chat-Dienst hierzulande. Die Handy-Anwendung ermöglicht den Austausch von Nachrichten, Bildern oder Videos in nur wenigen Schritten. Manchmal stellt sich die Frage, wer von den Kontakten eigentlich die eigene Nummer gespeichert hat. Mithilfe der Broadcast-Funktion bei WhatsApp lässt sich genau das herausfinden.

Der Trick funktioniert so: Erstellen Sie eine neue Broadcast-Nachricht und wählen zunächst einen Kontakt aus, von dem Sie sicher wissen, dass dieser Ihre Nummer gespeichert hat.

Anschließend fügen Sie einen weiteren Kontakt hinzu, bei dem Sie sich unsicher sind, ob er Ihre Nummer gespeichert hat. Jetzt müssen Sie nur etwa zwei bis drei Stunden warten, um zu überprüfen, ob der zweite Kontakt Ihre Nachricht gelesen hat oder nicht.

Sollte der fragliche Kontakt unter "Gelesen von" aufgeführt sein, bedeutet das, dass er tatsächlich Ihre Handynummer gespeichert hat. Erscheint der Kontakt jedoch nur unter "Zugestellt an", so hat dieser Empfänger Sie vermutlich nicht in seiner Kontaktliste eingespeichert und konnte somit die Nachricht auch nicht lesen.

Sie sollten dabei aber beachten, dass einige Personen möglicherweise selten auf WhatsApp aktiv sind und daher mehr Zeit benötigen könnten, um die Nachricht zu lesen.

Hier die Vorgehensweise unter iOS und Android im Detail:

- Tippen Sie in WhatsApp unter iOS oben rechts auf das "+", unter Android auf die drei Punkte, und dann auf "Neuer Broadcast".
- Wählen Sie zwei Kontakte aus – einen, von dem Sie wissen, dass er Ihre Telefonnummer gespeichert hat, und einen, von dem Sie es wissen wollen.
- Tippen Sie oben rechts auf "Erstellen".
- Verfassen Sie eine Nachricht und versenden Sie die Mitteilung.
- Warte Sie einige Stunden, um den Kontakten ausreichend Zeit zum Lesen zu geben.
- Tippen Sie lange auf die versendete Nachricht und dann auf "Info".
- Ist der Kontakt unter "Gelesen von" aufgelistet, dann hat er Ihre Telefonnummer vermutlich gespeichert.
- Steht der Kontakt nur unter "Zugestellt an", dann höchstwahrscheinlich nicht.

Beachten Sie bitte: Sie und der Kontakt, von dem Sie wissen wollen, ob er Ihre Telefonnummer gespeichert hat, muss in den Einstellungen unter Datenschutz die Lesebestätigung aktiviert haben. Andernfalls sehen Sie nicht, ob Ihre Kontakte die von Ihnen versendeten Nachrichten gelesen haben.

Quelle: https://www.t-online.de/digital/aktuelles/id_100326874/whatsapp-trick-so-pruefen-sie-wer-ihre-nummer-gespeichert-hat.html

11) Ratgeber – Alle gespeicherten Passwörter auf dem Android-Handy anzeigen

Erfahren Sie, wie Sie mit wenigen Schritten auf Ihre gespeicherten Passwörter auf Ihrem Android-Handy zugreifen können.

Bei all den Diensten und Apps von heute ist es praktisch unmöglich, sich jedes einzelne Passwort zu merken. Zum Glück bietet Android eine nützliche Funktion, mit der Sie alle Ihre

Passwörter, die Sie in Apps und auf Webseiten verwendet haben, speichern und bei Bedarf sogar einsehen können. So geht’s.

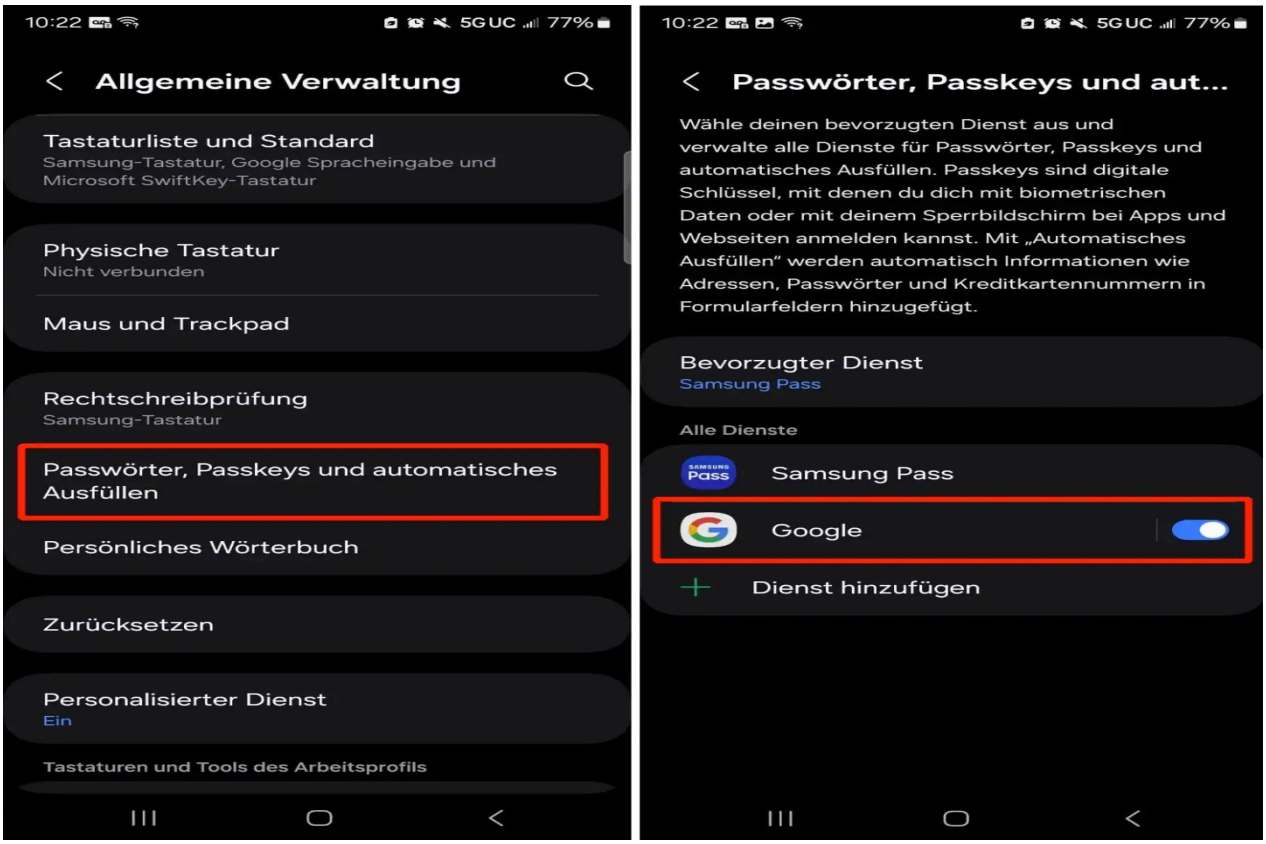
Gespeicherte Passwörter auf Android-Handy einsehen

