33. Cybercrime Newsletter

30.01.2023

1) Anzeigenbetrug: Bis zu 11 Millionen iOS-Geräte von VASTFLUX betroffen

Eine gigantische Malvertising-Kampagne soll 1700 Apps fürs iPhone befallen haben, sagen Sicherheitsforscher. 120 Entwickler wurden offenbar zu Opfern.

Sicherheitsforscher haben eine großangelegte Malvertising-Kampagne aufgedeckt, die über iOS-Apps abgewickelt wurde. Bei dem Betrug, der mit dem Namen VASTFLUX bezeichnet wird, sollen laut Angaben des Unternehmens Human Security bis zu 11 Millionen iPhones betroffen gewesen sein. Das Ausspielen betrügerischer Anzeigen wurde demnach in insgesamt 1700 App-Store-Anwendungen von insgesamt 120 Entwicklern durchgeführt. Wie hoch der Gesamtschaden ist, lässt sich aktuell noch nicht beziffern.

Werbung, die niemand sieht, aber bezahlt wird

Anzeigenbetrug, auch Malvertising oder Ad Fraud genannt, gibt es im Web, aber eben auch in Apps. Dabei versuchen Kriminelle, Geld betrügerisch mit bezahlter Online-Werbung zu verdienen, die die jeweilige Zielgruppe aber tatsächlich nicht zu sehen bekommt. Oft wird dies mit Klickbetrug (Click Fraud) kombiniert, bei dem die Reklame auch (scheinbar) geklickt wird. Den Schaden haben vor allem die Werbetreibenden, deren gekaufte Anzeigen nicht an echte Menschen ausgeliefert werden – aber auch Marktplätze und Dienstleister ebenso wie Anbieter von Apps können betroffen sein, sollte es zu Rückforderungen kommen.

Bei VASTFLUX wurde mit manipuliertem JavaScript-Code gearbeitet, der in Anzeigen injiziert wurde, so Human Security. Den Betrügern gelang es so, zahlreiche für den Nutzer unsichtbare Videoplayer in Apps hintereinander zu platzieren – offenbar bis zu 25 Stück gleichzeitig – und darüber dann Ad Views (Anzeigenauslieferungen) zu generieren. Der Name VASTFLUX ergibt sich aus einer Kombination mehrerer Techniken, im Speziellen die DNS-Manipulation Fast Flux und das Video-Reklame-Template VAST des Internet Advertising Bureau.

App-Spoofing und immer neue Werbung

Laut den Sicherheitsforschern nutzten die Angreifer, die bislang offenbar noch nicht gefasst wurden, Apples restriktive In-App-Infrastruktur aus, um auf Anzeigeplätze zu bieten. Gegenüber Werbetreibenden wurde zudem die jeweils verwendete App an sich gespooft – Anzeigen landeten also statt in qualitativ hochwertigen Programmen in App-Müll. Dies half dabei, mehr Geld zu generieren. Werbeplätze wurden zudem regelmäßig neu befüllt – sogar über die 25 versteckten Videoplayer hinaus.

Laut Human Security basiert VASTFLUX auf einer ähnlichen Masche aus dem Jahr 2020, die sogar für eine versuchte Manipulation von Wählern in den USA eingesetzt worden sein soll. VASTFLUX umging auch Ad-Verification-Tags, die Malvertising eigentlich verhindern

sollen. Insgesamt soll es zu bis zu zwölf Milliarden Werbeausspielungen gekommen sein – pro Tag. Die Steuerserver von VASTFLUX wurden mittlerweile außer Betrieb gesetzt.

Quelle: https://www.heise.de/news/Anzeigenbetrug-Bis-zu-11-Millionen-iOS-Geraete-von-VASTFLUX-betroffen-7469040.html

2) Betrüger zielen auf Nutzer des Facebook-Messengers

Kriminelle verschicken derzeit Betrugsnachrichten über den Facebook-Messenger, warnen Sicherheitsexperten. Nutzer sollen teure Abos abschließen.

Betrüger versuchen derzeit, über den Meta Messenger (früher Facebook-Messenger) Nutzer in teure Abofallen zu locken. Das berichten die Sicherheitsexperten von "Eset". Die Kriminellen "versuchen mit einer perfiden Masche, Nutzer zu einem unüberlegten Klick auf einen Link zu verleiten", heißt es.

Wie das geht? Die Empfänger bekommen laut "Eset" eine vermeintliche Nachricht von Kontakten aus ihrer Freundesliste. Darin werde in den meisten Fällen ein Inhalt im sozialen Netzwerk Tiktok angepriesen und auch verlinkt.

"Alternativ kann der Nutzer zu irreführenden Spiel- oder Glücksspielportalen mit obligatorischer Registrierung weitergeleitet werden", heißt es weiter.

Nutzer sollen zahlen

Egal wohin die Empfänger geleitet werden, das Ziel der Betrüger sei immer dasselbe: Die Nutzer sollen angebliche Abos abschließen und dafür zahlen.

"In Deutschland sehen wir derzeit insbesondere Fälle von vermeintlichen Gewinnen. Hierzu sollen Nutzer persönliche Daten angeben, die dann zu einem teuren SMS-Abo führen", so Jiri Kropac, Leiter des ESET Forschungslabors in Brünn.

Er rät: "Schauen Sie sich die Nachrichten genau an: Achten Sie auf die Rechtschreibung und Grammatik. Häufig fällt hier bereits auf, dass etwas nicht stimmen kann".

Empfänger solcher sogenannter Phishing-Nachrichten sollen nicht einfach auf Links klicken, auch wenn der Inhalt noch so verlockend erscheint.

Phishing-Nachrichten an Verbraucherschützer weiterleiten

Phishing-Nachrichten sollten generell sofort gelöscht werden. Verbraucherzentralen bitten zudem darum, die falsche Nachricht vorher an sie weiterzuleiten.Auf ihrer Webseite listen die Verbraucherschützer nämlich die falschen Nachrichten und informieren so andere Nutzer. Eine Mail-Adresse lautet: phishing@vz-nrw.de.

Wie sich Phishing-Nachrichten außerdem erkennen lassen, haben wir in einem Artikel zusammengefasst. Dort steht auch, was Nutzer tun können, wenn sie Opfer eines solchen Betrugs geworden bin?

Quelle: https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100116734/betrugsmasche-kriminelle-zielen-auf-nutzer-des-facebook-messengers.html

3) Täuschend echt – Passwörter von Webhoster werden mit neuem Trick abgefischt

Passwörter des Webhosters Ionos werden aktuell mit gefälschten Mails abgefischt. Die Masche ist so raffiniert, dass sie kaum Verdacht bei den Opfern erregt.

Kunden des Webhosters Ionos sollten auf der Hut sein: Derzeit erhielten viele von ihnen gefälschte E-Mails, die nicht von der 1&1-Tochter, sondern von Kriminellen stammen. Davor warnt das Landeskriminalamt (LKA) Niedersachsen. Darin wird etwa fälschlicherweise behauptet, dass das Passwort fürs E-Mail-Postfach ablaufe oder die Geschäftsbedingungen aktualisiert würden. Im ersten Fall soll man das Passwort ändern, im zweiten Fall fordern die Kriminellen zum Log-in auf, angeblich zum Bestätigen der AGB-Änderungen.

Am besten erst gar keine Links anklicken

In beiden Fällen werden Nutzerinnen und Nutzer auf gefälschte Log-in-Seiten geführt, die ähnlich wie die E-Mails relativ echt aussehen. Dort fischen die Kriminellen dann die Zugangsdaten ab.

Das Fiese an der Masche: Benutzername und Passwort werden laut LKA sogar zeitgleich bei Ionos überprüft und man erhält eine Fehlermeldung, sollten die Daten fehlerhaft eingegeben worden sein. Die Opfer bemerken im schlimmsten Fall nicht rechtzeitig, dass es sich um Betrug handelt.

Wegen des Phishings und wegen der Gefahr, sich Schadsoftware auf den Rechner zu holen, sollte man am besten gar nicht erst auf Links in den Mails klicken, sondern die Nachrichten direkt löschen.

Wer Zweifel hat, kontaktiert am besten immer sofort den Kundensupport und fragt nach, ob an den Aufforderungen etwas dran ist, rät das LKA. Das gelte auch für den Fall, dass man den Kriminellen auf den Leim gegangen ist.

Großflächig Passwörter ändern

Zudem sollte man dann auch direkt die Zugangsdaten ändern. Und zwar nicht nur die für den Kundenbereich, sondern für sämtliche Passwörter, die den Webspace oder den Onlinespeicher betreffen: von Datenbanken über FTP-Zugänge bis hin zu Mail-Postfächern.

Als Nächstes ist es den Angaben zufolge wichtig, genau zu prüfen, ob bereits Daten verändert oder neue E-Mail-Adressen beziehungsweise -Weiterleitungen eingerichtet worden sind. Im Anschluss empfiehlt das LKA eine Anzeige bei der örtlichen Polizei oder auf der fürs eigene Bundesland zuständigen Onlinewache.

Quelle: https://www.t-online.de/digital/aktuelles/id_100116072/phishing-neuer-fieser-trick-beim-passwort-klau-per-e-mail.html

4) Dein Passwort ist in Gefahr – Kunden dieser 4 Banken betroffen

Die Sicherheitsvorkehrungen von Banken gehören in den meisten Fällen zum Besten, was die zivile Cybersicherheit zu bieten hat. Dennoch werden sämtliche Maßnahmen gelegentlich umgangen. Wir verraten, wie die Betrüger vorgehen und welche Banken derzeit betroffen sind.

Die Verbraucherzentrale NRW listet im Rahmen ihres Phishing-Radars kontinuierlich die neuesten Phishing-Mails auf. Selbstverständlich ist die Liste nicht erschöpfend; auch andere Mails sind im Umlauf. Sie zeigt allerdings, bei welchen E-Mails man als Nutzer derzeit auf jeden Fall ein Auge offen halten sollte. In der laufenden Woche gehören dazu die folgenden Unternehmen und Organisationen:

- Sparkasse
- DKB
- Postbank

- ING
- Amazon

Aktuelle Phishing-Lage – Vier Banken und Amazon

Grundsätzlich gilt: Ausnahmslos jedes an das Internet angeschlossene Gerät kann theoretisch gehackt werden. Und das gilt auch für digitale Konten. Bei letzteren spielt der Sicherheitsgrad im Grunde eine sekundäre Rolle. Denn es existiert ein entscheidender Unsicherheitsfaktor: der Mensch respektive der Kontoinhaber. Mittels sogenanntem Social Engineering, also der direkten menschlichen Beeinflussung, versuchen Kriminelle dieses Einfallstor zu öffnen. Am geeignetsten sind dabei sogenannte Phishing-Angriffe, wie die folgenden.

Sparkasse

Bei einer der aktuell betroffenen Banken handelt es sich um die Sparkasse. In ihrem Namen verschicken Cyberkriminelle zurzeit Phishing-Mails, in denen eine Optimierung der Systeme und ein noch sichereres Banking thematisiert werden. Vor diesem Hintergrund werden die Empfänger dazu aufgefordert, ihre Identität über eine in der E-Mail hinterlegte Verlinkung zu bestätigen. Die Konten derer, die dieser Aufforderung nicht nachkommen, sollen bereits in den kommenden Tagen temporär deaktiviert werden. Dennoch solltest du auf keinen Fall auf den hinterlegten Link klicken. Dieser führt im Regelfall zu einer gefälschten Sparkasse-Website. Alle hier eingetragenen Nutzerdaten wie Passwörter, Kontonummern und Benutzernamen landen bei den Cyberkriminellen. Und selbst die sogenannte Zwei-Faktor-Authentifizierung schützt nur bedingt vor einer Kontoübernahme, denn auch diese lässt sich mittels Phishing umgehen.

Wie solltest du also vorgehen? Da eine direkte Kundenansprache nicht gegeben ist und das Äußere der E-Mail nur bedingt dem der echten Sparkassen-Mails entspricht, solltest du die Nachricht unbeantwortet in den Spam-Ordner verschieben. Solltest du dir unsicher sein, kannst du alternativ beim Kundensupport der Sparkasse anrufen und entsprechende Erkundigungen einholen.

DKB

Auch Kunden der DKB erhalten gegenwärtig per Mail eine Aufforderung zum Aktualisieren ihres Profils. Inhaltlich heißt es hier, dass der Empfänger seine Kredit- oder Debitkarte nach dem 12. Januar 2023 nicht mehr verwenden könne. Er müsse überprüfen, ob sein Sicherheitssystem aktiv ist. Dazu müsse er seine persönlichen Daten und die Debitkarte bestätigen. Die Aktualisierung soll dabei zum wiederholten Male über eine hinterlegte Verlinkung erfolgen. Auch hier gilt: Auf keinen Fall auf die hinterlegte Verlinkung klicken, sondern die E-Mail stattdessen in den Spam-Ordner verfrachten.

Postbank und ING

Die E-Mails der Postbank und von ING scheinen aus der gleichen Feder zu stammen. Darauf deuten die minimalistische und teils bereits veraltete Optik sowie der wortkarge Aufbau hin. Vonseiten der vermeintlichen Banken heißt es in beiden Fällen, der Empfänger hätte eine dringende neue Information respektive Nachricht in seiner Mailbox. Daher müsse er sich über eine hinterlegte Verlinkung anmelden, um diese einsehen zu können. Bei der angeblichen Postbank-Mail gehen die Cyberkriminellen allerdings etwas gewiefter vor und geben einen Linktext für eine URL aus. Dabei wird ein Linktext in Form einer URL verfasst, die damit verknüpfte, echte URL führt allerdings zu einer gänzlich anderen Seite. Ein Beispiel: Klickst du auf https://meine.postbank.de, landest du nicht auf der Seite der Postbank, sondern auf unserem Phishing-Ratgeber.

Amazon

Obgleich die meisten Phishing-Mails im Namen unterschiedlicher Banken verschickt werden, können auch andere Dienste betroffen sein. Aktuell werden etwa Amazon-Nutzer mit einer sowohl optisch als auch inhaltlich überzeugenden Phishing-Mail konfrontiert. Sie werden darüber informiert, dass ihre Geldkarten aufgrund eines Problems nicht belastet werden können. Daher seien ihre Mitgliedsvorteile derzeit ausgesetzt. Glücklicherweise bedürfe es lediglich einer Aktualisierung der Karteninformationen, um das Problem zu beheben. Selbstverständlich mittels einer in der E-Mail hinterlegte Verlinkung. Direkte Kundenansprache? Fehlanzeige.

Phishing 2023 – Bisherige Fälle

Die Liste an Phishing-Versuchen in Deutschland wird immer länger. Klar zu erkennen ist, dass es vorwiegend große Unternehmen betrifft. Sie haben viele Kunden und damit viele potenzielle Opfer von Phishing. Diese Liste zeigt, welche Unternehmen im Jahr 2023 schon von Phishing-Betrügern genutzt wurden, um deine Daten oder dein Geld zu stehlen:

- Amazon
- Bitcoin-Erpressung
- DKB
- ING
- LBB
- PayPal
- Postbank
- Sparkasse

Was ist Phishing eigentlich?

Wenn man an Cyberkriminelle denkt, kommen einem automatisch Hollywood-Bilder von Unbekannten in Kapuzenpullis in den Sinn, die in einem Keller vor fünf Bildschirmen sitzen und ihren Blick auf das Pentagon richten. Die Wahrheit sieht allerdings oftmals ganz anders aus. Denn man braucht weder fünf Bildschirme noch große Kenntnisse über Sicherheitssoftware, um an das Geld von Internetnutzern zu gelangen. Sogar ein Kapuzenpulli ist dafür nicht zwingend erforderlich. Viele Anwender verraten ihre Zugangsdaten nämlich freiwillig, wenn man sie darum bittet.

Alles, was dazu benötigt wird, ist eine E-Mail im beispielsweise Amazon-Look, die Empfänger über ungewöhnliche Kontoaktivitäten oder eine AGB-Änderung unterrichtet. Anschließend wird das Opfer dazu aufgefordert, eine Autorisierung durchzuführen, indem er einen Link anklickt und sich in seinem Account anmeldet. Nur führt der Link nicht zur Amazon-Website, sondern zu einer Kopie. Die hier eingetragenen Login-Daten landen direkt bei den Cyberkriminellen. Mittlerweile steckt hinter Phishing eine regelrechte Industrie.

