37. Cybercrime Newsletter

30.08.2023

1) Kleinanzeigen – Betrug über Kleinanzeigen: Auch Verkäufer bleiben nicht unbehelligt

Gerade erst ging die Anzeige online, schon reagiert jemand darauf. Was für ein Glück! Doch auf Kleinanzeigen ist vor allem für Verkäufer derzeit Vorsicht geboten: Betrüger heucheln Interesse, fragen Sie dann nach sensiblen Daten und locken Sie auf fremde Seiten. Das sollten Sie über die derzeit gängigste Betrugsmasche auf der Plattform wissen.

Ob am Telefon, durch eine E-Mail oder SMS: Die Maschen von Betrügerinnen und Betrügern sind vielfältig. Gemeinsam haben sie alle, dass sie auf Ihr Geld oder sensible, persönliche Daten aus sind. Auch auf Online-Portalen wie Kleinanzeigen sind Nutzerinnen und Nutzer nicht vor ihnen sicher. Dabei stehen nicht nur die Käuferinnen und Käufer im Fokus, sondern auch die Verkäufer.

Die derzeit gängigste Betrugsmasche auf der Plattform dreht sich um die Kleinanzeigen-Option "Sicher bezahlen". Die Betrüger schreiben Ihnen teilweise nur wenige Sekunden nach Anzeigenerstellung, geben zunächst Interesse an Ihrem Produkt vor und wollen es dann über das Portal bezahlen. Sie erhalten daraufhin eine Nachricht wie beispielsweise:

Unmittelbar nachdem ich auf die Zahlungsseite gegangen bin,
werde ich aufgefordert, die E-Mail des Verkäufers anzugeben.
Bitte notieren Sie Ihre E-Mail für mich.
Quelle: private Nachricht über Kleinanzeigen

Auch nach Ihrer Telefonnummer können die Betrüger fragen. Es kann sogar sein, dass der Gesprächspartner ein Foto einer gefälschten Kleinanzeigen-Seite als "Beweis" mitschickt. Geben Sie die gewünschten Informationen weiter, erhalten Sie eine E-Mail, SMS oder WhatsApp-Nachricht mit einem Link. Dort sollen Sie dann Ihre Zahlungs- oder Kreditkartendaten hinterlegen.

Die Nachrichten und Webseiten sind dem Kleinanzeigen-Design nachempfunden, enthalten teilweise sogar Details der ursprünglichen Anzeige, wie Titel oder Bilder. Geben Sie dort Ihre Daten ein, sind Sie schnell Tausende Euros los.

Kleinanzeigen warnt davor, sensible Daten preiszugeben

Fiona Kleinert, Communications Managerin bei Kleinanzeigen, stellt in diesem Zusammenhang klar: "Die Abwicklung von Transaktionen mit 'Sicher bezahlen' funktioniert vollständig über unsere App beziehungsweise Website." Die Plattform verschicke im Zusammenhang mit der Funktion keine SMS oder Messenger-Nachrichten und warne davor, E-Mail-Adresse oder Telefonnummer preiszugeben.

"Wenn Käufer oder Verkäufer nach diesen Informationen fragen,
weil sie diese angeblich für die Abwicklung

der Zahlung über unsere Plattform benötigen,
handelt es sich ausnahmslos um Betrug."
Quelle: Fiona Kleinert von Kleinanzeigen

"Wir raten Nutzerinnen und Nutzern generell, sensibel mit ihren Daten umzugehen", so Kleinert weiter. Das passiere auch innerhalb der Plattform im Nachrichtensystem. "Wenn jemand kurz davor ist, eine E-Mail-Adresse oder Telefonnummer zu teilen, erscheint ein Hinweisfenster vor dem Absenden der Nachricht." Dieses warne vor der Weitergabe sensibler Daten.

Nicht auf Links klicken oder Dateianhänge öffnen

Generell gilt: Zugangsdaten und persönliche Daten, wie das Geburtsdatum, persönliche Fotos oder Videos sowie Kopien von persönlichen Dokumenten, beispielsweise einem Personalausweis, sollten unter keinen Umständen weitergegeben werden.