Auf Google Pixel

- Öffnen Sie die „Einstellungen“.
- Wählen Sie den Menüpunkt „Passwörter und Konten“.
- Klicken Sie auf das Zahnradsymbol neben „Google“ und dann auf den Eintrag „Google Passwortmanager“.
- Im Passwortmanager wählen Sie den gewünschten Eintrag aus und bestätigen Ihre Identität, sei es per Passwort, Fingerabdruck oder Gesichtserkennung.
- Um das Passwort zu enthüllen, drücken Sie auf das „Auge-Symbol“ neben dem entsprechenden Account.

Auf Samsung-Smartphones

- Öffnen Sie die „Einstellungen“.
- Gehen Sie zu „Allgemeine Verwaltung“.
- Scrollen Sie nach unten zu „Passwörter, Passkeys und autom. Ausfüllen“.
- Tippen Sie auf Einstellungen von „Google“, um zum Passwortmanager zu kommen.
- Wählen Sie einen Eintrag aus und authentifizieren Sie sich mit Ihrem Passwort, Fingerabdruck oder Gesichtserkennung.
- Um das Passwort anzuzeigen, drücken Sie auf das „Auge-Symbol“.



Auf Samsung Handys finden Sie Ihre gespeicherten Passwörter unter “Allgemeine Verwaltung”. Bild: IDG

Alternativen

Nicht immer müssen Sie den Weg über die Einstellungen Ihres Smartphones nehmen. Eine weitere Möglichkeit, Passwörter einzusehen, besteht darin, direkt in die Übersicht Ihrer genutzten Konten zu gehen. Suchen Sie nach „Konten“ oder „Konten und Sicherung“, um Ihre Google-ID zu finden.

Wenn Sie auf Ihr Google-Konto tippen, gelangen Sie meist direkt in die Kontoübersicht. Im Bereich „Sicherheit“ finden Sie weiter unten den „Passwortmanager“, der alle im Account gespeicherten Passwörter auflistet.

Eine weitere universelle Lösung bietet die Webseite „passwords.google.com“. Nach der Anmeldung erhalten Sie Zugang zu all Ihren gespeicherten Passwörtern und können diese verwalten.

Quelle: https://www.pcwelt.de/article/2239437/gespeicherte-passworter-auf-android-handy-anzeigen.html?utm_date=20240227140047&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Alle%20gespeicherten%20Passw%C3%B6rter%20auf%20dem%20Android-Handy%20anzeigen&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

12) Online-Konto (scheinbar) gehackt: So gehen Sie vor

Wenn eine Website Ihre Anmeldedaten plötzlich nicht mehr akzeptiert, fällt der Verdacht schnell auf einen Hacker. Doch zunächst sollten Sie noch einige andere Optionen prüfen.

Es ist ein krimineller Angriff, unter dem zahlreiche Menschen zu leiden haben: Bei einer Umfrage der Verbraucherzentralen gaben 30 Prozent der Internetnutzer an, dass schon mindestens einmal einer ihrer Onlineaccounts gehackt wurde.

In 35 Prozent der Fälle handelte es sich um ein Konto bei einem sozialen Netzwerk, 27 Prozent der Betroffenen nannten dabei Facebook. Bei 28 Prozent der Opfer hackten die Kriminellen ein E-Mail-Konto, dahinter folgten Accounts bei Onlinemarktplätzen wie Amazon, Ebay oder Zalando sowie Onlinebanking-, Paypal- und Kreditkarten-Konten.

Die Auswirkungen reichen von ärgerlich bis hin zu dramatisch: Die Hacker benutzen beispielsweise Ihren Social-Media-Account, um in großem Stil Werbeanzeigen zu verbreiten, sie missbrauchen Ihr Konto als Spam-Schleuder oder bestellen in Ihrem Namen oder beziehungsweise auf Ihre Kosten Waren bei Online-Händlern. Was nun?

Erste Maßnahmen

Zunächst einmal gilt es, Ruhe zu bewahren. Denn die häufigste Ursache für diese Meldung ist immer noch ein Tippfehler. Wiederholen Sie also die Eingabe von Benutzernamen und Kennwort und versuchen Sie erneut, sich anzumelden.

Bei vielen Anmeldefenstern erscheinen die eingegebenen Zeichen im Passwortfeld in Form von schwarzen Punkten. Das soll die Gefahr reduzieren, dass andere Personen in der Nähe das eingetippte Kennwort mitlesen. Auf der anderen Seite wird so allerdings verhindert, dass Sie Ihre Eingabe kontrollieren können.