Weitere Betrugsmaschen & Schutzmechanismen:

- eBay Kleinanzeigen und Co.: Mit diesen Betrugsmaschen zockt man dich ab
- WhatsApp Abzocke: Das sind die hinterlistigen Maschen der Betrüger
- Privatsphäre durch Zukleben der Webcam? So löst du das Problem eleganter

So erkennst du Phishing-Mails

Sobald die Betrüger deine Nutzerdaten erbeutet haben, können sie diese beispielsweise zum Identitätsdiebstahl verwenden. Sollten die Anmeldedaten zu einem mit dem Bankkonto verknüpften Dienst gehören, könnte auch dein Portemonnaie darunter leiden. Darum solltest du auf E-Mails im Allgemeinen und auf Nachrichten der oben genannten Anbieter im

Besonderen achten. Weist die E-Mail Rechtschreibfehler auf? Wie sieht es mit direkter Kundenansprache aus? Handelt es sich bei dem Absender respektive bei der E-Mail-Adresse des Absenders im Kopf der E-Mail tatsächlich um PayPal? Gehört die verlinkte Webseite dem Online-Bezahldienst, oder ist die URL eher kryptisch? Alle diese Fragen können eine Phishing-Mail enttarnen.

Eine weitere, gute Selbstschutz-Maßnahme stellt die Zwei-Faktor-Authentifizierung (2FA) dar. Dabei handelt es sich um einen doppelten Anmeldeschutz, bei dem neben den Anmeldedaten eine zweite Anmeldeschranke eingerichtet wird – etwa in Form eines Codes, der auf eine zuvor hinterlegte Telefonnummer zugestellt wird. Diesen können Cyberkriminelle in der Regel nicht so einfach ergattern. Obwohl auch diese Schutzlinie nicht unüberwindbar ist. Weitere Informationen zu dem Thema erhältst du in unserem Phishing-Ratgeber.

Quelle: https://www.inside-digital.de/news/phishing-woche-aktuelle-faelle-banken-kw3-bank-passwort-in-gefahr

5) Amazon: Unglaublich dreister Betrug aufgeflogen – auch in Deutschland

Selbst auf der Amazon-Website bist du als Verbraucher keinesfalls vor Betrug geschützt. Wobei mit „Betrug“ nicht irgendwelche Manipulationsversuche an den Algorithmen gemeint sind. Sondern waschechter Schwindel, der gegen das Strafgesetzbuch verstößt. Wir verraten, worauf du achten musst.

Von unseriösen Händlern ist man dies bereits gewohnt: Als Verbraucher bekommt man nicht immer das, was man bestellt. Doch Amazon gehört nicht zu den unseriösen Händlern. Bei dem US-amerikanischen Unternehmen handelt es sich um einen der größten Online-Versandhändler und Hersteller der Welt. Daher überlegen manche Käufer nicht allzu lange, wenn sie ein preiswertes Produkt entdecken. Ein großer Fehler, wie ein aktueller Fall offenlegt.

Unverhohlener Betrug auf Amazon

Suchst du bei Amazon nach einer externen SSD mit hoher Kapazität, dürftest du schon bald auf einige unschlagbare Angebote treffen. SSD-Dateiträger mit um die 16 TB (etwa 16.000 GB oder 16.000.000 MB) werden für unter 100 Euro verscherbelt. Und das, obwohl entsprechende Markenprodukte tausende Euro auf die Preiswaage legen. Ein Betrug? So wirkt es auf den ersten Blick. Doch die Bewertungen sind ausgezeichnet und Amazon übernimmt sogar den Versand. Geht also doch alles mit rechten Dingen zu? Mitnichten! Das unterstreicht Josh Hendrickson, Chefredakteur des Portals ReviewGeek. Dieser erwarb einen der erwähnten Datenträger und nahm ihn auseinander. Zum Vorschein kam eine Micro-SD-Karte mit USB 2.0 und einer Speicherkapazität von 64 GB. Und damit ein Datenträger mit lediglich etwa 0,4 Prozent der angekündigten Kapazität. Tatsächlicher Kostenpunkt: um die 10 Euro

Im Rahmen unserer Recherche sind wir auch auf der deutschen Amazon-Website auf zahlreiche ähnliche Angebote gestoßen. Dabei müssen es nicht zwingend 16 TB sein. Manchmal sind es auch 18 TB oder etwa 6 TB. Letztere SSD-Festplatte wird zurzeit übrigens für lediglich 48,99 Euro verkauft. In den meisten Fällen deuten jedoch bereits die Nutzerreviews – sofern es welche gibt – auf einen Betrug hin. So berichten einige von einer geringeren Kapazität, in den meisten Fällen werden die jeweiligen Speichermedien jedoch als „unbrauchbar“ abgestempelt. Dies lässt sich in erster Linie darauf zurückführen, dass die Datenträger schlichtweg keine Daten abspeicherten und die aufgespielten Dateien daher unwiderruflich verloren gingen. Und das, obgleich einige der SSD-Datenträger tatsächlich von

Amazon versandt wurden. Gefälschte Artikel mit einer guten Sternebewertung konnten wir allerdings nicht ausfindig machen.

Wie kommen Fälschungen an gute Sternebewertungen?

Hendrickson geht davon aus, dass Händler die Bewertungen anderer Produkte übernahmen. Dies funktioniert wie folgt: Man nimmt einen bereits existierenden Produkteintrag mit guten Bewertungen und ändert die Überschrift, die Bilder sowie die Beschreibungstexte. Die Bewertungen bleiben jedoch unverändert – obgleich sie inhaltlich ein gänzlich anderes Produkt in den Fokus rücken. In einer Stellungnahme betont Amazon gegenüber Reviewgeek, dass man die Übernahme von Produktlisten nicht erlaube. Selbiges gelte für falsche Produktinformationen. Der Versandhändler spricht von einer Nulltoleranzpolitik. Dennoch können wir bestätigen, dass entsprechende Praktiken durchaus auch im deutschsprachigen Amazon vorkommen und daher auch für die hiesigen Verbraucher eine reale Gefahr darstellen.

So minimierst du das Betrugsrisiko

Zunächst einmal empfiehlt es sich, vor einem Kauf stets auf die Produktreviews zu achten. Und zwar nicht auf die 5-Sterne-Bewertungen, sondern auf diejenigen, die negativ ausfallen. Sollten sämtliche Bewertungen durchwegs positiv sein, ist dies ebenfalls ein Grund, um misstrauisch zu werden. Denn zahlreiche Amazon-Bewertungen sind nach wie vor bezahlt. Ist dies der Fall, kann eine ungewöhnliche Häufung an Bildern und Videos einen Hinweis liefern. Denn bezahlte Bewertungen werden oftmals um multimediale Elemente ergänzt.

Bleiben noch die Bewertungen, die die Verkäufer selbst vorweisen. Wir haben uns drei Fälle von SSD-Betrug auf Amazon genauer angeschaut. Dabei konnten zwei der drei Verkäufe jeweils lediglich eine einzige Bewertung vorweisen. Beim letzten Händler waren es dagegen zwei Bewertungen. Wobei drei der vier Bewertungen nicht älter als drei Wochen sind.

Bleibt noch der Hinweis, dass wenn etwas zu schön ist, um wahr zu sein, es vermutlich auch nicht wahr ist. Heißt: Solltest du ein Produkt finden, welches zu einem Bruchteil des eigentlichen Kaufpreises verkauft wird, dann stehen die Chancen gut, dass du am Ende sowohl ohne Produkt als auch ohne Geld dastehst.

Passend dazu: Phishing-Betrug: Darauf müssen Nutzer von Amazon, PayPal & Co. achten

Wohnungsanzeigen-Betrug boomt – so vermeidest du Konsequenzen

Quelle: https://www.inside-digital.de/news/amazon-dreister-betrug-aufgeflogen

6) PayPal informiert über Hacker-Angriffe: Betroffene Nutzer müssen jetzt dringend reagieren

PayPal informiert zahlreiche Nutzer aktuell über einen Hacker-Angriff, von dem Zehntausende Kunden betroffen sind. Die betroffenen User sollten nun dringend aktiv werden und den Anweisungen von PayPal folgen.

Wie die Webseite "BleepingComputer" berichtet, wurden PayPal-Konten bei groß angelegtem sogenannten Credential-Stuffing-Angriff gehackt. Deshalb hat das Unternehmen Tausende von Nutzern, auf deren Konten zugegriffen wurde, über die Datenschutzverletzungen benachrichtigt. Bei dem Angriff wurden persönliche Daten erbeutet.
Bei Credential-Stuffing-Angriffen versuchen Hacker auf ein Konto zuzugreifen, indem sie Benutzernamen- und Passwortpaare ausprobieren, die aus Datenlecks auf verschiedenen Websites stammen. Diese Art von Angriff beruht auf einem automatisierten Ansatz, bei dem

Bots Listen mit Anmeldeinformationen ausführen, um Anmeldeportale für verschiedene Dienste zu "stopfen".

Fast 35.000 Nutzer von Angriff auf PayPal betroffen

PayPal erklärt, dass der Credential-Stuffing-Angriff zwischen dem 6. und 8. Dezember 2022 stattfand. Das Unternehmen hat ihn damals erkannt und konnte ihn begrenzen. Eine interne Untersuchung wurde eingeleitet, um herauszufinden, wie die Hacker Zugriff auf die Konten erhalten haben.
Laut dem Bericht von PayPal über die Datenschutzverletzungen sind 34.942 Nutzer von dem Vorfall betroffen. Während der zwei Tage hatten Hacker Zugriff auf die vollständigen Namen, Geburtsdaten, Postanschriften, Sozialversicherungsnummern und individuelle Steueridentifikationsnummern der Kontoinhaber. Die Angreifer haben nicht versucht oder es nicht geschafft, Transaktionen von den gehackten PayPal-Konten durchzuführen.

PayPal-Datenklau: So sollten Nutzer jetzt reagieren

"Wir haben die Passwörter der betroffenen PayPal-Konten zurückgesetzt und erweiterte Sicherheitskontrollen implementiert, die Sie dazu auffordern, ein neues Passwort einzurichten, wenn Sie sich das nächste Mal bei Ihrem Konto anmelden", so PayPal in einem Statement. Betroffene Benutzer erhalten von Equifax zwei Jahre lang einen kostenlosen Identitätsüberwachungsdienst.
Darüber hinaus empfiehlt PayPal den Benutzern, den Zwei-Faktor-Authentifizierungsschutz (2FA) im Menü "Kontoeinstellungen" zu aktivieren, der verhindern kann, dass Unbefugte auf ein Konto zugreifen, selbst wenn sie über einen gültigen Benutzernamen und ein gültiges Passwort verfügen.
Grundsätzlich gilt, dass Nutzer Ihre Passwörter so wählen sollten, dass sie nicht einfach zu knacken sind. Sichere Passwörter verfügen über eine Kombination aus Buchstaben, Zahlen und Sonderzeichen. Sie sollten mindestens zwölf Zeichen lang sein, die Buchstaben sollten in Groß- und Kleinschreibung genutzt werden. Auch ist es sinnvoll, nicht die Namen von Kindern, Ehegatten oder Haustieren zu verwenden. Eine wahllose Kombination von Zeichen ist sinnvoller.

Quelle: https://www.chip.de/news/PayPal-von-Hacker-Angriff-betroffen-Viele-Nutzer-muessen-ihr-Passwort-aendern_184620924.html

7) Amazon: Vorsicht vor falschen SSD-Festplatten – sie locken mit einem Hammerpreis

SSD-Festplatten sind für alle mit hohem Speicherbedarf sehr nützlich. Doch aktuell gibt es bei Amazon einige im Angebot, von denen du besser die Finger lässt.

Im Internet gibt es allerlei zwielichtige Webseiten, wo zweifelhafte Waren angeboten werden. Man sollte aber meinen, dass ein so großes Einkaufsportal wie **Amazon** nicht dazu gehören würde. Trotzdem erscheinen dort beizeiten Artikel, die nichts anderes sind als Betrug. Deshalb solltest du dich aktuell vor SSD-Festplatten hüten, deren Preis-Leistungs-Verhältnis einfach zu gut sind, um wirklich wahr zu sein.

Amazon: Externe SSD-Festplatten lächerlich günstig

Wer Bedarf nach einer SSD-Festplatte hat, wird vor allem auf zwei Dinge wert legen: Viel Speicherplatz und eine besonders hohe Lesegeschwindigkeit. Wenn dann noch der Preis stimmt, umso besser. Bei Amazon gibt es unter anderem ein Exemplar der Marke Generic („Generisch“ auf Deutsch) im Angebot, das mit satten 16 Terabyte (TB) Speicher und einem USB 3.1-Anschluss wirbt. Das Beste daran? Das Beispiel kostet weniger als 100 Euro.

Was traumhaft klingt, sollte aber laut Review Geek direkt stutzig machen. Zwar existieren tatsächlich SSDs mit so viel Speicherkapazitäten. Allerdings kosten die für gewöhnlich zwischen mehreren Hundert bis Tausende von Euro. In einem ausführlichen Test förderte man dann auch die Wahrheit zutage.

64 GB-Speicher statt 16 TB

Bei Review Geek hat man sich eine solche Festplatte bestellt und sie überprüft. Bereits beim Verschieben von einem Dateiordner mit einer Größe von 1 Gigabyte (GB) stellte man fest, dass es viel zu lange dauerte. Was nur eine Minute hätte dauern müssen, brauchte 20 Minuten. Das deutete schon einmal auf nur einen USB 2.0-Port hin und nicht auf 3.1.

Als man aber den Speicher komplett füllen wollte, war nach nur 64 GB Schluss. Darauf hin hat man die Festplatte ganz einfach auseinandergenommen – und innen drinnen eine einfache micro SD-Speicherkarte vorgefunden. Diese war einfach nur in eine Leitplatte gesteckt, die als USB-C-Adapter getarnt war. Trotzdem hatte beim Test Windows 16 TB vorhandener Speicher angezeigt. Das könnte an der verwendeten Software liegen, die schlichtweg falsche Werte anzeigte.

Richtige und falsche Kundenbewertungen

Bei Review Geek nahm man sich zwar eine falsche SSD einer anderen Marke als im oben verlinkten Beispiel zur Brust. Schaut man sich aber dort die Nutzerbewertungen an, wird schnell deutlich, dass das gleiche Problem vorliegt:

> „[…] Geschwindigkeit extrem langsam, nicht einmal USB 2.0 erreicht […]“
>
> *Amazon/Bertl*
>
> „Ich schick sie wieder zurück, denn obwohl sie nach anscliessen sichtbar war so hat sie beim kopieren von Daten eine Geschwindigkeit von 19MB/s. das heist ein Terrabite dauert ca einen Tag. Finger weg [sic]“
>
> *Amazon/Rolf Schulz*
>
> „[…] Statt einer originalen, mit mehreren und insgesamt 16 Terabyte großen Speicherchips belegten Platine, sind bei diesen ‚Billigstangeboten‘ nur ordinäre/billige, wenige Gigabyte ‚große‘/kleine USB-Sticks oder MicroSD Karten und ein Aluminiumblock als Gewicht in einem mehr oder weniger ‚schicken‘ normalen Laufwerksgehäuse verbaut […]“
>
> *Amazon/Jonas*

Im englischsprachigen Raum ist es zudem zu vielen positiven Rezensionen gekommen, die sich als falsch und für ein falsches Produkt geschrieben entpuppten. Zudem wurde schon beobachtet, dass Angebote zwischenzeitlich verschwanden, nur um an anderer Stelle zurückzukommen.

Wenn du also wieder bei Amazon unterwegs bist, sieh dich also vor falschen SSD-Festplatten vor. Ist das Angebot zu gut, um wahr zu sein, dass ist es das auch einfach nicht. Wirf am besten einen ganz genauen Blick auf die Bewertungen, wofür sie geschrieben sind und was einzelne tatsächlich geschrieben haben.

Quelle: https://www.futurezone.de/digital-life/article417628/amazon-fake-ssd-festplatten.html

8) „Neue“ Nutzungsbedingungen – Sparkassen- und Postbank-Kunden betroffen: falscher Klick und Daten sind weg

Die Verbraucherzentrale warnt vor neuen Betrugsmaschen im Internet. Kriminelle versuchen über gefälschte Kundenmails von Banken an private Daten zu kommen.

Kassel – Kunden verschiedener Bankinstituten wie Volksbank, Sparkasse, Commerzbank haben in den vergangenen Tagen womöglich elektronische Post von ihrem jeweiligen Kundenservice bekommen. Verbunden mit einer Aufforderung zur Daten-Verifizierung. Diesem Appell sollte man aber besser nicht nachkommen, raten Verbraucherschützer.