Haben Sie eine E-Mail oder SMS von einem Absender erhalten, den Sie nicht kennen, ist Vorsicht geboten. Werden Sie sich zunächst darüber im Klaren: Wer ist der Absender? Was steht im Betreff, wie ist die Schreibweise? Kann das Geschriebene der Wahrheit entsprechen? Lassen Sie sich in keinem Fall unter Druck setzen und reagieren Sie am besten gar nicht darauf.

Lesen Sie auch: Um Betrüger zu entlarven, rät die Polizei zur SHS-Regel

Links, die von Kleinanzeigen wegführen, wo nach Daten gefragt wird oder sogar Downloads erforderlich sind, sollten niemals angeklickt werden. Falls Sie auf einer solchen Seite gelandet sind: auf keinen Fall einen Download ausführen. Auch Dateianhänge sollten in keinem Fall geöffnet werden.

Da die Seiten, auf die die Betrüger Sie führen möchten, täuschend echt aussehen können, rät Kleinanzeigen, den Link zunächst per Rechtsklick zu kopieren und zum Beispiel in ein Textverarbeitungsprogramm zu kopieren. So können Sie sich die URL genauer ansehen. Häufig lautet diese ganz anders als das Original. Auch wenn Sie mit der Maus über einen Link hovern, sehen Sie in der Regel, wohin dieser wirklich führt.

Betrüger benutzen nicht nur neu erstellte Konten

Wenn Sie nur wenige Sekunden nach Anzeigenerstellung eine Nachricht eines Interessenten bekommen, kann das durchaus ein Hinweis auf einen Betrugsversuch sein, wie Kleinert erklärt. Mithilfe ihres Nutzerprofils lassen sich Betrüger allerdings selten entlarven.

Sie nutzen häufig sogenannte "Account-Takeover", "also Fremdzugriffe auf bereits bestehende Konten". Es kann dementsprechend sein, dass Betrüger mit Konten agieren, die wegen ihrer langjährigen Mitgliedschaft oder Bewertungen verlässlich wirken.

Wenn Sie davon ausgehen, dass ein Betrüger mit Ihnen schreibt, ist es ratsam, denjenigen gleich an Kleinanzeigen zu melden. Das Konto wird dann zeitnah gesperrt. "Außerdem werden andere Personen, die im Kontakt mit dem mutmaßlichen Betrüger standen, gewarnt," erklärt Kleinert.

Sichern Sie Beweise und erstatten Sie Strafanzeige bei der Polizei

Und was ist zu tun, wenn man auf die Betrugsmasche hereingefallen ist und Kontodaten preisgegeben hat? Wenden Sie sich zunächst an Ihre Bank. Konten lassen sich vorübergehend sperren, sodass die Betrüger nicht mehr darauf zugreifen können. Außerdem werden Zahlungen häufig nicht sofort gebucht, sodass diese noch vor Ausführung gestoppt werden können. Wurde ein anderer Zahlungsdienstleiter wie PayPal verwendet, sollten Sie

auch diesen umgehend kontaktieren.

Außerdem rät Kleinert, alle Beweise, wie Gesprächsverläufe oder Kaufverträge, zu sichern, und anschließend bei der Polizei Strafanzeige zu erstatten. Dank der Onlinewachen geht das bequem von zu Hause aus.

Lesen Sie auch: Häufige Betrugsmaschen: Wie Kriminelle mit dem Moment des Entsetzens spielen

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/betrug-kleinanzeigen-verkaeufer-unbehelligt-38548252

2) Schamgefühl als Druckmittel – Verbraucherschützer warnen vor Abzocke bei Sexportalen

Das Druckmittel ist Scham, die Rechnungen sind hoch. Verbraucherschützer warnen vor gefälschten Rechnungen von Sexportalen.

Eine neue fiese Betrugsmasche setzt darauf, dass Männer aus Scham keine Gegenwehr leisten und hohe Rechnungen begleichen. Wie die Verbraucherzentrale Berlin berichtet, erhalten immer mehr Männer Rechnungen per Post für angebliche Mitgliedschaften bei Dating-Portalen, über die Sex-Treffen zustande kommen sollen. Einige Portale drucken demnach sogar ungefragt Fotos der Betroffenen auf die Rechnung.