Oftmals besteht jedoch die Möglichkeit, dass Sie sich die eingegebenen Zeichen anzeigen lassen können. Dazu erscheint innerhalb des Passwort-Felds am rechten Rand ein schwarzes Auge, teilweise allerdings erst nach Eingabe des ersten Zeichens. Sobald Sie dieses Symbol anklicken, können Sie die eingetippten Zeichen erkennen und das Kennwort auf Tippfehler überprüfen.

Passwort vergessen

Immer mal wieder kommt es auch vor, dass ein Benutzer sein Passwort schlicht und einfach vergessen hat.

In diesem Fall ist zunächst einmal Vorsicht geboten: Viele Websites und Onlinedienste akzeptieren lediglich eine begrenzte Anzahl von falschen Eingaben. Teilweise sperren sie den Account nach mehreren Fehleingaben, in anderen Fällen geben sie das Eingabefeld nach jedem Versuch erst nach einem immer länger werdenden Zeitintervall wieder frei.

Wenn Sie also nach zwei oder drei erfolglosen Eingaben einigermaßen sicher sind, dass dies nicht das richtige Kennwort ist, sollten Sie keine weiteren Versuche starten. Überlegen Sie lieber noch einmal, ob Sie das Passwort vielleicht doch irgendwo notiert haben, und ansonsten setzen Sie das Kennwort zurück. Diese Möglichkeit bietet nahezu jeder Onlinedienst an.

Abhängig vom Anmeldeverfahren, geben Sie zu diesem Zweck entweder Ihren Benutzernamen oder Ihre E-Mail-Adresse an, und klicken auf einen Link, der beispielsweise „Kennwort zurücksetzen“ heißt. Üblicherweise bekommen Sie nach wenigen Minuten eine E-Mail mit einem temporären Kennwort, das Sie für eine einmalige Anmeldung nutzen können.

Sobald Sie sich auf diese Weise bei dem Dienst authentisiert haben, werden Sie aufgefordert, ein eigenes, neues Passwort zu definieren, das Sie von nun an für die Anmeldung nutzen. Dieses Verfahren verwenden Sie auch für den Fall, dass Ihr Account gehackt wurde. Mit der Einrichtung eines neuen Kennworts sperren Sie wiederum den Hacker aus.

Fehlerursache Passwort-Manager

Auch wenn Sie Ihre Kennwörter einem Passwort-Manager anvertrauen und die Software die Anmeldemaske automatisch ausfüllt, kann es passieren, dass ein Onlinedienst den Log-in verweigert. Das kann zum einen das Werk eines Hackers sein, der das Kennwort geändert hat.

Es ist aber auch möglich, dass der Passwort-Manager einfach nicht auf dem aktuellen Stand ist – beispielsweise, weil Sie Ihr Kennwort zurückgesetzt haben. War das Programm währenddessen aktiv, hat es die Änderung bemerkt. Falls Sie die Software jedoch deaktiviert hatten, konnte sie das neue Kennwort auch nicht speichern.

Ein anderes Problem taucht mitunter im Zusammenhang mit den integrierten Passwort-Managern der großen Browser auf. Falls Sie diese Funktion in Ihrem Browser nicht deaktivieren, läuft sie parallel zum Passwort-Manager eines Drittanbieters und bietet ebenfalls an, Anmeldedaten festzuhalten und bei Bedarf zur Verfügung zu stellen.

Dabei kann es geschehen, dass die beiden Manager nach einer Änderung des Kennworts unterschiedliche Zeichenkombinationen speichern. Beim Ausfüllen von Anmeldemasken kommt es in diesem Fall immer wieder zu Konflikten und Fehlermeldungen.

Um die Passwort-Manager von Chrome, Edge und Firefox zu deaktivieren, gehen Sie folgendermaßen vor:

Bei Chrome klicken Sie rechts oben auf die drei Punkte und rufen im Menü die „Einstellungen“ auf. Gehen Sie auf der nächsten Seite in der Menüleiste auf der rechten Seite auf „Autofill und Passwörter“ und wählen Sie in der Mitte „Google Passwortmanager“. Auf der folgenden Seite klicken Sie auf der linken Seite auf „Einstellungen“ und schalten in der Mitte die Option „Speichern von Passwörtern anbieten“ auf „Aus“.

Auch in Edge klicken Sie in einem ersten Schritt rechts oben auf die drei Punkte und wählen dann „Einstellungen“. Klicken Sie dann unter „Ihr Profil“ auf „Kennwörter“ und auf der

nächsten Seite oben auf „Einstellungen“. Deaktivieren Sie dann die Optionen „Speichern von Kennwörtern anbieten“ und „Autoausfüllen von Kennwörtern und Passwörtern“.

Bei Firefox führt der Weg zum Passwort-Manager über das Menüsymbol mit den drei horizontalen Strichen rechts oben und einen Klick auf „Einstellungen“. Wählen Sie dann auf der linken Seite „Datenschutz & Sicherheit“ und löschen Sie im Abschnitt „Zugangsdaten und Passwörter“ das Häkchen vor „Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen“.

Gehacktes Konto erkennen

Wenn Sie die beschriebenen Möglichkeiten überprüft haben, bleibt schließlich meist nur noch die Erkenntnis übrig, dass ein Hacker Ihr Konto übernommen hatten.

Oft verzichten die Kriminellen darauf, die Anmeldedaten zu ändern. Damit vermeiden sie, dass der Inhaber des Kontos misstrauisch wird, weil er sich selbst nicht mehr anmelden kann. So können sie noch einige Tage länger in seinem Namen Social-Media-Posts verfassen oder auf seine Kosten Streamingvideos schauen.

Hinweise darauf, dass sich jemand in einem Ihrer Accounts eingenistet hat, können beispielsweise Meldungen der Social-Media-Dienste über unzulässige Posts sein. Andere Indikatoren sind Mails, die auf Anmeldungen von bislang unbekannten Orten hinweisen oder Rücksetz-Codes für das Passwort anbieten, verdächtige Aktivitäten mit Geschenkkarten, oder, bei Onlineshops, nicht autorisierte Bestellungen sowie Bestellungen, bei denen Bezahlinformationen und Rechnungsdaten nicht übereinstimmen. Kontrollieren Sie daher in regelmäßigen Abständen den Status Ihrer Bestellungen.