Sparkassen- und Postbank-Kunden aufgepasst: Daten und Geld mit einem Klick weg

Oftmals stecken Betrüger hinter den Benachrichtigungen, erklärt die Verbraucherzentrale auf ihrer Homepage. Dort werden im sogenannten „Phishing-Radar“ alle aktuellen Warnungen von Betrugsmaschen gesammelt.

Beim „Phishing“ handelt es sich um umfangreiche Methoden von Cyber-Kriminellen, die sich als vertrauenswürdige Kommunikationspartner tarnen und darüber persönliche Daten der Internetnutzer zu „angeln“. Jüngster Versuch der Betrüger: Sich als Service-Mitarbeiter von Banken auszugeben.

Betrugsmasche mit neuen „Nutzungsbedingung“: Warnung vor Sparkassen- und Postbank-Mails

In ihrem Vorgehen machen sich die Betrüger den Jahreswechsel zunutze: So erreichte die bundesweite Beratungszentrale jüngst Meldungen, dass etwa Sparkassen-Kunden per E-Mail ihre Kontoinformationen bestätigen müssten, da sich EU-Regularien zum 1. Januar geändert hätten, berichtet hna.de.

Diese sehe einen neuen Konto-Login vor, wofür die Bank die sogenannte „SHA1-Fingerprint“-Methode entwickelt habe. Um ihn nutzen zu können, sei die Verifizierung der Kundendaten auf einer externen Internetseite „unabdingbar“ (mehr Service-News bei RUHR24).

Diese Banken sind laut der Verbraucherzentrale von den Betrugsmaschen betroffen:

- **Sparkasse**
- **Postbank**
- **Volksbank**
- **Commerzbank**
- **Deutsche Bank**
- **comdirect**

Sparkasse, Postbank und Co. von neuer Betrugsmasche betroffen: Daten in Gefahr

Ähnlich geht es aus einer vermeintlichen E-Mail der Postbank hervor, meldet die Verbraucherzentrale. Auch hier müssten die sensiblen Daten bestätigt werden; aufgrund neuer Nutzungsbedingungen. Dann folgt die klassische Phishing-Masche:

Über einen Link-Button gelangen die Kunden auf eine Webseite, auf der sie die benötigte Verifizierung vernehmen sollen. Erfolge diese nicht, drohe eine Sperrung oder Deaktivierung des Online-Bankings. Panikmache, auch ein wesentlicher Bestandteil der Phishing-Versuche, warnt die Verbraucherzentrale und rät, dubiose E-Mails zu löschen oder in den Spam-Ordner zu verschieben.

Betrug um vermeintlichen Datenschutz: Phishing-Mails sind das trojanische Pferd des digitalen Zeitalters

Besonders heimtückisch sind auch die Maschen, die die Betrüger unter dem Namen von Commerzbank, ING-Diba und Volksbank angewandt haben. Denn in diesen Phishing-Nachrichten wird den Kunden weisgemacht, dass es sich dabei um Datenschutz-Maßnahmen handelt.

Kunden der Commerzbank sollten etwa für ihre „photoTAN Card“, die das Institut ihren Kunden tatsächlich fürs Online-Banking anbietet, Daten übermitteln. Die E-Mail mit der täuschend echten Aufmachung und Werbematerial, verspricht, dass die Mobile-Aktivierungen so „einfacher, schneller und gleichzeitig mit der gewohnten Sicherheit“ funktioniere.

So erkennt man die Betrugsmaschen im Internet und so kann man sich schützen:

- **Niemals auf Links in einer dubiosen E-Mail klicken:** Im Zweifelsfall versuchen, die im E-Mail-Text genannte Seite über die Startseite der betreffenden Organisation zu erreichen oder direkt beim Anbieter vor Ort oder telefonisch nachfragen.
- **Keinesfalls persönliche Daten weitergeben:** Passwörter, Kreditkarten- oder Transaktionsnummern via E-Mail nicht preisgeben – egal, wie vertrauenerweckend eine E-Mail erscheint.
- **Niemals einen Download-Link** direkt aus einer E-Mail heraus starten, deren Echtheit nicht hundertprozentig gegeben ist. Auch angehängte Daten nicht öffnen.
- **Regelmäßig den Saldo des Bankkontos** sowie Umsätze kontrollieren, um unbefugte Konto-Aktivitäten schnellstmöglich zu entlarven und Maßnahmen ergreifen zu können.
- *Quelle: Bundesamt für Sicherheit in der Informationstechnik*

Betrugsmasche: Phishing-Mails sind oft täuschend echt, lassen sich aber an ein paar Merkmalen erkennen

Die Kundschaft der Volksbank wird derweil in Mails aufgefordert, das neue Web-Sicherheitssystem zu aktualisieren. Und auf den Karten der ING-Kunden seien vermeintlich verdächtige Aktivitäten festgestellt worden. Damit die Karte aktiv bliebe – Link anklicken.

Das Gefährliche an der perfiden Masche: Die Betrüger imitieren dabei ein tatsächliches Vorgehen einiger seriöser Konzerne, wie es beispielsweise Google tut. Nur, dass es sich dabei um eine Maßnahme zum tatsächlichen Datenschutz von Nutzern handelt. Erkennen könne man die hinterhältigen Phishing-Mails meist an der unpersönlichen Anrede und fehlerhaften Absenderadresse, erklärt die Verbraucherzentrale.

Wird mit einer Kontoeinschränkung gedroht oder geht es in Mails oder Internet-Seiten und -plattformen um persönliche Daten, sollten bei den Nutzern sofort die Alarmglocken angehen. Lieber einmal zu viel bei der Bank nachgefragt, als Kriminellen ins Netz zu gehen.

Quelle: https://www.ruhr24.de/service/sparkasse-postbank-spam-mail-nutzungsbedingungen-anh-r24-warnung-betrug-verbraucherzentrale-92031297.html

9) DHL warnt vor neuer Betrugsmasche per SMS

Derzeit kursiert eine neue Betrugsmasche. Kriminelle wollen an die Daten von DHL-Kunden kommen. Die Nachrichten sollen "sehr authentisch" wirken.

Der Paketdienst DHL hat in den sozialen Medien vor einer neuen Betrugsmasche gewarnt. Dem Beitrag zufolge seien aktuell SMS-Nachrichten in Umlauf, mit deren Hilfe private Daten abgegriffen werden sollen. Kunden werden nach ihrer Adresse gefragt oder aufgefordert, ihre Daten zu aktualisieren.

DHL ruft dazu auf, nicht auf den entsprechenden Link zu klicken, auch wenn der Absender als "DHL" oder "DHL Paket" deklariert ist. Ein Kunde berichtet unter dem Tweet des Paketdienstes sogar, dass er eine Phishing-SMS bekommen habe, die im selben Nachrichtenverlauf wie echte DHL-Nachrichten aufgetaucht sei.

DHL: Betrüger-SMS "wirken sehr authentisch"

Das bestätigt auch DHL: "Teilweise tauchen diese SMS sogar in den echten älteren SMS-Verläufen mit DHL Paket auf und wirken dadurch sehr authentisch", heißt es auf Facebook. Weiter fügt das Unternehmen hinzu, dass es grundsätzlich seine Kunden nie per SMS zu Zahlungen oder Änderungen von Daten aufrufen würde.

Wer eine dieser Nachrichten bekommt, sollte auf keinen Fall auf den Link klicken. Sind Daten einmal preisgegeben, kursieren sie im Internet. Betroffene sollten bestenfalls einen Screenshot von der SMS machen und sich an die Polizei wenden.

So können Sie Phishing-Nachrichten erkennen

Betrüger sind nicht unfehlbar – manchmal ist es sogar recht offensichtlich, dass eine SMS oder E-Mail gefälscht ist. Darauf sollten Sie achten:

- Schreibfehler in der Nachricht
- Es gibt keine persönliche (namentliche) Anrede
- "Mail-Spoofing": Betrüger können ihre E-Mail-Adressen mit Namen bekannter Unternehmen tarnen. Bewegt man den Mauszeiger aber über die Absenderadresse, kann man den wahren Absender erkennen.

Besonders wichtig ist vor allem: Niemals auf eine seltsam wirkende Nachricht antworten und keine Links öffnen!

Quelle: https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100118394/dhl-vorsicht-neue-sms-betrugsmasche-das-muessen-kunden-wissen.html

10) Comdirect-Kunden im Visier von Betrügern – Details entlarven Kriminelle

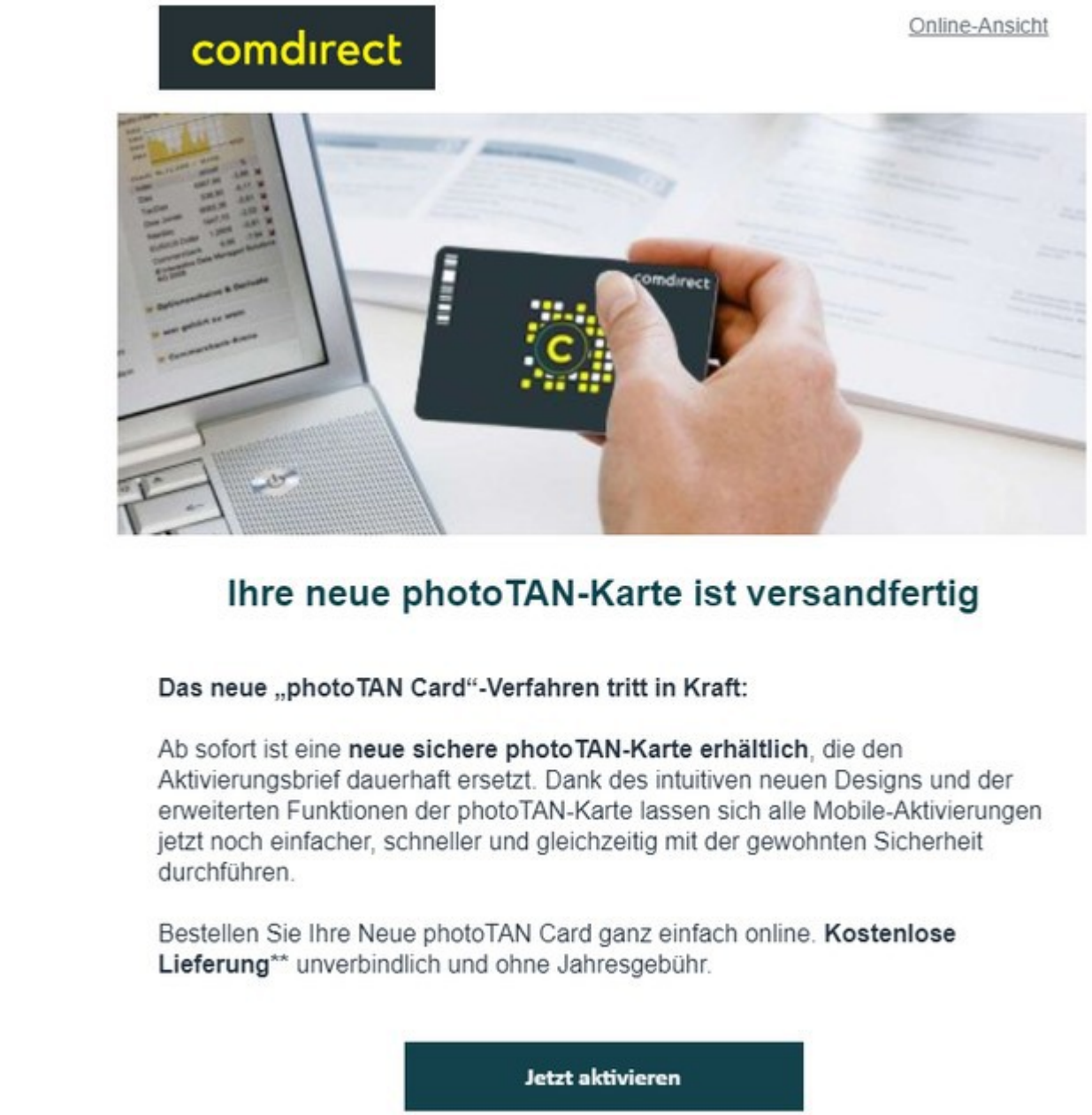
Betrügende versuchen, mit immer neuen Maschen andere übers Ohr zu hauen. Das Ziel: Auf illegale Weise an das Geld oder sensible Daten zu kommen. Besonders häufig sind Kund:innen von Abonnements und Banken Zielscheibe von perfiden Betrugsmaschen.

Dafür finden häufig ähnlich konzipierte Maschen Anwendung, jeweils in leicht abgewandelter Form. Beliebt sind etwa Fake-SMS oder Phishing-Mails. Letztere zirkulieren derzeit vor allem in Nordrhein-Westfalen, wie die Verbraucherzentrale des Landes warnt. Die Wahrscheinlichkeit ist aber groß, dass nicht nur Menschen aus NRW Ziel des neuen Betrugsversuches werden.

Empfänger der Mail sollen auf Link klicken und sensible Daten angeben

Konkret geht es um Mails, die sich an die Kund:innen von Comdirekt richten. Für die Betrugsmasche nutzen die Betrüger:innen ein Verfahren, das tatsächlich bei der Bank Anwendung findet: die sogenannte photoTAN-Funktion. **Die Mail hat den Betreff "Ihre neue photoTAN-Karte ist versandfertig" und sieht täuschend echt aus.** Mit integriert: die typischen Comdirekt-Farben sowie das Logo und ein Foto der photoTAN-Karte.

In der Mail ist dann die Rede von der Bestellung einer photoTAN-Karte, die mobile Aktivierungen "einfacher, schneller und gleichzeitig mit der gewohnten Sicherheit" machen sollen.



Quelle: Die Mail sieht täuschend echt aus und ist mit dem Logo der Bank versehen. Bild: Verbraucherzentrale NRW

Hinter der Comdirekt-Mail steckt eine perfide Betrugsmasche

Der Clou: Kund:innen können angeblich durch einen einfachen Klick auf den beigefügten Button die Karte aktivieren, heißt es in der Aufforderung im Text. **Wer eine solche Mail erhält, sollte dies jedoch tunlichst vermeidet.**

Auf der Seite, auf die der Link führt, wird der Empfänger oder die Empfängerin dazu aufgefordert, sensible Daten einzugeben. Selbst geübte Internet-Nutzer:innen könnten in die Versuchung geraten, auf die Masche hereinzufallen. **Die Mail sieht extrem authentisch aus, wie die Verbraucherzentrale weiter schreibt.**

Nur die unpersönliche Anrede und die unauthentische Absende-Adresse lassen einen Betrugsversuch vermuten. Die Verbraucherzentrale rät dringend, im Zweifel die Mail in den Spam-Ordner zu schieben und sie anschließend zu löschen.

Kunden können sich vor Phishing-Betrug schützen

Die Verbraucherzentralen haben mehrere Tipps zusammengestellt, um Phishing-Mails zu entlarven. Aufgrund ihres authentischen Aussehens ist das meist gar nicht so einfach. Grundsätzlich gilt aber: **Wer die Echtheit einer Mail bezweifelt, sollte sicherheitshalber beim Anbieter nachfragen.** Natürlich nicht als Antwort auf eben jene Mail.

Ein deutlicher Hinweis auf Betrugsversuche ist es außerdem, wenn der eigene Name in der Anrede fehlt. Das spricht dafür, dass eine Mail nicht vom vorgegebenen Anbieter stammt. **Einige Betrügende haben aber möglicherweise den Nachnamen durch Recherche herausgefunden.** Verlassen kann man sich darauf im Umkehrschluss also nicht. Es gilt nicht als Hinweis für die Echtheit.

Skepsis ist vor allem dann angebracht, wenn persönliche Daten sowie eine PIN oder TAN gefragt abgefragt werden. "Geldinstitute werden so etwas niemals telefonisch oder per E-Mail tun", schreibt die Verbraucherzentrale. Das zu beachten, gilt als eine der wesentlichen Sicherheitsregeln.

Wenn der Absender eine dringende Aufforderung formuliert, dass man auf einen Link klicken soll, ist das verdächtig. Auch wenn die Mail-Adresse nicht authentisch wirkt, sollte man die Finger von der Mail lassen. Dann ist es ratsam, besagte Nachricht zu löschen.