Die Masche hinter der Sexportal-Rechnung

In Kombination mit der sexuellen Anspielung im Namen der Website, der prominent auf dem Briefkopf abgedruckt ist, sollen sich die Verbraucher bloßgestellt fühlen.
"Die Betroffenen sehen sich mit Rechnungen von bis zu 500 Euro konfrontiert und zahlen, weil sie aus falscher Scham die Beratung scheuen", berichten die Verbraucherschützer.Simon Götze, Rechtsexperte der Verbraucherzentrale Berlin, erklärt: "Die Unternehmen gelangen durch verschiedene Methoden an persönliche Daten der Verbraucher. Anschließend hoffen sie darauf, dass die Betroffenen zu viel Scham haben, um Gegenwehr zu leisten."

Die Verbraucherzentrale rät

1. Keine falsche Scham bei der Abwehr von Betrug
2. Beim Surfen und in sozialen Netzwerken sollten Verbraucher stets Vorsicht walten lassen
3. Bei überraschenden Kontaktaufnahmen durch vermeintliche Singles ist Misstrauen geboten
4. Widerrufsrecht geltend machen
5. Rechtliche Beratung in Anspruch nehmen

Götze appelliert an Betroffene: "Scham hilft hier nicht: Die Betroffenen müssen sich beraten lassen, sonst verlieren sie unnötigerweise viel Geld an Betrüger." Wer sicher ist, keine Mitgliedschaft bei so einem Portal abgeschlossen zu haben, sollte sich rechtlich beraten lassen und unbedingt Widerruf einlegen.

Quelle: https://www.t-online.de/digital/aktuelles/id_100231768/abzocke-in-sex-portalen-verbraucherschuetzer-warnen-vor-falschen-rechnungen.html

3) Phishing-Versuch – Betrüger haben es auf Kunden der Deutschen Bank abgesehen

TAN-Aktivierungsbrief ungültig: Mit diesem Hinweis wollen Kriminelle an die Daten von Deutsche-Bank-Kunden gelangen. Verbraucherschützer warnen.

Kriminelle verschicken vermehrt Betrugs-Mails an Kunden der Deutschen Bank. Das teilen die Verbraucherzentralen auf ihrer Seite mit. Demnach versendeten die Betrüger ihre Phishing-Mails mit dem Betreff "Ihr photoTAN-Aktivierungsbrief ist ungültig!".

Im Gegensatz zu anderen Phishing-Versuchen stimme der Betreff der Mail mit dem Inhalt überein, heißt es weiter. Die Gefahr: Die Nachricht lasse sich dadurch kaum von echten Mitteilungen unterscheiden. Zumal auch die restliche Mail einen seriösen Eindruck hinterlasse.

Die Kriminellen wiesen in ihrer Nachricht darauf hin, dass ein "photoTAN-Aktivierungsbrief" angeblich nur 120 Tage gültig sei und nun erneuert werden müsse. Als Beweis werde eine europäische Richtlinie erwähnt, die ein gültiges TAN-Verfahren als notwendig beschreibe.

Betrüger wollen private Daten erbeuten

"Darauf folgt der Hinweis, dass ein Aktivierungscode für eine Aktivierung des photoTAN-Verfahrens notwendig sei", schreiben die Verbraucherschützer. Der Code könne angeblich nur über einen beigefügten Link erneuert werden.

Wie bei Phishing-Versuchen üblich, führe der Link auf die Seiten der Betrüger. Dort wollen diese die privaten Daten der Mail-Empfänger erbeuten.

Der Hinweis der Verbraucherschützer: "Lassen Sie sich von der vermeintlichen Seriosität nicht täuschen, denn besonders die Absendeadresse und die unpersönliche Anrede deutet definitiv auf einen Phishing-Versuch hin." Die Mail sollte unbeantwortet in den Spam-Ordner verschoben werden.

Was ist Phishing?

Beim sogenannten Phishing versuchen Kriminelle, an persönliche Daten ihrer Opfer zu kommen. Dazu gehören der Name, die E-Mail-Adresse, Passwörter oder das Geburtsdatum.