Gehacktes Konto wiederherstellen

Professionelle Hacker, die Betrug im großen Stil betreiben, ändern hingegen nicht nur das Passwort, sondern, falls möglich, auch die E-Mail-Adresse, den Benutzernamen, die Postanschrift und weitere Daten. Es ist dann nicht mehr möglich, einfach das Passwort zurückzusetzen, um die Kontrolle über den Account zurückzugewinnen.

Viele Online-Dienste, darunter vor allem die großen Vertreter wie Microsoft, Google, Amazon und dergeleichen, halten für diese Fälle Assistenten bereit, die in mehreren Schritten Ihre Identität überprüfen und Ihnen wieder einen Zugang zu Ihrem Konto verschaffen.

Sie müssen dabei häufig umfassende Angaben zu Ihrer Adresse, zu Ihrem letzten sowie den vorangegangenen Passwörtern und Ihrem Wohnort machen. Einige Firmen verlangen auch die Beantwortung von zuvor definierten Sicherheitsfragen. Anschließend kann es ein bis zwei Tage dauern, bis ein Mitarbeiter Ihre Antworten überprüft und den Kontozugang wiederhergestellt hat. In der nebenstehenden Tabelle finden Sie Links, die zu den Wiederherstellungsassistenten einiger der wichtigsten Onlinedienste führen.

Sicheres Passwort wählen

Um zu verhindern, dass andere Personen sich bei Ihrem Konto anmelden oder es sogar übernehmen, sollten Sie verschiedene Vorsorgemaßnahmen treffen. Nach wie vor ist bei vielen Anwendern der größte Schwachpunkt ein unsicheres Passwort.

Beherzigen Sie bei der Wahl Ihres Kennworts daher folgende Regeln:

- Ein sicheres Passwort sollte heute mindestens 16 Zeichen lang sein
- Es sollte aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen
- Das Passwort darf nicht im Duden oder einem anderen Lexikon verzeichnet sein
- Benutzen Sie ein Kennwort niemals für mehrere Dienste

Verwenden Sie zum Erzeugen Ihrer Kennwörter am besten einen Passwort-Generator wie das Tool unter www.datenschutz.org/passwort-generator. Speichern und verwalten Sie Ihre Anmeldedaten mit einem Passwort-Manager wie beispielsweise Keepass oder Bitwarden. Diese Programme bringen fast immer auch einen Passwort-Generator mit.

Mit einem Passwort-Manager müssen Sie sich nur noch ein Master-Passwort merken. Dafür sollten Sie dann eine lange und hinreichend komplexe Zeichenkombination wählen. Ist das Tool aktiv – die meisten dieser Programme sind als Browser-Add-on ausgeführt –, füllt es bei bekannten Websites die Anmeldemaske selbsttätig aus und bietet bei neu besuchten Sites automatisch an, die Daten in seine Datenbank zu übernehmen.

Zwei-Faktor-Authentisierung einsetzen

Neben einem sicheren Passwort ist mittlerweile eine Zwei-Faktor-Authentisierung nahezu unverzichtbar. Sie kennen das Verfahren vermutlich schon vom Onlinebanking: Neben Benutzernamen und Kennwort müssen Sie auch noch den Inhalt eines SMS oder den in einer Smartphone-App angezeigten Code eintippen.

Zwar bietet auch eine Zwei-Faktor-Authentisierung keinen hundertprozentigen Schutz vor einem Kontodiebstahl, doch sie verringert drastisch die Wahrscheinlichkeit, dass es zu solch einer kriminellen Übernahme kommt. Nahezu alle großen Onlinedienste wie Microsoft, Google, Amazon bieten das Anmeldeverfahren heute an.

Welches der zweite Faktor für die Anmeldung sein soll, lässt sich in vielen Fällen einstellen. Einige Programme wie etwa Bitwarden unterstützen Windows Hello. Damit stehen Ihnen sämtliche Anmeldevarianten zur Verfügung, die Sie in den „Einstellungen“ von Windows unter „Konten –› Anmeldeoptionen“ eingerichtet haben, also etwa die Eingabe einer PIN, eine Gesichts- oder Fingerabdruckerkennung oder auch die Anmeldung mit einem Hardware-Sicherheitsschlüssel für den USB-Port, auch Fido2-Stick genannt.

Wenn Sie Ihre Anmeldung dagegen per Smartphone bestätigen, haben Sie oft die Wahl zwischen dem Auslesen eines Codes oder einer PIN in einer App und der Bestätigung Ihrer Identität über den Fingerabdruckscanner des Geräts.

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

Quelle: https://www.pcwelt.de/article/2244639/online-konto-gehackt-so-gehen-sie-vor.html?utm_date=20240227140831&utm_campaign=Security&utm_content=Title%3A%20Online-Konto%20%28scheinbar%29%20gehackt%3A%20So%20gehen%20Sie%20vor&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

13) Die besten Amiga-Spiele: Mehr als 13.000 Klassiker jetzt kostenlos spielen

Mehr als 13.000 kultige Programme aus den frühen Home-Computer-Zeiten kostenlos im Browser spielen. Das Internet Archive macht es möglich.

Amiga-Games kostenlos spielen: Bubble Bobble, Double Dragon, Leisure Suit Larry

Unglaublich, welche Spiele-Hits bereits zu Amiga-Zeiten (Mitte 1980ger bis frühe 1990ger-Jahre) aufgefahren wurden. Viele Spiele gingen in Serie und sind bis heute bekannt: Bubble Bobble, Double Dragon, Project X, Lemmings, Emerald Mine, Leisure Suit Larry, King's Quest, R Type, Marble Madness. Archive.org stellt die Amiga-Software auf deren Webplattform kostenlos und legal zum Abruf bereit.