Quelle: https://www.watson.de/leben/geld%20&%20shopping/694786700-comdirect-kunden-im-visier-von-bank-betruegern-details-entlarven-kriminelle

11) „Passwörter ändern“: Experten warnen plötzlich vor beliebtem Passwortmanager – Millionen Nutzer betroffen

Fachleute für Sicherheit raten LastPass-Nutzer*innen, das Tool dringend zu wechseln. Grund dafür sind einige Sicherheitslücken und der Umgang des Herstellers damit

Der Passwortmanager **LastPass** hat nach eigener Aussage weltweit rund 33 Millionen Nutzerinnen und Nutzer. Dennoch legen die Sicherheitsexpert*innen von Intego nahe, das Programm umgehend zu wechseln. Wegen mehrerer Sicherheitslücken in den vergangenen Monaten sei es nicht sicher.

LastPass nicht zu empfehlen: Das wird geraten

„Wir empfehlen nicht, LastPass als Passwortmanager zu nutzen“, heißt es in dem entsprechenden Blogeintrag. Man rechne damit, dass Hacker bereits Zugriff auf jegliche Passwörter und Informationen in entsprechenden Konten gehabt haben könnten. Nutzer*innen sollten deshalb gleich zwei Maßnahmen ergreifen.

> „1. LastPass-User sollten sofort damit beginnen, zu einem anderen Passwortmanager umzuziehen.
>
> 2. Nach der Migration zu einem neuen Passwortmanager sollten ehemalige LastPass-Nutzer die Passwörter zu allen Diensten ändern, die sie in LastPass gespeichert hatten.“ *Intego*

Bei der expliziten Warnung und den Handlungsempfehlungen beziehen sich die Expert*innen unter anderem auf Vorfälle seit August 2022. Aber auch die Reaktion von LastPass darauf sowie die Technologie, die das Unternehmen zum Schutz seiner Nutzerschaft verwendet, stehen in der Kritik.

Bestehende Vorwürfe gegen den Passwortmanager

Wie Intego berichtet, kam es bereits im August 2022 zu einem initialen Sicherheitsleck. Damals unterrichtete LastPass seine Kundschaft, dass es einen Zugriff auf die Entwicklungsumgebung durch unautorisierte Dritte gegeben habe. Nutzungsdaten sollen dabei nicht gestohlen worden sein.

Im November veröffentlichte der Passwortmanager dann ein neues Statement. Demnach seien „bestimmte Elemente […] von Kundeninformationen“ durch Hackerinnen oder Hacker entwendet worden.

Schließlich soll LastPass im Dezember zugegeben haben, dass die von den Hackern erbeuteten Daten für einen weiteren Angriff genutzt wurden.

Man habe damit einen Mitarbeiter des Unternehmens so getäuscht, dass dieser Schlüssel zu Anmeldedaten herausgab, mit denen später Kundeninformationen eingesehen und entschlüsselt werden konnten.

Auch andere Experten üben Kritik

Laut anderen Fachleuten, wie dem Sicherheitsforscher Wladimir Palent, seien die Statements von LastPass „voll von Auslassungen, Halbwahrheiten und geradeheraus gelogen“.

Eine diesbezügliche Anschuldigung lautet, dass die von LastPass implementierten Algorithmen zur Passwortstärkung gemessen an Industriestandards nicht stark genug seien. Nutzer könnten demnach viel zu leicht gehackt werden.

LastPass-Konkurrent 1Password erklärte, es würde Angreifer nur 100 Dollar oder weniger kosten, das Masterpasswort für LastPass-Tresore zu knacken.

Quelle: https://www.futurezone.de/digital-life/article416592/lastpass-passwortmanager-warnung.html

12) Phishing-Alarm – "Klicken Sie nicht auf den Link": IHK Coburg warnt vor gefährlichen Mails

Die IHK Coburg warnt vor gefährlichen Fake-Mails. Betriebe werden darin fälschlicherweise im Namen der IHK dazu aufgefordert, sensible Daten preiszugeben.

- **Coburg: IHK warnt vor Datenklau - "bitte ignorieren Sie diese Mail"**
- **Handelskammer** gibt **Tipps** zum **Umgang** mit **Fake-Mails**
- "Übermitteln Sie **keine Daten**": IHK mit dringlichem **Appell** an **Betriebe**

Wie die **IHK Coburg** berichtet, erhalten **Betriebe** zurzeit vermehrt **falsche Mails**, "in denen sie aufgefordert werden, einen **digitalen IHK-Schlüssel** zu beantragen". Und das "seit Neuestem sogar **mit dem aktuellen DIHK-Logo**", wie die **Handelskammer** jetzt mitteilt.

Coburg: Betriebe sollen keine Daten übermitteln - "digitaler IHK-Schlüssel" ist Fake

Mit dem besagten "**digitalen IHK-Schlüssel**" sei es den Betrieben dann angeblich möglich, "sicher die **Dienstleistungen** der Handelskammer zu nutzen". Für den Fall, dass bis zum angegebenen **Stichtag** kein Antrag gestellt werden sollte, erwarte die Betriebe sogar

schwerwiegende Konsequenzen.

Demnach werde den betroffenen Betrieben in den Fake-Mails außerdem gedroht, dass "die **Gesellschaftsform** als **inaktiv**" gestellt werden würde, "falls bis zum angegebenen **Stichtag** kein Antrag gestellt werde". Somit bestünde dann "**kein Anspruch** mehr auf eine **Eintragung** bei der Handelskammer".

"Wer der **Aufforderung** folgt, die enthaltene **Schaltfläche** anzuklicken ("um Ihre Identität zu bestätigen und Einblick in Ihren Fall zu erhalten"), öffnet ein **Formular**, in dem er seine **Daten** ausfüllen und absenden soll", warnt die IHK Coburg jetzt eindringlich und stellt klar: "**Einen solchen "digitalen IHK-Schlüssel" gibt es nicht**. Bitte **ignorieren** Sie diese Mail, klicken Sie nicht auf den **Link**, und übermitteln Sie keine Daten!".

Quelle: https://www.infranken.de/lk/coburg/coburg-ihk-warnt-vor-gefaehrlichen-mails-klicken-sie-nicht-auf-den-link-art-5619781

13) Computer-Sperrungen angekündigt – so löst du das Problem

Hast du in jüngster Zeit eine Warnmeldung vom Microsoft Defender bekommen, laut der der Zugriff auf deinen Computer gesperrt wurde? Dann bist du damit nicht allein. Dennoch solltest du dir deine nächsten Schritte genau überlegen, denn die Meldung ist alles andere als ungefährlich.

„Der Zugriff auf diesen PC wurde aus Sicherheitsgründen gesperrt.“ Das ist die Meldung, mit der aktuell einige Windows-Nutzer konfrontiert werden. Der aufgeführte Grund: Auf dem Rechner wurde ein Trojaner-Virus entdeckt. Daher soll das in Windows integrierte Antivirus-Tool, Microsoft D**efender, diese Maßnahme ergriffen haben. Nur funktioniert das Sicherheitscenter nicht auf diese Weise. Wie kommt es also zu der Meldung?**

Das steckt hinter der angekündigten PC-Sperrung

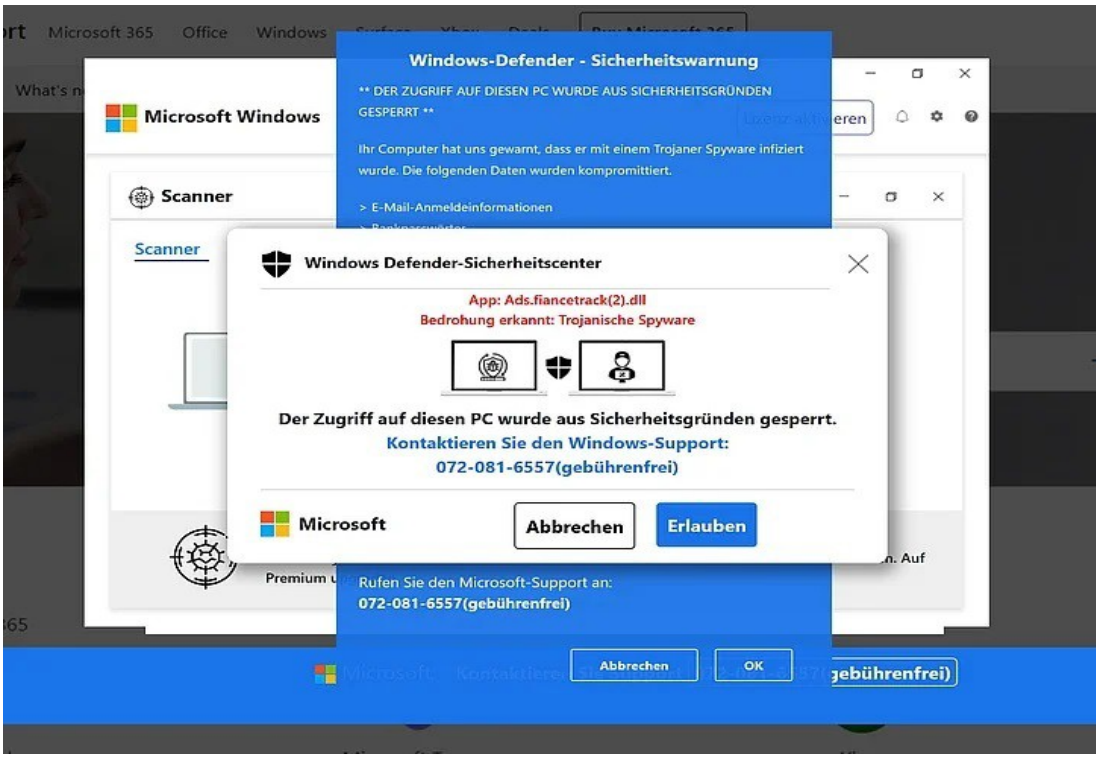
Bei der angeblichen PC-Sperrung handelt es sich um eine Phishing-Masche, die Kriminelle jedoch im Gegensatz zu den meisten Phishing-Kampagnen nicht mittels einer E-Mail realisieren. Stadtessen poppt die Defender-Warnung mitten auf dem Display auf – beinahe wie eine echte Defender-Info. Watchlist Internet geht davon aus, dass die dazugehörigen Pop-up-Fenster auf bestimmten eher unseriösen Internetseiten automatisch eingeblendet werden. Ähnlich, wie es bei Werbeanzeigen der Fall ist.

Das Pop-up-Fenster fordert den Empfänger dazu auf, den Windows-Support telefonisch zu kontaktieren. Am anderen Ende der Leitung befinden sich allerdings keineswegs Microsoft-Mitarbeiter, sondern Cyberkriminelle. Diese bieten ihren Opfern an, ihr nicht existierendes Virus-Probem zu lösen. Ihre Lösung nimmt allerdings die Form einer Fernwartungssoftware an, die den Betrügern einen praktisch uneingeschränkten Zugriff zu deinem Computer und somit auch zu deinen Daten und Konten gewährt. Daher solltest du die angegebene Telefonnummer auf keinen Fall anrufen.

Stattdessen solltest du versuchen, das Pop-up zu schließen. Gelingt dies nicht, könnte ein Neustart des Computers helfen. Auch das Löschen von Website-Daten, der Cookies und des Cache im Browser kann helfen. Sowie eine Neuinstallation des selbigen. Übrigens: Befindet sich tatsächlich ein Computervirus auf deinem Rechner, kannst du diesen unter Umständen selbst loswerden. Wie das geht, verrät unser Ratgeber zum abgesicherten Modus für Windows 10 und 11.

Die gleiche Masche funktioniert auch offline

Das Perfide an dieser Masche ist, dass selbst Nutzer, die ausschließlich vertrauenswürdige Websites aufrufen, nicht gänzlich geschützt sind. Erst gestern meldete das Polizeipräsidium Ulm einen Fall, im Rahmen dessen sich Kriminelle als Microsoft-Mitarbeiter ausgaben und einen Senioren über eine Schadsoftware auf seinem Computer unterrichteten. Ab hier ist das Vorgehen ähnlich: Auf dem Rechner des Opfers wird eine Fernwartungssoftware installiert und Daten werden ausgespäht. Konkret meldeten sich die Betrüger bei verschiedenen Bezahldiensten an und transferierten unter anderem mehrere hundert Euro auf ein bislang unbekanntes Konto.



Quelle: Computer-Sperrungen angekündigt www.inside-digital.de

Quelle: https://www.inside-digital.de/news/pc-sperrungen-angekuendigt-so-loest-du-das-problem

14) Fake im Netz – Winterschlussverkauf: So erkennen Sie einen Online-Betrug

Der Winterschlussverkauf ist eine spannende Zeit für Schnäppchenjäger, aber auch für Betrüger. So lassen sich Fake-Angebote von seriösen unterscheiden.

Im Internet ist der Winterschlussverkauf angekommen. Auf Online-Portalen werben Händler mit neuen Tiefpreisen. Warum auch nicht: Laut einer Umfrage des Finanzdienstleisters Revolut shoppen bereits 54 Prozent der Deutschen über das Internet.

Dennoch sind die Deutschen skeptisch, was die Sicherheit auf den Shopping-Plattformen angeht. Laut Revolut haben 25 Prozent der Befragten Angst davor, ihr Geld durch den Klau der Bankdaten zu verlieren.

Dass diese Furcht berechtigt ist, machen Verbraucherschützer klar. Sie warnen derzeit vor den Risiken durch Online-Betrüger. Einige Betrugsmaschen ließen sich relativ schnell erkennen, andere wiederum wirkten täuschend echt.

Diese Betrugsmaschen kommen besonders häufig vor

1. Scam

Bei einem Scam, zu Deutsch Betrug, überredet der Betrüger das Opfer dazu, Geld in Echtzeit zu überweisen. Das geschieht zum Beispiel dann, wenn sich der Scammer mittels geklauter Daten als Freund oder Familienmitglied ausgibt. Der Inhalt solcher Nachrichten kann unterschiedlich ausfallen, meist handelt es sich jedoch um einen angeblichen Notfall.

Kein Geld zurück

Wer eine Transaktion autorisiert und erst im Nachhinein den Betrug erkennt, bekommt das Geld nicht zurück. Der Grund: Das Opfer hat die Zahlung selbst autorisiert.

2. Betrügerische E-Mails

Nicht immer melden sich jedoch vermeintliche Freunde und Verwandte. Mit sogenannten Phishing-Mails, mit Textnachrichten auf dem Smartphone (Smishing) oder Telefonanrufen (Vishing), versuchen Betrüger bekannte Unternehmen oder Behörden nachzuahmen. In den meisten Fällen scheitern diese Versuche jedoch an einer fehlerhaften Rechtschreibung.

Wer gerne online einkauft, könnte auch schon über eine andere Phishing-Betrugsmasche gestolpert sein: Service-Webseiten, die Gutscheine für beliebte Produkte anbieten.

Post von der Bank

Eine Bank verlangt keine Zugriffsdaten per E-Mail. Sollte ein Login-Link in der Mail enthalten sein, handelt es sich um einen Betrugsversuch. Wer sich über den Urheber der Mail unsicher ist, kann diese an die Verbraucherzentrale Nordrhein-Westfalen weiterleiten und prüfen lassen (phishing@verbraucherzentrale.nrw).

3. Fake-Onlineshops

Rabattaktionen werden oft von Onlinehändlern in Newslettern oder als Werbebanner auf anderen Internetseiten beworben. Fake-Onlineshops können diese Werbekampagnen nutzen. Bei dieser Forme des Onlinebetrugs handelt es sich um einen auf den ersten Blick seriösen Onlineshop, der dem originalen Händler sehr ähnelt.

Woran sie gefälschte Onlineshops erkennen:

- **Das Vorhängeschloss-Symbol**: Seriöse Online-Shops erkennt man an dem Symbol eines Vorhängeschlosses links neben der URL. Ein Mausklick auf das Symbol zeigt etwa an, ob es sich bei der URL um eine sichere Verbindung handelt. In manchen Fällen erscheint anstelle des Vorhängeschlosses direkt der Warnhinweis "Nicht sicher".
- **HTTPS**: Die Buchstabenfolge steht für "Hyper Text Transfer Protocol Sevice" und gilt als Merkmal dafür, dass die Internetseite vertrauenswürdig ist.
- **Domainendungen**: Endet die Adresse nicht auf ".de", sondern auf "de.com.", ist die Seite ein Fake.
- **Zahlungsweise**: Beim Onlineshopping gestaltet sich der Bezahlvorgang in der Regel immer gleich: Sobald ein Produkt im Einkaufskorb liebt, stehen verschiedene Zahlungsmethoden zur Auswahl. Stutzig sollte man werden, wenn lediglich die Option Vorkasse angeboten wird. Das könnte bedeuten, dass die Ware nach der Überweisung nicht zugestellt wird.
- **Extrem günstiges Angebot**: Sind die Produktpreise im Vergleich zu anderen Onlinehändlern sehr günstig, könnte es sich um eine Betrugsmasche handeln. Ein solches Schnäppchen wäre aufgefallen, gerade wenn es sich hierbei um beliebte Elektrogeräte oder Kleidung handelt.