Diese Daten können die Kriminellen verkaufen oder selbst nutzen, um sich in Online-Accounts wie das Bankkonto einzuloggen und dieses zu plündern.

Für Phishing-Versuche nutzen Kriminelle gern gefälschte E-Mails, Websites oder Chat-Nachrichten. Dabei erhalten Nutzer eine Mail, die aussieht, als würde sie von einem großen Unternehmen stammen.

In einem anderen Artikel erklären wir, was Phishing genau ist, was hinter der erweiterten Methode Spear-Phishing steckt und wie Sie solche Betrugs-Mails erkennen können.

Quelle: https://www.t-online.de/digital/aktuelles/id_100232372/phishing-versuch-bei-deutschen-bank-betrueger-haben-es-auf-kunden-abgesehen.html

4) Betrug im Internet: Kemptenerin (35) fällt auf betrügerisches Jobangebot herein - mehr als 32.000 Euro verloren

Auf ein falsches Jobinserat ist im Juni eine Frau aus Kempten hereingefallen. Statt für eine große US-Handelskette zu arbeiten verlor sie über 32.000 Euro.

Frau aus Kempten will angeblichen Job bei großer US-Handelskette antreten

Die 35-jährige Frau aus Kempten entdeckte laut Polizei auf einer Jobbörse im Internet ein angebliches Jobangebot einer großen US-Handelskette. Für den Job sollte die Frau bei einem vermeintlichen Online-Portal des Händlers einen Account anlegen. Ihre angebliche

Aufgabe: Sie sollte Verbindungen von eingehenden Bestellungen herstellen. Um die Finanzierungslücke zu schließen, die dadurch vermeintlich entstand, sollte die 35-Jährige selbst Geld auf dieses Portal einzahlen.

Doch das klappte nicht. Als die 35-Jährige kein Geld auf dieses Portal einzahlen konnte, täuschten die Täter vor, dass sie Geld auf dem Account der Frau gutschreiben würden, den die 35-Jährige angeblich bei dem US-Händler eröffnet hatte. Um den Job vollständig übernehmen zu können, sollte sie das geliehene Geld aber wieder zurückzahlen.

Frau zahlt 32.700 Euro auf Handelsplattform für Kryptowährung ein

Die unbekannten Täter forderten die Frau anschließend auf, eine App herunterzuladen. Die Frau dachte, dass die App zu einer Bank gehöre, wohin sie Geld überweisen könne. Doch tatsächlich handelte es sich um eine Plattform, über die man mit verschiedenen Kryptowährungen handeln kann. Im Zuge von vier Wochen zahlte die Frau dort insgesamt 32.700 Euro ein.

Kriminalpolizei rät zu erhöhter Vorsicht bei Jobangeboten im Internet

Die Kriminalpolizei rät dazu, Jobangebote auf den verschiedenen Plattformen im Internet genau zu prüfen. Denn dort werden immer häufiger unseriöse oder betrügerische Nebenjobs angeboten. Wer Zweifel hat, ob es sich um ein echtes Jobangebot handelt, sollte Kontakt zur zuständigen Kriminalpolizei aufnehmen und das Ganze überprüfen handeln. Grundsätzlich gilt aber: Wenn eine Stellenanzeige zu gut klingt, um wahr zu sein, stecken häufig Betrüger dahinter.

Quelle: https://www.all-in.de/polizei/betrug-frau-35-in-kempten-faellt-auf-falsches-jobangebot-herein-fast-33-000-euro-verloren_arid-304636

5) Sparkasse verlangt Geräteerkennung? Unbedingt ablehnen!

Die Sparkasse entwickelt ihre Services stetig weiter. Mit Blick auf die Cyberkriminalität soll nun die sogenannte Geräteerkennung mehr Sicherheit bieten. Wer eine entsprechende Benachrichtigung erhält, sollte jedoch sehr vorsichtig sein. Andernfalls könnte der Geldbeutel darunter leiden.

Die Verbraucherzentrale 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.