Amiga-Games steuern: Keyboard, Gamepad, Maus

Gesteuert werden die angebotenen Amiga-Programme in der Regel mit dem Keyboard, manchmal auch bereits mit der Maus. Oft funktionieren hier die Spiele besser, wenn man sie in den Vollbild-Modus schaltet.

Leider klappt die Steuerung per Gamepad teilweise nicht, deswegen empfehlen wir Ihnen für den vollen Spiele-Genuss das Tool JoyToKey. Damit können Sie Keyboard-Tasten auf den Controller umlegen und so viel entspannter daddeln. Wenn Sie mit der Tastatur spielen wollen, aber die Tasten ungünstig belegt sind, können Sie diese mit SharpKeys umbelegen. Wir wünschen viel Spaß.

Amiga Games: Die besten Remakes zum Download

Viele der Spiele bei Archive.org funktionieren leider nicht wirklich gut und lassen sich nur sehr hakelig steuern. Komfortabler spielen Sie mit den herunterladbaren Versionen. Einige der Amiga Spiele stehen mittlerweile zum kostenlosen Download bereit. Wer es etwas moderner mag, kann außerdem gleich zu Remakes der Spiele-Klassiker greifen. Die besten Amiga Remakes stellen wir Ihnen in unserer Fotostrecke vor. Dort finden Sie auch die passenden Download-Links, um die Spiele herunterzuladen und sofort in die Retro-Gaming-Welt einzutauchen.

Quelle: https://www.chip.de/news/Die-besten-Amiga-Spiele-Mehr-als-13.000-Klassiker-jetzt-kostenlos-spielen_98053263.html?utm_source=chip_1001311&utm_medium=email&utm_campaign=1012001&utm_content=27.02.2024

14) Über 8.000 Tbyte-Browser Daten verkauft: Was Nutzer von Avast jetzt tun können

Die Security-Firma Avast zahlt in den USA eine Millionenstrafe, weil sie jahrelang unerlaubt Nutzerdaten weiterverkauft hat. Zwar ist das Unternehmen schon zurückgerudert, viele Nutzer dürften aber das Vertrauen verloren haben. Alternativen gibt es genug.

Avast ist eine bekannte und überaus beliebte Software-Marke. Vor allem die kostenlosen Virenscanner bieten starke Leistungen und werden oft empfohlen, auch von CHIP oder Stiftung Warentest. Doch die Leistung ist die eine Sache, das Geschäftsmodell hinter den Kulissen eine andere.

Letzteres basierte bei Avast teilweise auf dem Weiterverkauf von Nutzerdaten. Die amerikanische Handelskommission FTC (Federal Trade Commission) hat einen umfangreichen Bericht erstellt, in dem das Geschäftsgebaren von 2014 bis 2020 zerlegt wird und eine Strafe von 16,5 Millionen US-Dollar gegen Avast verhängt.

Die FTC prangert dabei vor allem die Doppelmoral von Avast an: Denn der Anbieter gab bei seinen Produkten explizit vor, Nutzer vor Verfolgung im Internet zu schützen, nur um dann selbst Browser-Daten zu sammeln und diese zu Geld zu machen. Das geschah im großen Stil, die Rede ist von über 8 Petabyte an Daten, die die Avast-Tochter Jumpshot gehortet haben soll.

Gegenüber CHIP erklärt Avast: Avast hat sich mit der FTC auf einen Vergleich geeinigt. Die Untersuchungen rund um die Weitergabe von Kundendaten durch Avast an das Tochterunternehmen Jumpshot, das Avast im Januar 2020 freiwillig aufgelöst hat, sind abgeschlossen. Wir sind unserer Mission verpflichtet, das digitale Leben von Menschen zu schützen und zu verbessern. Obwohl wir den Aussagen und der Darstellung der Fakten durch die FTC nicht zustimmen, sind wir froh, diese Angelegenheit beizulegen und freuen uns darauf, weiterhin unseren Millionen von Kunden auf der ganzen Welt weiterzuhelfen.

Avast-Software loswerden

Weiterhin heißt es von Avast mit Hinblick auf die aktuellen Produkte: Avast verkauft keine Verbraucherdaten, und die operativen Bestimmungen des Vergleichs stehen im Einklang mit den aktuellen Datenschutz- und Sicherheitsprogrammen des Unternehmens. Der Vergleich bezieht sich auf das Verhalten der Tochtergesellschaft Jumpshot, die Avast vor über vier Jahren freiwillig geschlossen hat.

Avast will das Thema also schnell abräumen, das ist aus Sicht des Unternehmens verständlich, schließlich ist Vertrauen speziell bei Sicherheits-Software eine wichtige Sache. Jedoch dürften viele Nutzer nicht bereit sein, sofort wieder zur Tagesordnung überzugehen. Die gute Nachricht: Es gibt jede Menge Alternativen zu Avast-Software, wenn Sie wechseln möchten.

Windows-Nutzer, die auf Avast-Software setzen, können den Virenschutz über die eingebaute Windows-Funktion entfernen. In diesem Fall übernimmt nach einem Neustart Windows Defender wieder das Ruder. Sie sind also weiterhin geschützt.

Sollte der Standardweg zum Entfernen nicht funktionieren, gibt es mit Avast Clear ein Zusatz-Programm, das den Virenscanner komplett vom System entfernt. Das klappt über den abgesicherten Modus von Windows.

Tipp: Avast Clear (Avast Deinstallations-Tool) https://www.chip.de/downloads/Avast-Clear-Avast-Deinstallations-Tool_49840395.html

Alternative Virenscanner nutzen

Ist Avast entfernt, wird Windows vom Defender geschützt und das ist ein solider Grundschutz. Unsere Bestenliste zeigt Alternativen auf. Besonders interessant ist Bitdefender, das eine sehr gute Bewertung erhalten hat.