- **Gefälschte Gütesiegel**: Bewirbt ein Onlineshop in seinem Internetauftritt auffällig platzierte und unbekannte Gütesiegel, könnte es sich um eine betrügerische Seite handeln. Ob das Siegel echt ist, lässt sich ganz einfach mit einem Mausklick testen. In der Regel sind Siegel verlinkt und führen auf die Internetseite des Siegel-Betreibers.
- **Kundenbewertungen**: Bestehen die meisten Kommentare auf einer Internetseite nur aus überschwänglichem Lob, ist Vorsicht geboten. Auch sich ähnelnde User-Namen oder sehr unterschiedliche Bewertungen sollten misstrauisch stimmen. Sollte eine User-Bewertung den Betrug benennen, sollte dieser Vorwurf auch ernst genommen werden.
- **Fake-AGB**: Sobald die Geschäftsbedingungen des Onlinehändlers in einem fehlerhaften Deutsch verfasst sind, ist Vorsicht geboten. Fehlt die allgemeine Geschäftsbedingung völlig, ist die Seite ein Fake.
- **Unvollständiges Impressum**: Das Impressum listet in der Regel alle wichtigen Informationen über das Unternehmen auf. Fehlen im Impressum zum Beispiel Angaben zum Registergericht, der Registernummer und der Steuernummer, ist der Onlineshop mit hoher Wahrscheinlichkeit eine Fälschung.

Fakeshop-Finder

Die Verbraucherzentrale bietet unter www.verbraucherzentrale.de/fakeshopfinder eine Suchfunktion für Onlineshops an. Hierfür muss URL des betroffenen Händlers in ein Suchfeld eingegeben werden. Die Seite untersucht die Internetseite auf ihre Echtheit und zeigt etwa die wichtigsten Angaben des Impressums und Nutzerbewertungen an.

Handlungsschritte für Betrugsopfer

Wer Opfer eines Betruges im Internet wurde, sollte sofort handeln und folgende Schritte unternehmen:

- Sämtliche Bankkonten und Karten sperren lassen
- Kundenservice der Bank kontaktieren und unberechtigte Abbuchungen zurückbuchen lassen
- Strafanzeige bei der Polizei erstatten (online möglich unter https://online-strafanzeige.de)
- Identitätsdiebstahl bei der Schufa und anderen Behörden melden
- Mögliche Rechnungen und Inkassoschreiben schriftlich beantworten und die Kopie der Strafanzeige beifügen

Quelle: https://www.t-online.de/digital/internet-sicherheit/sicherheit/id_100117172/winterschlussverkauf-so-entlarven-sie-fake-onlineshops.html

15) DHL warnt Kunden vor Betrug – plötzliche Mitteilung „nicht von uns“

Wartest du auf ein DHL-Paket, könntest du mit einem Mal eine alarmierende SMS erhalten. Jedoch solltest du aktuell nicht übereilt handeln.

Aktuell kursiert eine Betrugsmasche, die es auf die Kundinnen und Kunden von **DHL** abgesehen hat. In den echt wirkenden SMS werden die Betroffenen dazu aufgefordert, sensible Daten von sich preis zu geben. Ein Detail sorgt dafür, dass sich die Nachricht kaum von einer echten Mitteilung des Postdiensts unterscheiden lässt.

DHL fragt keine Adressen ab und will auch nicht dein Geld

Auf der Facebook-Seite von DHL Paket warnen die Mitarbeitenden aktuell eindringlich vor dem Betrugsversuch. Beim sogenannten Smishing, ein Kofferwort aus „SMS“ und „Phishing“, versuchen Kriminelle sensible Informationen über schädliche SMS-Links zu erhalten.

In diesem Fall geben sie sich als DHL-Dienstleister aus und verlangen, dass du entweder deine Adressdaten aktualisierst oder gar eine Zahlung über den SMS-Link leistest. Das die Daten oder gar Geldbeträge eben nicht bei DHL landen, ist selbsterklärend.

Falsche SMS im echten Verlauf machen Masche besonders perfide

Besonders gefährlich ist, dass die betrügerischen Mitteilungen teilweise, vermutlich durch Spoofing, in echten, älteren SMS-Chats mit DHL auftauchen. Mithilfe von Spoofing kann eine Rufnummer so getarnt werden, dass sie einer anderen gleicht. So kann der Laie kaum erkennen, dass es sich hierbei um eine Gaunerei handelt.

Daher erklären die Social Media-Beauftragen auf Facebook: „Wir fordern dich grundsätzlich nie per SMS zu Zahlungen oder (Adress-)Datenänderungen auf.“ Am besten löschst du die Nachricht. Hast du Zweifel, rufe die DHL-Webseite auf und kontaktiere den offiziellen Kundensupport. Willst du deine DHL-Sendungsnummer herausfinden, können auch wir dir weiterhelfen.

Quelle: https://www.futurezone.de/digital-life/article421385/dhl-warnt-kunden-vor-betrug-ploetzliche-mittelung-nicht-von-uns.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

16) Behörden warnen vor Android-App: Perfider Trojaner könnte dein Konto leerräumen

Der Android-Trojaner Godfather machte erst jüngst Schlagzeilen. Nun warnen auch BaFin und BSI vor der Malware.

Im Laufe der vergangenen Wochen hat ein altbekannter **Handy-Trojaner** abermals stark an Aufmerksamkeit dazugewonnen. Grund dafür war sein Einsatz bei einer Android-App, die in erster Linie auf türkische Nutzerinnen und Nutzer abzielte. Mittlerweile ist die Malware zu einem solchen Risiko herangewachsen, dass sie auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nicht länger ignorieren kann.

Handy-Trojaner: Jetzt warnen BaFin und BSI

Insgesamt 400 Banking- und Krypto-Apps soll der Trojaner namens Godfather angreifen. Unter ihnen befinden sich, so die Bundesanstalt, auch einige Anwendungen von Betreibern aus Deutschland. „Wie genau die Software auf die infizierten Endgeräte von Verbraucherinnen und Verbrauchern kommt, ist unklar“, heißt es in einer offiziellen Mitteilung. „Bekannt ist, dass Godfather gefälschte Websites von regulären Banking- und Krypto-Apps anzeigt. Loggen sich Verbraucher über diese Websites ein, werden ihre Login-Daten an die Cyber-Kriminellen übermittelt.“

Zudem versende der Android-Trojaner Push-Benachrichtigungen. Diese sollen es den Betrügerinnen und Betrügern hinter der Software ermöglichen, an deine Zwei-Faktor-Authentifizierung zu gelangen. Auf diese Weise könnten sie sich direkten Zugang zu deinen Bankkonten und deiner Krypto-Wallet verschaffen.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte im Voraus vor Godfather gewarnt. Den Anstoß dazu gab ein Bericht des IT-Sicherheitsunternehmens Cyble, der auf Godfather und der damit einhergehenden Android-App MYT Müzik aufmerksam

machte. Mittlerweile nehme die Malware Nutzerinnen und Nutzer in rund 16 Ländern ins Visier.

App-Sicherheit vom BSI

Neben seiner Warnung an die Bevölkerung hat das BSI vor einem Monat ein umfangreiches Video herausgegeben. Es soll Kindern und Erwachsenen dabei helfen, sich im Umgang mit Apps auf unterschiedlichen Plattformen keinen Risiken auszusetzen.

Wir verraten dir zudem, auf welche Indizien du achten musst, um einen Trojaner erkennen zu können.

Quelle: https://www.futurezone.de/apps/article416122/handy-trojaner-behoerden-warnen-vor-perfider-android-app.html

17) POL-RT: Warnung vor Erpressungsmasche Sextortion

Sextortion: Wenn der Internet-Flirt zum Albtraum wird - Das Polizeipräsidium Reutlingen warnt vor erpresserischen Internet-Bekanntschaften und Emails

Sextortion, ein zusammengesetzter Begriff aus den englischen Wörtern Sex und Extortion (Erpressung) ist eine Betrugsmasche, die im Internet kursiert, Frauen wie Männer betrifft, und auch im Zuständigkeitsbereich des Polizeipräsidiums Reutlingen immer wieder zur Anzeige gebracht wird.

Was als vermeintlich harmloser Flirt beginnt, endet mit hohen Geldforderungen. Die meist männlichen Opfer erhalten über soziale Netzwerke eine Einladung oder eine Freundschaftsanfrage einer ihnen unbekannten Frau. Nach der Annahme der Anfrage und einer ersten Unterhaltung schlagen die Betrüger vor, in einen Video-Chat zu wechseln. Dort bringen sie die Geschädigten dazu, sich vor der Webcam auszuziehen und sexuelle Handlungen an sich vorzunehmen. Ohne dass das Opfer es bemerkt, wird die Übertragung aufgezeichnet. Anschließend werden hohe Geldsummen gefordert und gedroht, den Mitschnitt ansonsten zu veröffentlichen.

Neben dieser beschriebenen klassischen Masche gibt es aber auch andere Varianten. So werden Computer, Tablets oder Smartphones von Personen, die auf präparierten Webseiten mit pornografischen Inhalten surfen, mit einer Malware infiziert. Diese aktiviert die Webcam und filmt die ahnungslosen Opfer währenddessen. Die häufig kompromittierenden Filmaufnahmen werden an die Täter übermittelt, die ihre Opfer anschließend unter Drohung, das Filmmaterial zu veröffentlichen oder an die ebenfalls gestohlenen Freundeslisten zu senden, erpressen.

Eine weitere, häufig registrierte Form ist die sogenannte Spam-Variante. Dabei werden die vorher beschriebenen Erpressungsversuche als Spam wahllos an zahlreiche Personen als "leere Drohung" versandt. Die kriminellen Absender behaupten, von ihren Opfern kompromittierende Sexvideos aufgenommen zu haben und drohen mit der Veröffentlichung der Videos, falls die geforderten Geldbeträge nicht bezahlt werden. Meist werden diese Emails bereits vom jeweiligen Email-Anbieter erkannt und automatisch in den Spam-Ordner sortiert. In diesen Fällen ist der Computer der Betroffenen weder infiziert noch befinden sich die Kriminellen tatsächlich in Besitz von kompromittierendem Material.

Die Polizei rät:

- Nehmen Sie keine Freundschaftsanfragen von unbekannten Personen an.
- Stimmen Sie nicht vorschnell einem Videochat zu, wenn Sie Ihr Gegenüber nicht kennen. Kleben Sie im Zweifel Ihre Webcam ab, um lediglich verbal zu kommunizieren und das Geschehen zu beobachten.

- Stimmen Sie keinen Entblößungen oder intimen Handlungen zu, wenn Sie die Person erst seit Kurzem kennen.

- Seien Sie besonders zurückhaltend mit der Online-Veröffentlichung von persönlichen Daten wie Geburtsdatum, Anschrift oder gar Arbeitgeber.

- Prüfen Sie regelmäßig Ihre Privatsphäre-Einstellungen in Ihrem Account.
- Halten Sie die Betriebs- und Virenschutzsysteme auf Ihrem Laptop, Tablet, Computer oder Smartphone stets auf dem aktuellen Stand. Bitte bedenken Sie, dass mittels einer Schadsoftware Ihre Webcam problemlos aktiviert werden kann, um Sie zu filmen.

Sollte es dennoch bereits zu einer Erpressung gekommen sein:

- Überweisen Sie kein Geld. Die Erpressung hört nach einer Zahlung in der Regel nicht auf.
- Brechen Sie den Kontakt zu der Person sofort ab und reagieren Sie nicht auf Nachrichten.
- Sichern Sie die Chatverläufe und Nachrichten, ggf. per Screenshot und erstatten Sie Anzeige bei der Polizei!

Weitere Tipps und Hinweise erhalten Sie im Internet unter www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sextortion/

Quelle: https://www.presseportal.de/blaulicht/pm/110976/5414773

18) Dauerärgernis Telefonwerbung

Sie ärgern sich über Telefonwerbung? Das können wir gut verstehen. Unerwünschte Werbeanrufe sind für viele Menschen ein tägliches Ärgernis. Bei der Bundesnetzagentur beschweren sich jedes Jahr Zehntausende. Fast 65.000 Beschwerden gingen 2022 bei der Behörde ein, die über eine Million Euro an Bußgeldern verhängt hat.

Das Wichtigste in Kürze

1. Telefonwerbung ist für viele Verbraucherinnen und Verbraucher noch immer ein tägliches Ärgernis, dabei ist sie oft schlichtweg verboten. Im vergangenen Jahr hat die Bundesnetzagentur Bußgelder in Höhe von mehr als eine Million Euro verhängt.
2. Die meisten Verträge, die am Telefon geschlossen werden, sind leider rechtsgültig. Sie müssen nicht zusätzlich schriftlich bestätigt werden.
3. Ausnahmen gelten nur für Telekommunikations-, Energielieferungs- (Strom, Gas) und Gewinnspielverträge.

Stand: 13.01.2022

Telefonwerbung ist noch immer ein tägliches Ärgernis, dabei ist sie meistens schlichtweg verboten. Nur wenn Sie ausdrücklich zugestimmt haben, darf ein Unternehmen Sie zu Werbezwecken anrufen.

Zwar wurden vor 10 Jahren mit dem Gesetz gegen unseriöse Geschäftspraktiken, dem sogenannten Anti-Abzocke-Gesetz, die Vorschriften zur Bekämpfung unerlaubter Telefonwerbung verschärft, doch dessen Auswirkungen sind kaum zu spüren. Die Zahl der Beschwerden bei der Bundesnetzagentur zu unerlaubter Telefonwerbung ist nach wie vor hoch. Im Jahr 2022 erreichte sie mit 64.704 schriftlichen Beschwerden wieder einen Höchstwert. 2021 waren es sogar 79.702.

Warum ist unerlaubte Telefonwerbung ein Problem?

Die Gefahr ist groß, dass Verbraucherinnen und Verbrauchern durch offensive Verkaufstaktiken und unlautere Tricks am Telefon unliebsame Verträge untergeschoben werden.

Verträge über die Registrierung bei Gewinnspielen müssen deswegen schon länger schriftlich bestätigt werden. Seit Dezember 2021 gilt das auch für am Telefon abgeschlossene Telekommunikationsverträge, also zum Beispiel DSL- oder Mobilfunkverträge. Diese werden erst wirksam, wenn Verbraucherinnen und Verbraucher sie nach Erhalt der Vertragszusammenfassung in Textform genehmigen. Für Energielieferungsverträge außerhalb der Grundversorgung wurde das sogenannte Textformerfordernis im Juli 2021 eingeführt.

Auch, wenn es erfreulich ist, dass Verträge mittlerweile in einigen Bereichen nicht mehr einfach am Telefon abgeschlossen werden können, gelten diese Regelungen für viele Branchen weiterhin nicht. Verträge über Finanzprodukte oder Versicherungen, Zeitungsabos oder Nahrungsergänzungsmittel können am Telefon noch immer wirksam mündlich abgeschlossen werden. Verbraucherinnen und Verbrauchern bleibt in diesen Fällen nur das Widerrufsrecht. Es ist also nicht verwunderlich, dass Unternehmen weiterhin zum Hörer greifen.

Unter welchem Vorwand wird angerufen?

Telefonwerbung ohne Ihre vorherige ausdrückliche Einwilligung ist wettbewerbswidrig. Dies gilt beispielsweise auch

- für telefonische Befragungen zur Kundenzufriedenheit,
- Anrufe von Meinungsforschungsinstituten,
- Telefonanrufe zur Ankündigung oder Vereinbarung von Vertreterbesuchen,
- Meinungsumfragen, die mittelbar der Verkaufsförderung dienen,
- und Gewinnmitteilungen mit Rückrufaufforderung unter 0900er-Nummern.

Auch Bestandskunden eines Unternehmens dürfen nicht ohne ihre Einwilligung zu Werbezwecken angerufen werden. Im Dezember 2022 verhängte die Bundesnetzagentur beispielsweise ein Bußgeld in Höhe von 142.000 Euro gegen ein Call-Center, das unter im Auftrag eines Telekommunikationsanbieters Verbraucherinnen und Verbraucher anrief, um Produkte und Services zu verkaufen.