Aktuelle Phishing-Lage: Sparkasse, ING, Amazon & Disney+

Sparkasse

In den vergangenen Monaten führte die Sparkasse eine Geräteerkennung ein. Diese stellt eine Art Zwei-Faktor-Authentifizierung dar und soll zusätzlichen Schutz gegen digitale Angriffe bieten. Für Bankkunden bedeutet dies zunächst, dass sie künftig bei einer Anmeldung von einem unbekannten Gerät zur Freigabe per chipTAN respektive pushTAN aufgefordert werden – zusätzlich zur Eingabe des Anmeldenamens und der Online-Banking-PIN. Genau diesen Umstand machen sich Cyberkriminelle nun jedoch zunutze, um sich Zugang zum Bankkonto zu verschaffen.

Gegenwärtig sind optisch überzeugende Phishing-Mails im Umlauf. Diese werden im Namen der Sparkasse verschickt und greifen die zuvor aufgeführte Thematik auf. Der große Unterschied besteht darin, dass die Betrüger einen eigenen Link bereitstellen, über den sich Empfänger anmelden sollen. Die Verlinkung führt jedoch nicht zur Website der Sparkasse, sondern zu einer Fälschung. Sämtliche hier eingetragenen Anmeldeinformationen und TANs landen bei den Cyberkriminellen. Daher empfiehlt es sich, entsprechende E-Mails umgehend in den Spam-Ordner zu verfrachten. Auch dann, wenn eine direkte Kundenanrede vorhanden ist – was aktuell der Fall zu sein scheint. Merke: Die Sparkasse stellt keinen gesonderten Link für die Freigabe von Geräten bereit. Die Abfrage der TANs erfolgt bei unbekannten Geräten automatisch im Rahmen der Anmeldung über die üblichen Kanäle.

ING

Auch Kunden der ING stehen derzeit im Fokus von Cyberkriminellen. In einer entsprechenden E-Mail ist von ungewöhnlichen Kontoaktivitäten die Rede. Kunden werden aufgefordert, sich über eine hinterlegte Verlinkung einzuloggen, um die fraglichen Transaktionen zu überprüfen. Im Gegensatz zur vorangegangenen Phishing-Mail wirkt diese jedoch nur bedingt überzeugend. Einerseits fehlt die direkte Kundenanrede und andererseits finden sich mehrere Zeichensetzungs- und Formatierungsfehler. Zudem prangert auf dem beigefügten Logo nach wie vor der Schriftzug „ING DiBa“ – obwohl die Direktbank bereits seit geraumer Zeit den Markennamen „ING“ verwendet. Wer sich dennoch unsicher ist, kann die Echtheit der E-Mail jederzeit vom ING-Kundendienst verifizieren lassen.

Amazon

Abseits von Banken werden gegenwärtig auch Amazon-Mails von Cyberkriminellen verbreitet. Inhaltlich thematisieren diese eine Kontosperrung aufgrund ungewöhnlicher Anmeldeaktivitäten. Als Folge seien „aus Sicherheitsgründen“ sämtliche Dienste des Kontos deaktiviert, bis einer Rückmeldung erfolgt. Die geforderte Verifizierung soll derweil abermals über einen hinterlegten Link-Button ablaufen. Daher sollten auch Betroffene wiederholt zur selben Lösung greifen wie schon zuvor: dem Spam-Ordner.

Disney+

Abschließend müssen sich derzeit Nutzer des Streamingdiensts Disney+ vor Cyberkriminellen hüten. Diese verschicken wenig überzeugende Phishing-Mails, in denen sich Inhalt und Betreff gegenseitig widersprechen. Während als Betreff „Abrechnungsprobleme“ angegeben werden, thematisiert der Inhalt eine regelmäßige Überprüfung von Kontoinformationen. Um Disney+ weiterhin nutzen zu können, sollen die Empfänger ihre Kontoinformationen über einen eingebetteten Link aktualisieren. In solchen Fällen empfiehlt es sich, sich auf dem üblichen Weg im eigenen Nutzerkonto anzumelden. Funktioniert dieses wie gehabt, handelt es sich bei der E-Mail zweifelsohne um Phishing.