Bei uns im Test war die Bezahl-Software Bitdefender Internet Security vertreten. Wer kein Geld ausgeben möchte, kriegt mit Bitdefender Antivirus Free aber auch die Möglichkeit, kostenlos einzusteigen. Kürzlich wurde die kostenlose Bitdefender-Variante auch von Stiftung Warentest empfohlen.

Auch Avast Secure Browser betroffen

Von der FTC werden neben den Virenscannern auch explizit die Browser-Erweiterungen sowie der Avast Secure Browser als Datensammler genannt. Auch diese Software lässt sich entfernen und durch Alternativen ersetzen.

Ein datensparsamer und sicherer Browser ist zum Beispiel Brave. Auch Firefox ist als Alternative denkbar, wenn man nicht direkt Chrome oder Edge nutzen möchte. Als Zweit-Browser kann man sich Tor Browser installieren, der die Anonymität seiner Nutzer über alles stellt.

Quelle: https://www.chip.de/news/Ueber-8.000-TByte-Browser-Daten-verkauft-Was-Nutzer-von-Avast-jetzt-tun-koennen_185163840.html

Allgmeines:

1) Schnell gemacht – Dieser Antrag erhöht Ihre Rente um 110 Euro im Monat

Für bestimmte Zeiten können Sie sich bei der gesetzlichen Rentenversicherung Beiträge gutschreiben lassen. Für wen das gilt und wie es funktioniert.

Die gesetzliche Rente fällt im Schnitt nicht besonders üppig aus. Nach Zahlen des Statistischen Bundesamts müssen mehr als sieben Millionen Rentner mit weniger als 1.250 Euro im Monat auskommen. Da dürfte jede Möglichkeit gelegen kommen, die Bezüge zu steigern.

Tatsächlich gibt es einen einfachen Weg, mehr aus Ihrer Rente herauszuholen – und das mit nur einem Antrag. Bis zu 110 Euro mehr pro Monat sind damit drin. Die Rede ist von der Anerkennung der Kindererziehungszeiten.

Rente steigern mit einem Antrag

Ist Ihr Kind 1992 oder später geboren, könnten Sie sich die ersten drei Jahre nach der Geburt bei der Deutschen Rentenversicherung gutschreiben lassen. Für früher geborene Kinder können zwei Jahre und sechs Monate anerkannt werden ("Mütterrente"). Bei Mehrlingsgeburten wird die Zeit entsprechend vervielfacht.

Wichtig: Sie müssen für die Anerkennung selbst aktiv werden, sonst zählen diese Zeiten nicht für Ihre Rente. Das Formular für den Antrag können Sie hier herunterladen. Haben Sie solch einen Antrag bereits gestellt, brauchen Sie dies nicht erneut zu tun. Ob Ihre Kindererziehungszeiten schon erfasst wurden, können Sie auch Ihrem Versicherungsverlauf entnehmen, der Ihnen erstmals zusammen mit Ihrer ersten Renteninformation zugestellt wird.

Sind Sie bereits mindestens 43 Jahre, hat Sie die Rentenversicherung zudem um eine sogenannte Kontenklärung gebeten, bei der Kindererziehungszeiten mit abgefragt werden. Lesen Sie hier, wie Sie Ihren Rentenversicherungsverlauf prüfen.

Ein Jahr Kindererziehung bringt knapp einen Rentenpunkt

Die Rentenversicherung rechnet Ihnen die Kindererziehung auf Antrag so an, als hätten Sie in dieser Zeit eigene Rentenbeiträge gezahlt. In einigen Fällen entsteht so überhaupt erst ein Rentenanspruch. Denn für die gesetzliche Rente müssen Sie mindestens fünf Jahre lang Beiträge geleistet haben.

"Kindererziehungszeiten sind Pflichtbeiträge, die sich direkt auf Ihre Rentenhöhe auswirken", teilt die Deutsche Rentenversicherung mit. "Für die Zeit der Kindererziehung werden Sie in etwa so gestellt, als hätten Sie Beiträge aufgrund des Durchschnittsverdienstes aller Versicherten gezahlt."

Das bedeutet: Sie bekommen für ein Jahr Kindererziehungszeit knapp einen Rentenpunkt gutgeschrieben. Und der bringt Ihnen aktuell 37,60 Euro Rente pro Monat (Stand: Januar 2024). Bei bis zu drei möglichen Erziehungsjahren hätten Sie also eine um etwa 110 Euro höhere monatliche Rente. Haben Sie mehr Kinder, steigt die Rente entsprechend weiter.

Achtung: Kindererziehungszeiten kann immer nur ein Elternteil zur selben Zeit in Anspruch nehmen. Erziehen Sie Ihr Kind gemeinsam, hat grundsätzlich die Mutter Anspruch auf die Kindererziehungszeit. Soll sie der Vater erhalten, benötigt die Rentenversicherung eine gemeinsame Erklärung. Sie kann allerdings nur für maximal zwei Monate rückwirkend gelten. Das Formular können Sie hier herunterladen.

Nicht nur leibliche Eltern profitieren

Bei gleichgeschlechtlichen Eltern erhält der leibliche Elternteil die Erziehungszeit. Sind beide Elternteile nicht die leiblichen Eltern, hat derjenige Anspruch auf die Kindererziehungszeiten, der das Kind zuerst adoptiert hat. Trifft auch das nicht zu, teilt sich die Elternzeit zu gleichen Teilen im monatlichen Wechsel auf.

Kindererziehungszeiten gelten außer für leibliche und Adoptiveltern auch für Pflegeeltern und Stiefeltern. Auch Großeltern oder andere Verwandte können sich diese Zeiten anerkennen

lassen, wenn das Kind bei ihnen dauerhaft als Pflegekind in häuslicher Gemeinschaft wohnt.