Einige Anrufer bedienen sich immer dreisterer Methoden. Inzwischen geben sie sich als Anwälte, Behördenpersonal oder sogar Verbraucherzentralen aus. Als Tarnung schalten sie die tatsächliche Rufnummer der angegebenen Institution oder Behörde vor. Vielfach zeigt ein Rückruf, dass die Nummer nicht existiert.

Was kann ich dagegen unternehmen?

Nach unserer Einschätzung sind die Beschwerden, die der Bundesnetzagentur und den Verbraucherzentralen vorliegen, nur die Spitze des Eisbergs, denn viele Betroffene melden belästigende Werbeanrufe gar nicht. Das sollten sie aber tun.

Unser Tipp

Wer Werbeanrufe erhält, ohne dass eine Einwilligung vorliegt oder obwohl ein Werbewiderruf ausgesprochen wurde, kann sich bei der Bundesnetzagentur eine Beschwerde einreichen. Um die Täter überführen zu können, sind möglichst präzise und detaillierte Angaben hilfreich. Eine gute Dokumentation des Gesprächs ist daher besonders wichtig.

Was sollte die Politik tun?

Belästigungen mit unerlaubten Werbeanrufen – sogenannten Cold Calls – können von der Bundesnetzagentur verfolgt werden. Die mögliche Bußgeldhöhe liegt bei 300.000 Euro. Dennoch reißt der Strom unerwünschter Anrufe nicht ab. Die unlautere Vertriebsmethode lohnt sich für Unternehmen leider immer noch.

Daher fordern wir weiterhin, die sogenannte Bestätigungslösung für alle Vertragsarten anzuwenden. Das heißt: Wer bei einem unerwünschten Werbeanruf einem Vertrag zustimmt, muss ihn danach noch einmal in Textform bestätigen

Unser Rat

- Überprüfen Sie, ob Sie bei Vertragsschluss im Kleingedruckten eines Zeitschriftenabonnements, eines Telefon- oder Versicherungsvertrags Werbeanrufen zugestimmt haben. Korrigieren Sie dies und informieren Sie den Anbieter darüber. Dafür können Sie unseren Musterbrief nutzen.
- Geben Sie Ihre Telefonnummer nur an Unternehmen weiter, wenn dies dringend erforderlich ist, und streichen Sie von vornherein Klauseln aus Verträgen, die die Speicherung und Nutzung Ihrer Daten zu Werbezwecken erlauben.
- Schließen Sie am Telefon grundsätzlich keinerlei Verträge ab, denn diese sind in den meisten Fällen rechtsgültig.
- Sie haben sich am Telefon überrumpeln lassen und einen Vertrag abgeschlossen? Unsere Juristinnen und Juristen helfen weiter.

Quelle: https://www.vzhh.de/themen/telefon-internet/daueraergernis-telefonwerbung

Anwenderinformationen:

1) Schwere Sicherheitslücken bei Samsung-Smartphones: Galaxy-Besitzer müssen dringend reagieren

Aktuell müssen Besitzer von Samsung-Galaxy-Geräten aufpassen. Angreifer können über zwei Lücken im Galaxy Store Schadcode ausführen. Nutzer sollten daher nun reagieren.

Viele Besitzer von Galaxy-Smartphones sollten aktuell zwei Sicherheitslücken im Galaxy App Store beachten. Wie die Experten der NCC Group kürzlich bekanntgaben, können Angreifer darüber Schadcode auf den Handys der Opfer ausführen.
Die Schwachstelle CVE-2023-21433 sorgt dafür, dass Anwendungen jede derzeit im Galaxy Store verfügbare App ohne Wissen des Besitzers installieren können. Ein Angreifer könnte somit manipulierte Software, die er zuvor in den Galaxy Store geschleust hat, auf den Smartphones der Opfer verteilen.
Dieses Problem tritt nur bei Android 12 und niedriger auf. Nutzer von Android 13 sind nicht betroffen.

Update nötig: Sicherheitsprobleme im Galaxy App Store von Samsung

Das zweite Problem ist CVE-2023-21434. Es geht dabei um den Filter für Webansichten im Galaxy Store. Dieser limitiert eigentlich, welche Domains angesurft werden können. Allerdings ist er nicht korrekt konfiguriert, weshalb auch bösartige Seiten über einen Link, beispielsweise über Google Chrome oder einen manipulierte App, geöffnet werden können. Darüber kann dann JavaScript ausgeführt werden.
Die Forscher haben Samsung bereits Ende November beziehungsweise Anfang Dezember über die Lücken informiert. Das Unternehmen hat inzwischen reagiert und am 1. Januar ein Update für den Galaxy App Store veröffentlicht (Version 4.5.49.8). Falls Sie ein Galaxy-Smartphone besitzen und den Patch noch nicht installiert haben, sollten Sie dies umgehend nachholen.
Quelle: https://www.chip.de/news/Gefahr-fuer-Galaxy-Besitzer-Schwere-Sicherheitsluecken-bei-Samsung-Smartphones_184625887.html

2) Vorsicht: Trojaner übernimmt Kontrolle über deinen Rechner – er nutzt einen ungewöhnlichen Weg

Ein Windows-Virus kann auf unterschiedliche Arten in dein System gelangen. Neuerdings nutzen Tunichtgute dazu sogar OneNote-Dateien.

Mit immer neuen Updates wollen Unternehmen wie Microsoft die Sicherheit ihrer Community gewährleisten. Allerdings sind die Schöpferinnen und Schöpfer moderner Malware mindestens ebenso kreativ wie jene, die dich vor dem schädlichen Code schützen wollen. So finden sie immer neue Wege, ihre Software auf deinen Rechner zu bringen. Ein neuer **Windows-Virus** nutzt dazu einen besonders perfiden Weg.

Windows-Virus: Phishing-Mails werden immer kreativer

Phishing-Mails sind ein besonders beliebtes Werkzeug, um Trojaner in fremde Systeme einzuschleusen. Dabei spielt es meist keine Rolle, ob du die Nachricht auf einem PC oder deinem Smartphone öffnest. Denn die Software ist meist fortschrittlich genug, um sich an ihre Umgebung anzupassen, und die vorhandenen Sicherheitslücken für ihre Zwecke nutzbar zu machen.

Zum Teil dient die Malware dabei einzig und allein dem Zweck als Einfallstor. Will heißen, dass die Absenderin oder der Absender mit ihrer Hilfe erst den eigentlichen Windows-Virus auf deinem Rechner installieren. Dieser wiederum ermöglicht es anschließend, je nach bedarf Dateien, Passwörter oder gar ganze Krypto-Wallets abzugreifen.

In der Vergangenheit haben Tunichtgute ihre E-Mails dazu etwa mit schädlichen Links oder Buttons versehen. Sie geben vor, dich zur Anmeldeseite eines genutzten sozialen Netzwerks oder sogar deiner Bank weiterzuleiten. Mittlerweile nutzen sie dazu aber noch eine perfidere Methode: als Microsoft OneNote-Dateien getarnte Anhänge.

Microsoft OneNote als trojanisches Pferd

So warnte etwa das Team von Trustwave schon in einem Ende 2022 veröffentlichten Beitrag vor „trojanisierten OneNote-Dokumenten“. Auch die Expertinnen und Experten von Bleeping Computer haben diese Thematik mittlerweile aufgegriffen und machen auf die Gefahr aufmerksam, die von den kompromittierenden Dateien ausgeht.

Das Problem: OneNote ermöglicht das Anhängen von Dateien in das integrierte Notizbuch. Wählt man diese anschließend mit einem Doppelklick aus, werden diese ausgeführt – auch wenn es sich dabei tatsächlich um einen Windows-Virus handelt.

„Bedrohungsakteure missbrauchen diese Funktion, indem sie bösartige VBS-Anhänge anhängen, die das Skript automatisch starten, wenn sie doppelt angeklickt werden, um Malware von einer entfernten Website herunterzuladen und zu installieren. Die Anhänge sehen jedoch wie ein Dateisymbol in OneNote aus, sodass die Bedrohungsakteure die eingefügten VBS-Anhänge mit einer großen ‚Doppelklick zum Anzeigen der Datei‘-Leiste überlagern, um sie zu verbergen.“

Bleeping Computer

Schiebt man die Anzeige-Leiste zur Seite, so Bleeping Computer, werden die angehängten, schädlichen Dateien sichtbar.

So schützt du dich richtig

Willst du dich vor perfiden Vorgehensweisen wie dieser schützen, solltest du dich an einige altbewährte Methoden halten. In der Regel senden Banken, soziale Netzwerke und Paketdienste nämlich keine OneNote-Dateien mit. Ergo: Kannst du diese Anhänge in der Regel getrost ignorieren.

Ähnliches gilt übrigens für in der E-Mail verbaute Links und Buttons. Sie sollen zum Klicken animieren, dienen aber in vielen Fällen der Installation eines iOS-, Android- oder Windows-Virus. Behaupten Absenderin oder Absender also, dein Konto sei kompromittiert worden und du müsstest dich dringend weiterklicken, halte lieber einen kurzen Moment inne.

Wähle einen kleinen Umweg, statt der Aufforderung blind Folge zu leisten. Öffne den Browser und anschließend die offizielle Webseite des jeweiligen Dienstes. Dort kannst du dich sicher anmelden, ohne Gefahr zu laufen, dass es sich bei der Seite um einen Klon handelt, der lediglich deine Daten abgreifen will. Bist du eingeloggt, kannst du dir nochmal selbst ein Bild von den Behauptungen aus der E-Mail machen.

Quelle: https://www.futurezone.de/digital-life/article418981/windows-virus-trojaner-macht-sich-ungewoehnlichen-weg-zunutze.html

3) Änderung für Mindestbestellwert - Amazon: Gratis-Versand und Music Unlimited werden teurer

Drei große Änderungen beim Versandriesen Amazon: Der Mindestbestellwert für Gratis-Versand steigt, Music Unlimited wird teurer und Amazon Smile beendet.

Offenbar stehen im Jahr 2023 beim Versandhändler Amazon einige große Änderungen bevor. Die erste betrifft den Mindestbestellwert, den man für eine **Gratis-Lieferung ohne Prime-Abo** erreichen muss. Zuletzt lag dieser bei 29 Euro und könnte zukünftig auf 39 Euro erhöht werden. Das berichtet zumindest die Seite Caschys Blog, die eine aktualisierte Angabe auf Amazons Supportwebseite entdeckt hat.

Ob es sich dabei wirklich um eine bevorstehende Erhöhung des Mindestbestellwerts beim Gratis-Versand handelt, ist aktuell noch nicht sicher. Amazon hatte die Preise kurz darauf wieder zurückgesetzt. Es könnte sich also sowohl auf einen Fehler als auch auf vorschnelles Handeln zurückführen lassen.

Das letzte Mal, als der Mindestbestellwert auf Amazon gestiegen ist, liegt mittlerweile über acht Jahre zurück. Damals erhöhte man den nötigen Warenwert **von 20 Euro auf 29 Euro** und erntete damit viel Kritik der Nutzer*innen. Eine erneute Erhöhung würde wohl eine ähnliche Reaktion hervorrufen. Zumal die Kosten für das Prime-Abo mittlerweile ebenfalls gestiegen sind.

Amazon Music Unlimited wird teurer

Eine weitere Preiserhöhung ist bei Amazon bereits sicher. Die Kosten für **Amazon Music Unlimited** steigen nach neuesten Informationen ebenfalls, und zwar ab dem **21. Februar 2023.** Der Preis für das normale Abo wird auf 10,99 Euro statt der bisherigen 9,99 Euro monatlich erhöht. Für den Studententarif steigt der Preis von 4,99 Euro auf 5,99 Euro pro Monat.

Auch der Familientarif ist betroffen, mit dem bis zu sechs Personen das Musik-Angebot von Amazon nutzen können. Dieser kostet zukünftig 16,99 Euro monatlich. Für das Jahresabo zahlt man hingegen 169 Euro. Wer allerdings vor dem 21. Februar ein Abo bucht, kann bis zum Ablauf noch den **alten Preis zahlen.**

Die Preisänderungen werden auf einer Hilfeseite von Amazon ersichtlich. Im Sommer 2022 erhöhte man bereits die Preise für Amazon Music Unlimited, wenn dieses mit einem aktiven Prime-Abo gebucht wird. Nun sind auch Kund*innen ohne Prime-Abo betroffen.

Amazon beendet Spendenprogramm Smile

Zu guter letzte machte noch die Änderung die Runde, dass Amazon sein Spendenprogramm **Amazon Smile** einstellen wird. Hier konnte man bisher verschiedene Hilfsorganisationen auswählen, die bei einem Kauf auf Amazon automatisch Spenden erhalten.

Ab dem 20. Februar wird es dieses Angebot aber nicht mehr geben, nachdem es etwa sechs Jahre lang in Deutschland aktiv war. Aus einem Blog-Post geht hervor, dass man sich auf Projekte mit "größerem Einfluss" konzentrieren wolle.

Zwar konnten in Deutschland laut Amazon bisher **27 Millionen Euro** an verschiedene Organisationen gespendet werden. Doch gerade durch die Vielzahl an teilnehmenden Projekten kam nicht die erwünschte Summe bei jedem einzelnen an, so das Unternehmen.

Amazon plant, allen teilnehmenden Organisationen dieses Jahr eine **letzte, einmalige Spende** zu überweisen. Diese soll in Höhe von drei Monaten an Spenden aus dem Jahr 2022

ausfallen. Ab Februar sollen Wohltätigkeitsorganisationen zudem die Möglichkeit bekommen, direkt um finanzielle Unterstützung auf Amazon zu bitten.

Quelle: https://www.pc-magazin.de/news/amazon-aenderungen-2023-gratis-versand-mindestbestellwert-steigt-music-unlimited-teurer-smile-beendet-3204229.html?utm_source=nachrichten-NL&utm_medium=newsletter

4) Schwere Sicherheitslücken – Microsoft Edge: BSI warnt vor Nutzung des Browsers

Der Microsoft-Browser Edge gehört seit Jahren zum Lieferumfang von Windows. Aktuell sollten Sie aber lieber die Finger davon lassen. Das Bundesamt für Sicherheit in der Informationstechnik warnt vor gefährlichen Schwachstellen!

Die meisten Internet-Browser unterscheiden sich nur in Details voneinander. Für viele Menschen spielt es daher keine Rolle, mit welchem Programm sie durchs Netz navigieren, sie nehmen einfach, was da ist. Im Fall von Windows ist das der Edge-Browser, den Microsoft seit Jahren standardmäßig mit seinem Betriebssystem ausliefert. Ausgerechnet vor dem warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun allerdings. Sicherheitsexperten haben in der Software schwere Schwachstellen entdeckt, die ein hohes Sicherheitsrisiko für Nutzerinnen und Nutzer darstellen.

Hacker können aus der Ferne angreifen

Demnach ermöglichen die Sicherheitslücken im Edge-Browser potenziellen Angreifern per Fernzugriff das Ausführen beliebigen Programmcodes auf den Rechnern ihrer Opfer. Auf diese Weise ist es Eindringlingen möglich, ihre Privilegien für den Zugriff auf das System zu erweitern und so Daten zu stehlen oder zu manipulieren. Das Problem betrifft laut offizieller Ankündigung sowohl Edge unter Windows als auch die macOS-Version für Apple-Computer. Microsoft hat bereits auf die Meldung der Sicherheitslücken reagiert und schließt diese in einem aktuellen Update mit der Versionsnummer 109.0.1518.49.

Edge-Update sofort installieren

Um die aktuelle Fassung der Software zu installieren, reicht es für gewöhnlich, den Browser einfach neu zu starten. Trotzdem sollten Sie auf Nummer sicher gehen und die aktuell installierte Version im Einstellungsmenü überprüfen. Im Zweifelsfall stoßen Sie das Update dort auch manuell an. Wer sich angesichts des aufgetretenen Sicherheitsrisikos ganz vom Edge-Browser verabschieden möchte, guckt unter Windows in die Röhre. Das Programm ist wie schon der Vorgänger Internet Explorer fest in das System integriert und lässt sich nicht einfach deinstallieren. Allerdings gibt es Wege, um die Software zu deaktivieren und aus dem Start-Menü sowie der Taskleiste zu entfernen.