Quelle: https://www.t-online.de/finanzen/ratgeber/altersvorsorge/gesetzlicherente/id_100326186/kindererziehungszeiten-antrag-erhoeht-die-rente-um-110-euro-im-monat.html

2) Neue Regeln für Überweisungen – Diese Bankgebühren werden abgeschafft

Manche Überweisungen dauern bis zu drei Tage. Für eine Expressüberweisung hingegen wird eine Zusatzgebühr fällig. Die EU will das nun ändern.

Gute Nachrichten für alle Bankkunden: Bald ist Schluss mit Zusatzgebühren für Echtzeit-Überweisungen. Die EU-Länder billigten am Montag in **Brüssel** abschließend eine Verordnung, die solche Sofortzahlungen in Euro ermöglicht.

Genauer heißt es darin, dass Banken für Sofortüberweisungen, sogenannte Instant Payments oder Echtzeitüberweisungen, künftig keine Zusatzgebühren mehr verlangen dürfen. Sofortüberweisungen dürfen danach nicht mehr kosten als Standardüberweisungen, die in der Regel kostenlos sind. Die neuen Regeln sollen ab Herbst 2025 gelten.

Mehr Verbraucherschutz auch für Standardüberweisungen

Die Verordnung über Sofortüberweisungen soll es den in der EU lebenden Menschen ermöglichen, zu jeder Tageszeit, auch außerhalb der Geschäftszeiten, innerhalb von zehn Sekunden Geld zu überweisen, und zwar nicht nur innerhalb desselben Landes, sondern auch in einen anderen EU-Mitgliedstaat. Die anfallenden Gebühren dürfen nicht höher sein als die Gebühren für Standardüberweisungen.

Damit eine Sofortüberweisung nicht beim falschen Empfänger landet, müssen die Anbieter nach den neuen Vorschriften in Zukunft überprüfen, ob IBAN und Name des Empfängers übereinstimmen. Damit sollen Verbraucher vor einer Überweisung auf mögliche Fehler oder Betrug hingewiesen werden. Gleiches soll für Standardüberweisungen gelten. Die Verordnung berücksichtigt die Besonderheiten von Unternehmen außerhalb des Euroraums.

Auch Paypal wäre betroffen

Nach Informationen von "Focus" wären nach den neuen Regelungen auch digitale Zahlungsanbieter betroffen. Paypal-Nutzer zahlen beispielsweise für Sofortüberweisungen eine Gebühr in Höhe von einem Prozent des Überweisungsbetrages, aber mindestens 0,25 Euro und maximal zehn Euro.

Eine Standardüberweisung ist bei Paypal zwar kostenlos, aber die Bearbeitungszeit beträgt zwischen einem und drei Werktagen. Die Pressestelle des Europarates teilte auf Anfrage von "Focus" mit, dass Instant Payments für Zahlungsanbieter im Euroraum gelten. Damit sei auch Paypal betroffen, berichtet der "Focus".

Stärkung des europäischen Wettbewerbs im Zahlungsverkehr

Die neuen Regeln gelten als weiterer Schritt der Ländergemeinschaft, um europäische Anbieter im Zahlungsverkehr gegen die großen US-Konzerne Visa und Mastercard im Wettbewerb zu stärken. "Die neuen Regeln werden die strategische Autonomie des europäischen Wirtschafts- und Finanzsektors verbessern, da sie dazu beitragen werden, übermäßige Abhängigkeiten von Finanzinstituten und Infrastrukturen in Drittländern zu verringern", erklärte der Rat in Brüssel.

Das neue Gesetz soll bis April in Kraft treten und greift dann nach einer Übergangsfrist von 18 Monaten, also voraussichtlich im Herbst 2025. In Ländern, in denen nicht der Euro als

gesetzliches Zahlungsmittel gilt, soll die Neuerung ab 2027 für Überweisungen in Euro und ab 2028 für solche in den jeweiligen Nationalwährungen gelten.

Quelle: https://www.t-online.de/finanzen/aktuelles/verbraucher/id_100352980/sofortueberweisungen-bald-kostenlos-eu-beschliesst-neue-regeln-fuer-banken.html

3) Verbraucherzentrale – Sammelklage gegen Extraenergie eröffnet

Im Jahr 2022 sind die Energiekosten allgemein nach oben geschnellt. Ein Unternehmen erhöhte im Sommer so drastisch, dass es eine Sammelklage gab. Betroffene können sich nun daran beteiligen.

Wer im Sommer 2022 bei einem Anbieter wie ExtraEnergie, Extragrün, HitEnergie oder Prioenergie von drastischen Preiserhöhungen betroffen war, kann sich ab sofort kostenlos in ein Klageregister eintragen. Darauf weist der Verbraucherzentrale Bundesverband (vzbv) hin.

Damals hatte die ExtraEnergie Gmbh, zu der diese Anbieter gehören, die Preise für Strom und Gas teils verdoppelt und verdreifacht, sogar trotz geltender Preisgarantien. Mit der Sammelklage beim Oberlandesgericht Hamm sollen betroffene Kunden und Kundinnen Rückzahlungen erhalten. Je nach Fall könnten das laut dem Verband mehrere Tausend Euro sein.

So geht es mit der Klagebeteiligung: Online kann geprüft werden, ob der eigene Fall zu der Klage passt (**www.sammelklagen.de/extraenergie/klage-check**). Anschließend folgen konkrete Hinweise für das Eintragen. Auch wenn das Verfahren dauert, verjähren mit dem Eintrag die Ansprüche nicht.

Quelle: https://www.t-online.de/heim-garten/aktuelles/id_100353244/sammelklage-gegen-extraenergie-eroeffnet-so-koennen-sie-sich-anmelden.html

4) Probleme mit dem Infotainment – Wenn die Elektronik spinnt: Seat, Skoda, Audi, VW

Das Navi fällt aus, die Heizung schmiert ab. Das Infotainmentsystem des VW-Konzerns bereitet Autobesitzern riesige Probleme. Doch Werkstätten können die Fehler oft nicht beheben.