Quelle: https://www.computerbild.de/artikel/cb-News-Sicherheit-Microsoft-Edge-BSI-warnt-Nutzung-Browser-Sicherheitluecke-35070501.html

5) Plötzlich WhatsApp-Profilbild weg? Das kann 8 verschiedene Gründe haben

Bei WhatsApp kann das Profilbild auch von ein auf den anderen Tag verschwinden. Neben einer einfachen Entfernung durch dein digitalen Gegenübers, gibt es jedoch auch andere Ursachen für den Umstand.

Haben einige oder augenblicklich alle deine Kontakte **kein WhatsApp-Profilbild** mehr, können mehrere Ursachen dahinterstecken. Während es sich manchmal nur um einen

kurzweiligen Fehler handelt, kann es manchmal auch deine eigene Schuld sein. Wir verraten dir, wie du den Grund erkennst und was du tun kannst.

WhatsApp-Profilbild weg: 8 Gründe im Überblick

Es gibt viele Ursachen, die dazu führen können, dass du plötzlich kein WhatsApp-Profilbild mehr entdecken kannst. Alle findest du in der folgenden Übersicht. Aber Vorsicht: Einer davon hat mit dir zu tun und dürfte dir daher ganz und gar nicht gefallen:

1. Dein Kontakt hat vielleicht **gar kein WhatsApp-Profilbild hochgeladen** oder sein Altes gelöscht.
2. Ein interner **Server-Fehler** kann ebenso Schuld sein. In diesem Fall kannst du nichts machen, du musst auf WhatsApp warten.
3. Ein **WhatsApp-Update** hat nicht so funktioniert, wie es sollte. Auch in diesem Fall ist es ratsam, darauf zu warten, bis der Fehler vom Messengerdienst selbst behoben wird. Auch ein Neustart deines Handys bietet sich an.
4. Dein Kontakt hat ein **neues Handy** oder dich aus einem anderen Grund **nicht mehr in seinem Adressbuch** als WhatsApp-Kontakt hinterlegt. Du kannst ihn fragen, ob er dich noch gespeichert hat.
5. Der Kontakt hat seine **Telefonnummer geändert**. Hast du diese noch nicht gespeichert, ist möglicherweise sein WhatsApp-Profilbild weg.
6. Der Freund oder Bekannte hat seine **Privatsphäreeinstellungen in WhatsApp angepasst**. Unter „Einstellungen“ > „Account“ > „Datenschutz“ kann jeder festlegen, wer das eigene Profilbild sehen soll, auch „niemand“ ist möglich.
7. Das Profilbild wurde von dem Nutzer **gerade geändert**. Dann kann es etwas dauern, bis du sein neues Bild sehen kannst.
8. Der Kontakt hat dich **blockiert**. Damit ist für dich auch sein WhatsApp-Profilbild weg.

Und was nun? Diese 6 Maßnahmen können das Problem lösen

Hier fassen wir dir noch einmal zusammen, was du tun kannst, wenn du kein WhatsApp-Profilbild bei einem oder mehreren deiner Kontakte entdeckst:

1. Warte einige Zeit ab. Bei Serverfehlern oder einem frischen WhatsApp-Profilbild kann sich das durchaus lohnen.
2. Starte dein Handy neu und prüfe die App auf ausstehende Aktualisierungen.
3. Gibt es neben den verschwundenen Profilbild auch weitere Fehler, lohnt sich eventuell die Neuinstallation der Anwendung.
4. Schreibe den Kontakt an und prüfe so, ob die Nummer noch aktuell ist.
5. Fürchtest du bei WhatsApp blockiert worden zu sein, kannst du das auf diese Weise herausfinden. Immerhin weißt du dann, ob du das Problem selbst bist oder nicht. Wirst du negativ überrascht, solltest du mit der Person vielleicht ein Gespräch suchen. Aber Vorsicht: Streit in WhatsApp-Nachrichten kann gefährlich sein.
6. Außerdem kann es helfen, die Telefonnummer des Kontakts zu aktualisieren. Öffne dafür dein Adressbuch außerhalb von WhatsApp und passe die Nummer so an, dass statt der Vorwahl (für Deutschland +49 oder 0049) eine 0 dort steht oder umgekehrt. Das kann die Lösung dafür sein, wenn du plötzlich kein WhatsApp-Profilbild mehr entdeckst.

Quelle: https://www.futurezone.de/apps/article226990861/whatsapp-profilbild-ploetzlich-weg.html

6) Spam-Anrufe – Diese Nummern sollten Sie ignorieren

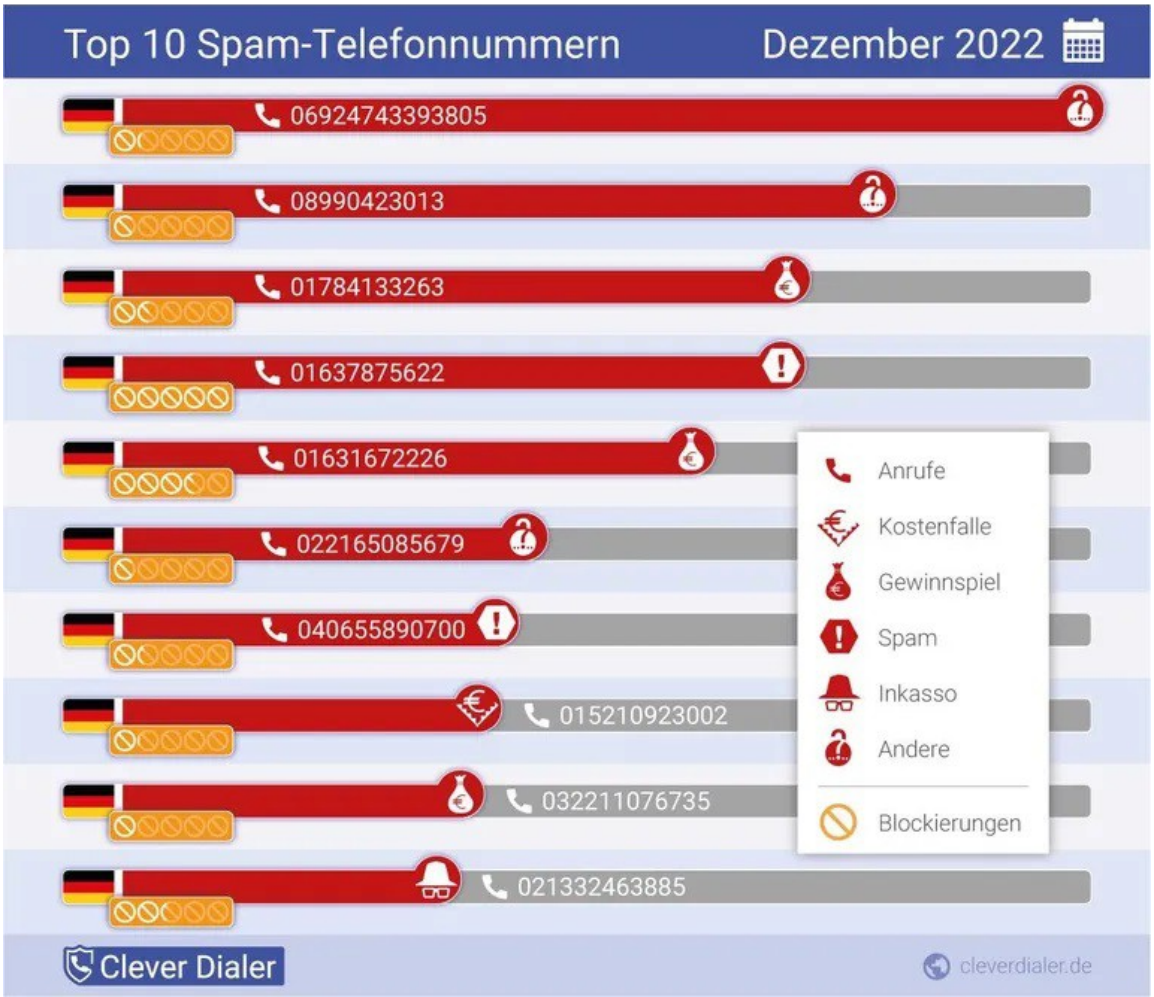
Bei Anruf Abzocke: Im Dezember kam es zu unzähligen Spam-Telefonanrufen. In unserer Liste finden Sie die häufigsten Nummern, die Sie blockieren sollten.

Spam-Anrufe sind heute leider fester Bestandteil eines Telefonanschlusses – egal ob Handy oder Festnetz. Dabei melden sich Personen oft im Namen von Firmen, um Nutzern neue Verträge zu verkaufen. Manchmal geht es auch um Gewinnspiele, in anderen Fällen sollen Nutzer in Kostenfallen gelockt werden.

Im Dezember hatten sich Betrüger die gestiegenen Heizkosten und die Kälteperiode der ersten beiden Wochen des Monats zunutze gemacht. Laut des Dienstleisters Cleverdialer gab es besonders viele Spam-Anrufer, um vermeintliche Stromverträge abzuschließen (022165085679), sich als Stadtwerke auszugeben (01637875622) oder Beratungen anzubieten (01631672226).

Clever Dialer bietet eine App zur Spam-Abwehr und hat seine Daten für den Dezember ausgewertet. In unserer Liste haben wir die zehn häufigsten Spam-Nummern für Sie zusammengefasst – diese sollten Sie ignorieren oder blockieren:

Top 10 der Spam-Nummern im Dezember 2022



Telefon-Spamliste aus dem Dezember. (Quelle: Clever Dialer)

Um sich zuverlässig vor Betrugsversuchen oder potenziellen Kostenfallen zu schützen, lauten die goldenen Regeln:

- Rufen Sie keine unbekannten Nummern zurück.
- Persönliche Daten sollten Sie am Telefon nicht bestätigen oder von sich aus nennen.
- Kommt Ihnen ein Anrufer oder eine Nummer suspekt vor, sollten Sie diese ignorieren oder blockieren.

Wie das funktioniert, erklären wir in unserer Schritt-für-Schritt-Anleitung. In vielen Fällen hilft es auch schon, einen Anruf schlicht abzubrechen und aufzulegen, wenn der Gesprächspartner mit dubiosen Anfragen an Sie herantritt.

Quelle: https://www.t-online.de/digital/handy/id_100111178/vorsicht-spam-anrufe-diese-telefonnummern-sollten-sie-blockieren.html

7) Anschwellendes Problem: Samsung-Handys zerstören sich weiter selbst

Vor einigen Monaten hat Samsung für unschöne Schlagzeilen gesorgt. Galaxy-Smartphones sind nach einiger Zeit angeschwollen und haben sich so selbst zerstört. Hat sich etwas geändert? Danach sieht es nicht aus, denn es hat wieder ein berühmtes Opfer getroffen. Daraufhin haben sich viele betroffene Samsung-Nutzer mit ähnlichem Problem gemeldet.

Samsung-Handys schwellen weiter an

Im Herbst 2022 hat ein bekannter YouTuber bemerkt, dass mehrere seiner Samsung-Smartphones angeschwollen sind. Samsung hatte Stellungnahme bezogen und Empfehlungen herausgegeben, wie man mit den Lithium-Ionen-Akkus umgehen soll. Jetzt hat es mit Even Blass wieder ein berühmtes Opfer getroffen. Sein Galaxy Z Fold 2 (Test) ist nämlich **angeschwollen und kann damit nicht mehr benutzt werden**.

Das ist im Übrigen **der zweite Akku**, der in dem Samsung Galaxy Z Fold 2 angeschwollen ist. Schon im Juli 2022 hatte er ein offenes Gehäuse seines Falt-Handys bemerkt und **den Akku damals austauschen** und das Handy reparieren lassen. Jetzt im Januar 2023 ist der neue Akku erneut angeschwollen. Nach nur sehr wenigen Monaten im Einsatz darf so etwas eigentlich nicht passieren. In den Kommentaren haben sich innerhalb weniger Stunden wieder viele Samsung-Besitzer mit ähnlichen Problemen gemeldet. Von anderen Herstellern kennt man solch empfindliche Akkus nicht.

Samsung hilft bei angeschwollenen Akkus

Damals hatte Samsung in seiner Stellungnahme gesagt, dass sich betroffene Besitzerinnen und Besitzer von angeschwollenen Akkus in Galaxy-Handys an den Hersteller wenden können. Doch wenn selbst die damals reparierten Handys jetzt schon wieder anschwellen, dann ist das Problem mit einem neuen Akku auch weiterhin nicht behoben. Besonders nicht, wenn das nur ein halbes Jahr später passiert. Irgendwas läuft da gehörig schief bei Samsung-Akkus.

Quelle: https://www.giga.de/news/anschwellendes-problem-samsung-handys-zerstoeren-sich-weiter-selbst/

8) Millionen Deutsche müssen handeln: Unbedingt Rauchmelder austauschen

Jeder Haushalt ist verpflichtet, Rauchmelder anzubringen. Doch viele wissen nicht, dass diese Lebensretter regelmäßig ausgetauscht werden müssen. Hier erfahren Sie, wann es so weit ist und welche Modelle geeignet sind.

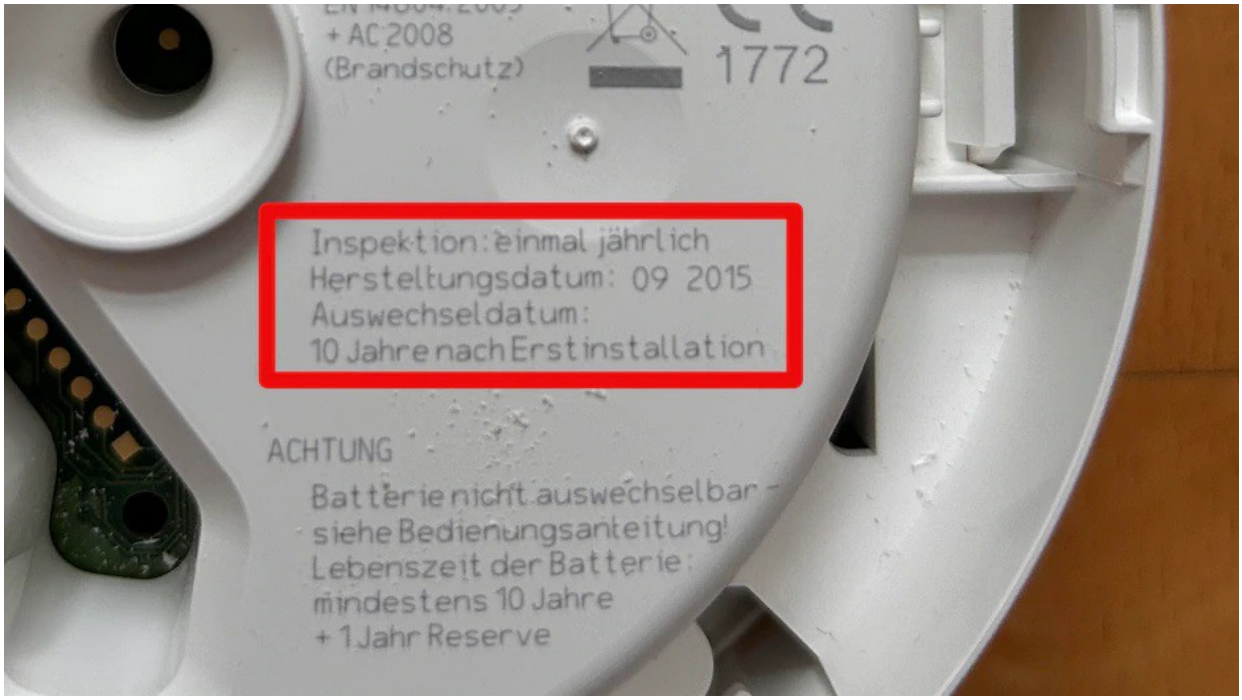
In Deutschland gilt eine **Rauchmelderpflicht für privat genutzten Wohnraum**. Doch eine bundesweit einheitliche Regelung gibt es dafür nicht, was bei Ihnen genau Sache ist, regelt Ihr Bundesland.
Und hier gibt es durchaus Unterschiede: Rheinland-Pfalz hat zum Beispiel schon 2003 mit einer Rauchmelderpflicht in Neubauten angefangen, in Sachsen gilt dagegen noch bis Ende

2023 eine Übergangsphase für Bestandsbauten.
Doch wenn die Rauchmelder erstmal hängen, hat man etwas Ruhe. Ewig dürfen Sie die Geräte aber nicht betreiben. Es gibt eine Austauschpflicht: **Nach 10 Jahren** müssen Rauchmelder ausgetauscht werden. Die entsprechende Norm spricht von einer Übergangszeit von sechs Monaten, 10 Jahren nach der Inbetriebnahme.