Häufig geht im Auto von Theo Schornstein gar nichts mehr. **Navi, Telefon, Radio, Heizung, Klimaanlage, Einparkhilfe** – alle Funktionen hängen am Infotainmentsystem seines Seat Ibiza. Doch das funktioniert oft nicht.

Der Ärger begann im November 2022. Da hatte Theo Schornstein den Ibiza seit gerade mal drei Monaten geleast. „Selbst vor der Haustür hat das Gerät nicht erkannt, dass ich zu Hause bin“, berichtet Theo Schornstein. Der Bildschirm habe sich nicht mehr bedienen lassen. Schornstein **reklamiert** den Mangel schriftlich. Der Wagen kommt in die **Werkstatt** – doch das Problem kann dort **nicht behoben** werden.

Software-Update verschlimmert die Probleme

Erst ein halbes Jahr später wird ein **Software-Update** aufgespielt. Die Probleme sind dadurch allerdings nicht beseitigt, im Gegenteil. Es sei zu immer mehr Navi-Ausfällen gekommen, erzählt Schornstein. Das Radio sei teilweise nicht nutzbar gewesen und wenn man den Schlüssel abgezogen habe, sei das Infotainment angeschaltet geblieben.

Viele VW-Marken von Elektronikproblemen betroffen

Theo Schornstein ist mit seinem Problem nicht allein. Im Internet finden sich jede Menge Beschwerden frustrierter Autobesitzer, die mit Infotainmentproblemen zu kämpfen haben. Nicht nur bei Seat.

Die Probleme gibt es auch bei anderen Marken aus dem VW-Konzern: **Skoda,** Audi, **Volkswagen**. Alle nutzen das gleiche Elektronik-System, den „Modularen Infotainment-Baukasten“ MIB. Und der fällt immer wieder aus: Monitore frieren plötzlich ein oder springen gar nicht erst an - oder sie fangen im Betrieb an zu flimmern.

Branchenexperte: Autos werden immer mehr zum Computer

Automobilwissenschaftler und Branchenexperte Stefan Bratzel hat dafür eine Erklärung. Die Autohersteller kämen mit der **Software-Entwicklung** nicht hinterher. Die hohe technische Komplexität, der Kostendruck und kurze Entwicklungszeiten würden immer häufiger zu Qualitätsproblemen führen.

Mit jeder neuen Fahrzeuggeneration steckt noch mehr Software im Auto. „Wenn man die Software-Entwicklung nicht im Griff hat, dann hat man ein Riesenproblem“, so Bratzel. Denn die Breite des Infotainments wachse und es werde zum kaufentscheidenden Merkmal. „Wenn das nicht funktioniert mit eigenen entsprechenden Entwicklungsabteilungen, braucht man tiefgehende Kooperationen.“, analysiert Bratzel.

VW will Software selbst entwickeln

Allerdings tut sich der VW-Konzern schwer, mit Partnern aus der IT-Welt zu kooperieren. Die **Software-Entwicklung** wolle man **aus eigener Kraft** stemmen, heißt es vom Konzern. Doch die Entwicklung kommt trotz milliardenschwerer Investitionen seit Jahren nicht wie gewünscht voran. Die Software-Probleme sind markenübergreifend so eklatant, dass VW-Chef Herbert Diess im Spätsommer 2022 unter anderem auch deswegen seinen Stuhl räumen musste.

Mängel bei VW sind teils sicherheitsrelevant

Dabei geht es keineswegs nur um streikende Navis oder flimmernde Bildschirme. Auch in **Assistenzsystemen** macht sich das Fehlervirus bei den VW-Marken offenbar breit und wird damit zum echten **Sicherheitsproblem**. Benutzer berichten von Ausfällen der **Notbremsfunktionen** und **Spurhalteassistenten**, Fehlern bei der **Verkehrszeichen-Erkennung**.

Wieso bekommt der VW-Konzern das Problem nicht in den Griff?

Auf Anfrage erklären Seat und die VW-Zentrale, man habe Fahrzeuge in einem großen Schritt digitalisiert und damit einen grundlegenden technologischen Umbruch vollzogen. Das sei nicht „gänzlich problemfrei“ gelaufen. Der Konzern räumt auch ein, dass er bislang nicht in jedem Einzelfall helfen konnte. Doch er verspricht:

Kunden haben Rücktrittsrecht

Seat-Fahrer Theo Schornstein will nicht warten, bis der VW-Konzern die Probleme gelöst hat. Er verhandelt seit einigen Monaten mit seinem Seat-Vertragspartner über die Rückabwicklung seines Leasingvertrags. Der Händler sperrt sich, dabei steht das Recht auf der Seite des Kunden.

Betroffene, egal ob **Käufer** oder **Leasingnehmer**, müssten mehrere erfolglose Nacherfüllungen **keineswegs akzeptieren**, erklärt der Stuttgarter Fachanwalt für Verkehrsrecht, Christian Steffgen.

Mit einer Reform des Schuldrechts habe der Gesetzgeber die Verbraucherrechte gestärkt. Kunden müssten Händler jetzt nur noch **ein Mal** zur Nachbesserung auffordern und auch **keine feste Frist** mehr setzen, so Steffgen. Wenn der Händler nach einer angemessenen Zeit – in der Regel etwa zwei Wochen – das Problem nicht behoben habe, sei der Kunde zum Rücktritt berechtigt.

Neuwagen und Leasingfahrzeuge können zurückgegeben werden

Damit hätten zahllose Kunden mit einem mangelhaften Infotainmentsystem das Recht, ihr Auto zeitnah wieder **zurückzugeben**, sofern der Fehler nicht behoben wird. In der Regel werden in so einem Fall die geleisteten Leasingraten erstattet und mit einer Nutzungsentschädigung verrechnet.

Auf diese Lösung hat sich schließlich auch das Autohaus von Theo Schornstein eingelassen – Dank seiner Hartnäckigkeit kann er den Leasingvertrag jetzt rückabwickeln.

Quelle: https://www.swrfernsehen.de/marktcheck/elektronikprobleme-bei-vw-100.html