- Rauchmelder: Das sollten Sie regelmäßig tun
- Rauchmelder-Test: Empfehlenswerte Geräte

Nach 10 Jahren: Rauchmelder austauschen

Man kann mehrere Gründe für die Begrenzung des Betriebs auf 10 Jahren finden, der wichtigste dürfte aber sein, dass die Sicherheit danach nicht mehr gewährleistet ist. Die einwandfreie Funktion ist durch Staub und Schmutz nach 10 Jahren eingeschränkt, deshalb müssen Rauchmelder getauscht werden.
Dabei handelt es sich auch nicht um eine Herstellervorgabe oder einen guten Rat eines Handwerkers, sondern um eine **Austauschpflicht**. In der Regeln müssen sich Eigentümer um die Rauchmelder kümmern. Möglicherweise werden die Geräte ohnehin von Experten gewartet. Steht ein Austausch an, wird das dann gleich gemacht und Mieter müssen sich um nichts kümmern.
Orientiert man sich an den Einführungspflichten der Bundesländer, sollten Bewohner von Baden-Württemberg, Bayern, Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz demnächst ihre Rauchmelder tauschen. Zumindest eine kurze Prüfung der Frist ist eine gute Idee.



Quelle: Das Herstellungsdatum finden Sie auf der Innenseite des Rauchmelders. Bild: CHIP

Doch wie findet man heraus, wie lange der Rauchmelder schon in Betrieb ist? Wenn Sie sich das Datum der Inbetriebnahme nicht notiert haben oder ein smarter Rauchmelder das nicht in der App anzeigt, reicht es meist aus, das Gerät kurz abzuschrauben. Innen sollten Sie in der Regel das **Herstellungsdatum** finden. Haben Sie das geprüft, sollte der Rauchmelder wieder montiert werden.
Angefügt haben wir Ihnen eine Tabelle mit den **Fristen in Ihrem Bundesland**. Dort ist auch vermerkt, wann wahrscheinlich der nächste **Austausch des Rauchmeldern** für Sie ansteht.
Wichtig: Wir orientieren uns bei den Angaben an den gesetzlichen Fristen für die

Rauchmelderpflicht. Es kann aber sein, dass Sie Ihre Rauchmelder zu einem anderen Zeitpunkt in Betrieb genommen haben. Dann müssen Sie das Austauschdatum selbst ermitteln.

Rauchmelder-Fristen und Austauschpflicht

Bundesland	Pflicht Neubauten/Bestandsbauten	Nächster wichtiger Austauschtermin*
Baden-Württemberg	2013/2015	2023
Bayern	2013/2018	2023
Berlin	2017/2021	2027
Brandenburg	2016/2021	2026
Bremen	2010/2016	2026
Hamburg	2006/2011	2026
Hessen	2005/2015	2025
Mecklenburg-Vorpommern	2006/2010	2026
Niedersachsen	2012/2026	2022
Nordrhein-Westfalen	2013/2017	2023
Rheinland-Pfalz	2003/2012	2022
Saarland	2004/2017	2024
Sachsen	2016/2024	2024
Sachsen-Anhalt	2009/2016	2026
Schleswig-Holstein	2005/2011	2025
Thüringen	2008/2019	2028

Quelle: https://www.chip.de/news/Millionen-Deutsche-muessen-handeln-Unbedingt-Rauchmelder-austauschen_184580450.html?utm_source=nl_chipd-dy+&utm_medium=chip-newsletter&utm_campaign=09-01-2023%2B17%253A00%253A02&utm_content=nl_chipmob&utm_term=

9) Post vom Beitragsservice: Wenn Sie diesen Brief ignorieren, wird es teuer

Kürzlich erhielt die "GEZ" mal wieder Daten von den Einwohnermeldeämtern und gleicht diese mit dem Bestand an Beitragszahlern ab. Wer nicht zugeordnet werden kann, kriegt bald Post vom Beitragsservice.

Der Beitragsservice, besser bekannt unter dem ehemaligen Kürzel GEZ, startete bereits im November mit dem sogenannten Meldedatenabgleich 2022.
Die Verwaltungsgemeinschaft der Rundfunkanstalten von ARD, ZDF und Deutschlandradio erhält dabei ausgewählte Daten der Einwohnermeldeämter zu allen volljährigen Bürgerinnen und Bürgern.
Diese Daten werden zur Klärung der Rundfunkbeitragspflicht mit den vorhandenen Bestandsdaten (46,1 Millionen Beitragskonten) der GEZ abgeglichen. Personen, die keiner zum Rundfunkbeitrag angemeldeten Wohnung zugeordnet werden können, schreibt der Beitragsservice **seit dem 10. Januar 2023** sukzessive an. Dieses sogenannte Klärungsschreiben sollten Sie keinesfalls ignorieren.

- GEZ erreichen: Hotline und Kontaktdaten
- GEZ für eine Zweitwohnung: Das ist die Rechtslage
- GEZ Beitragsnummer herausfinden

Rückmeldung auch online möglich

Der Meldedatenabgleich ist gesetzlich geregelt (Rundfunkbeitragsstaatsvertrag § 11 Abs. 5) und findet nach 2013 und 2018 zum inzwischen dritten Mal statt.
Angeschriebene sollten laut dem Beitragsservice (früher GEZ) "zeitnah auf das Klärungsschreiben reagieren und dem Beitragsservice die nötigen Angaben zu ihrer Wohnung übermitteln". Das geht auch online. Im Schreiben wird die Frist konkreter, betroffene Personen sollen sich innerhalb von zwei Wochen zurückmelden.
Angeschriebene Personen scannen dafür einfach den QR-Code auf dem Klärungsscheiben. Alternativ kann auch das beigefügte Antwortformular ausgefüllt und an den Beitragsservice zurückgesendet werden.
Melden die angeschriebenen Personen zurück, dass für die Wohnung bereits ein Beitrag gezahlt wird und teilen die entsprechende Beitragsnummer mit, sollen ihre Daten unverzüglich gelöscht werden.

GEZ-Zwangsanmeldung droht

Sie sollten das Schreiben der GEZ nicht ignorieren. Reagieren angeschriebene Personen nicht auf den ersten Brief, gibt es nochmal ein Erinnerungsschreiben.
Wird auch das ignoriert, meldet der Beitragsservice die betroffene Person automatisch an. Die GEZ geht dann davon aus, dass für die betreffende Wohnung der Rundfunkbeitrag zu zahlen ist. Auch bei Rückmeldung, dass noch kein Beitrag gezahlt wird, wird eine Anmeldung vorgenommen.
Wird bisher keine GEZ-Gebühr bezahlt, wird diese sogar rückwirkend zum Einzugsdatum berechnet. Es drohen also unter Umständen auch saftige Nachzahlungen. Eine rückwirkende Anmeldung erfolgt aber frühestens zum 1. Januar 2020.
Beim Meldedatenabgleich werden folgende Angaben von den Einwohnermeldeämtern übermittelt:

- Familienname
- Vornamen unter Bezeichnung des Rufnamens

- frühere Namen
- Doktorgrad
- Familienstand
- Tag der Geburt
- gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung
- Tag des Einzugs in die Wohnung

Seit dem 10. Januar 2023 werden erste Klärungsschreiben versendet werden. Das klappt aber nicht alles auf einen Schlag. Bis **Ende Juni 2023** sollen aber alle Schreiben verschickt worden sein.
Quelle: https://www.chip.de/news/Post-vom-Beitragsservice-Wenn-Sie-diesen-Brief-ignorieren-wird-es-teuer_184491249.html?utm_source=nl_chipd-dy+&utm_medium=chip-newsletter&utm_campaign=09-01-2023%2B17%253A00%253A02&utm_content=nl_chipmob&utm_term=

10) eBay "verpfeift" euch ans Finanzamt: Neues Gesetz macht ab 2023 eure Online-Geschäfte transparent

Ein neues Gesetz verpflichtet Online-Plattformen wie eBay und Airbnb, auch Umsätze privater Anbieter dem Finanzamt zu melden. Ab welchem Gesamtbetrag das passiert, lest ihr hier.

- Private Verkäufe auf eBay oder Airbnb müssen die Plattformbetreiber künftig dem Finanzamt melden.

- Dabei werdet ihr ab einer jährlichen Menge von mehr als 30 Verkäufen oder einem Gesamterlös von 2.000 Euro bereits dem Fiskus gemeldet.
- Nachträgliche Steuern für Privatverkäufe fallen dabei nicht an - allerdings kommt es so schneller zum Verdacht, ihr könntet gewerblich verkaufen oder vermieten.

Mit dem Jahr 2023 tritt das sogenannte Plattformen-Transparenzgesetz in Kraft - und eure Verkäufe bei eBay oder Vermietung von Wohnraum bei Airbnb rückt somit in den fiskalischen Fokus. Sprich: Die Betreiber von Handels- und Vermietungs-Plattformen sind fortan gezwungen, die Umsätze ihrer User den zuständigen Finanzämtern zu melden.

Das neue Gesetz wird allerdings erst ab einer gewissen Schallmauer wirksam: Wickelt ihr so über eBay weniger als 30 Verkäufe im Jahr ab und nehmt dabei auch weniger als 2.000 Euro insgesamt ein, erfolgt keine Meldung ans Finanzamt. Liegt die Zahl der Transaktionen jedoch höher oder ihr verkauft auch nur eine teure Stereo-Anlage Privat über eBay Kleinanzeigen, ist eure Tätigkeit dort bereits meldepflichtig.

Steuern und Transparenz: Private Verkäufer haben wohl nichts zu befürchten

Müsst ihr euch nun Sorgen machen, plötzlich Steuerschulden anzuhäufen, weil ihr eure Plattensammlung auflöst und über eBay verkauft? Nein - denn auch wenn ihr Mindestbetrag und Transaktionsmengen überschreitet, passiert außer dem Informationsfluss seitens der Plattform an die Steuerbehörde wohl zunächst nichts.

Labelt ihr jedoch gut laufende Versandgeschäfte mit täglichem Warenausgang als Privatverkäufe, wird das Finanzamt nun deutlich schneller Wind davon bekommen - genau wie, wenn ihr eine leer stehende Wohnung in eurem Haus laufend und damit quasi gewerblich über Airbnb vermietet, ohne ein Gewerbe dafür angemeldet zu haben und folgerichtig die entsprechende Steuererklärung einzureichen.

Quelle: https://www.netzwelt.de/news/212251-ebay-verpfeift-euch-ans-finanzamt-neues-gesetz-macht-ab-2023-online-geschaefte-transparent.html

11) Das gibt es nicht bei YouTube oder Netflix: Mehr als 54.500 VHS-Kassetten gratis zum Download

Hier finden Sie Filmklassiker, die es sonst so nirgends gibt: In der Schatztruhe des Internets, dem "Internet-Archiv", können Sie mehr als 54.500 digitale Aufnahmen von VHS-Kassetten kostenlos herunterladen.

Alles auf einen Blick:

- Die Sammlung beinhaltet über 54.500 VHS-Kassetten, hauptsächlich aus den 80er und 90er Jahren. Alle Titel wurden digital aufgezeichnet, bearbeitet und sind jetzt auf "archive.org" gratis für Sie abrufbar
- Das Archiv beherbergt Blockbuster wie König der Löwen oder Toy Story, aber auch Aufzeichnungen von Fernsehausstrahlungen, Serien, Trailer oder Shows, die Sie heutzutage nirgendwo kaufen können. Ein witziges Juwel: Der Windows 95 Video Guide mit den Friends-Darstellern Jennifer Aniston und Matthew Perry
- Die verschiedenen Videos stehen in diversen Qualitätsstufen und unterschiedlichen Formaten zum kostenlosen Download bereit
- Die Inhalte sind nahezu alle auf Englisch

Lange vor Streamingdiensten wie Netflix, Amazon Prime oder Disney+ gab es die DVDs und davor wiederum VHS-Kassetten. Die konnte man mit und ohne Inhalt kaufen. Mit einem Videorekorder ließ sich das Fernsehen auf Kassette aufnehmen und im schlimmsten Fall wurde dann ausgerechnet die Kassette mit dem Hochzeitsvideo aus Versehen überspielt. Das Internet-Archiv hat jetzt zahlreiche solcher aufgezeichneten oder damals käuflich erhältlichen Raritäten digital aufbereitet und zum Download bereitgestellt. Darunter Filme, Clips und Serien, die viele noch aus ihrer Kindheit kennen. Mankos: Die Inhalte sind fast ausschließlich auf Englisch verfügbar, die Videoqualität ist allein schon aufgrund der analogen Quelle recht bescheiden.

Riesiges Video-Archiv: So laden Sie seltene Aufnahmen herunter

Wenn Sie unserem Download-Button folgen, finden Sie sich direkt auf der passenden Website von "archive.org" wieder. Im Suchfeld können Sie nach verschiedenen Begriffen suchen - beispielsweise dem Titel oder dem Fernsehsender. Geben Sie hier etwa "Spongebob" ein, erhalten Sie 154 Treffer.
Möchten Sie sich jetzt beispielsweise die originale Pilotfolge von 1997 ansehen, wählen Sie einfach per Mausklick die gewünschte Aufnahme aus. Im folgenden Fenster sehen Sie jetzt einen Videoplayer. Klicken Sie jetzt auf das "Play"-Symbol, starten Sie die Wiedergabe des Clips. Unterhalb des Players finden Sie eine Beschreibung und zusätzliche Informationen. Möchten Sie sich Aufnahmen herunterladen, finden Sie auf der jeweiligen Seite der Aufnahme eine Infobox mit dem Titel "Download Options" und blau unterlegten Links. Klicken Sie hier auf "MPEG4" gelangen Sie direkt zur Videodatei im MP4-Format und können diese mit einem Rechtsklick speichern.
Quelle: https://www.chip.de/news/Das-gibt-es-nicht-bei-YouTube-oder-Netflix-Mehr-als-54.500-VHS-Kassetten-gratis-zum-Download_182532452.html?utm_source=nl_chipd-wy&utm_medium=chip-newsletter&utm_campaign=29-01-2023%2B07%253A00%253A36&utm_content=nl_chipmob&utm_term=

12) FritzBox: AVM stellt Support für 2 Modelle ein

Es gibt viele verschiedene Modelle der FritzBox auf dem Markt. Doch nun stellt Hersteller AVM den Support für gleich zwei von ihnen ein.

In punkto Internetrouter hat sich AVM schon vor geraumer Zeit zu einem der Top-Anbieter gemausert. Die eigens hergestellten **FritzBox**-Geräte versorgen seit Jahren zuverlässig Millionen Haushalte mit schnellem Internet. Wer allerdings über einige ältere Geräte verfügt, sollte jetzt über ein Upgrade nachdenken. Das Unternehmen stellt nämlich den Support ein.

2 FritzBox- und 2 FritzRepeater-Geräte ohne Support

Beim Online-Magazin Deskmodder ist aufgefallen, dass der Hersteller offenbar bei jeweils zwei weiteren FritzBox- und FritzRepeater-Geräten die Unterstützung einstellt. Bei den Routern handelt es sich um die Modelle 3490 und 4020, während bei den Repeatern die Produkte mit den Nummern 310 und 1750E betroffen sind. Eine offizielle Bestätigung von Seiten AVM liegt derzeit noch nicht vor.

Für gewöhnlich verläuft dieser Prozess in zwei Teilen: Zuerst wird die Bereitstellung neuer Updates und Patches eingestellt, was man „End of Maintenance“ nennt. Später kommt der „End of Support“ hinzu, bei dem es um persönliche Unterstützung per E-Mail oder Telefon geht.

Keine Überraschung für Unterstützungsende

Wer also eines oder gar mehrere der genannten Geräte besitzt, wird also keine Neuerungen und Verbesserungen mehr erwarten können. Immerhin soll man aber dem Bericht zufolge zumindest mit weiteren Sicherheitsupdates rechnen können, sofern es notwendig wird.

Das Support-Aus für die FritzBox- und FritzRepeater-Modelle sollte indes nicht überraschen. Schließlich sind sie allesamt älter als fünf Jahre. Für jüngere Geräte hat AVM wiederum vor Kurzem endlich das FritzOS 7.50 ausgerollt. Wir sagen dir, was es auszeichnet.

Quelle: https://www.futurezone.de/produkte/article421483/fritzbox-2-modelle-supportende.html