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:

- Advanzia Bank
- Amazon
- Apple
- Barclays
- Bitcoin-Erpressung

- Bundesfinanzministerium (BMF)
- Bundesministerium für Gesundheit (BMG)
- Commerzbank
- Comdirect
- Consorsbank
- Consors Finanz
- Deutsche Bahn (DB)
- Deutsche Bank
- DHL
- Disney+
- DKB
- GMX
- iCoud
- ING
- KfW
- LBB
- N26
- Netflix
- OLB Bank
- PayPal
- Postbank
- Santander
- Sparda-Bank
- Sparkasse
- Targobank
- Telekom
- UPS
- Vodafone
- VR
- web.de

Was ist Phishing eigentlich?

Wenn man an Cyberkriminelle denkt, kommen einem sofort 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 es 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 machst du es besser

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-kw34-sparkasse-geraeteerkennung

6) Neue Masche mit Mahnungen: Betrüger verschicken falsche Anwalts-Mails

Immer wieder tauchen Beschwerden über E-Mails von angeblichen Rechtsanwälten auf. Diese fordern zur Zahlung von mehreren hundert Euro auf.

Kassel – Betrüger versuchen es auf viele verschiedene Weisen, an sensible Daten oder das Geld von Verbrauchern zu gelangen. Es gibt einige Anhaltspunkte, die Sie auf eine betrügerische E-Mail hinweisen.

Beschwerden über E-Mails von angeblichen Rechtsanwälten nehmen zu

Wie die Verbraucherzentrale meldete, gingen zuletzt besonders viele Beschwerden über verdächtige E-Mails ein. Kontakt suchte per E-Mail die angebliche Anwaltskanzlei von Dr. Matthias Losert. Darin heißt es, dass Empfänger eine Urheberrechtsverletzung begangen hätten. Hintergrund sei das illegale Herunterladen eines Films aus dem Internet. Der „Anwalt“ fordert daraufhin einen Betrag von bis zu 500 Euro, da keine Unterlassungserklärung abgegeben oder sich anderweitig zur Thematik geäußert wurde. Auch mit Disney+ versuchen Betrüger, an Bankdaten von Nutzern zu kommen.

In der E-Mail wird angegeben, dass die Empfänger mithilfe des Internetanschlusses, der auf ihren Namen registriert ist, ausfindig gemacht wurden. Es handle sich um eine schwere Urheberrechtsverletzung, die Kosten für die Ermittlung und die außergerichtliche Verfolgung müssten bezahlt werden. Im Anschluss werden Empfänger dazu aufgefordert, sich über einen Link zu verifizieren, erst dann werden die Zahlungsinformationen weitergeleitet. Betont wird die außerordentliche Dringlichkeit, die in der Sache besteht.

Falsche Anwalts-Mails: So erkennen Sie Phishing-Versuche

Die Verbraucherzentrale betont, dass in solchen E-Mails niemals auf Links geklickt werden sollte. Diese führen meist auf eine Phishing-Seite, die häufig Schadsoftware enthält. Um solche Phishing-Mails zu erkennen, gibt die Verbraucherzentrale einige Tipps. Misstrauisch

werden sollten Verbraucher, wenn sie die vorgeworfene Urheberrechtsverletzung nicht begangen haben. Im eigenen Haushalt sollte dann geklärt werden, ob diese ein anderer begangen haben könnte. Auch bei einer falschen Bestellbestätigung von Amazon sollten Verbraucher aufpassen.

Wird in der E-Mail Druck ausgeübt, dass eine Zahlung umgehend erfolgen muss, sollten Empfänger ebenfalls hellhörig werden. Dringende Zahlungsaufforderungen, die nur in Großbuchstaben geschrieben wurden, sind ebenfalls unseriös. Offizielle Abmahnungen werden in aller Regel noch immer per Post und nicht per E-Mail verschickt. Nur, weil der Absender die Empfänger mit Namen anschreibt, bedeutet das nicht, dass es sich um eine seriöse Mail handelt. Das letzte Indiz für eine Fake-Seite liegt am Aufbau der URL, auf die die Empfänger klicken sollen. Diese endet meist nicht auf „.de“, sondern „.com“ oder „.eu“.

Quelle: https://www.hna.de/verbraucher/verbraucherzentrale-betrueger-phishing-emails-masche-mahnungen-anwalt-tipps-92480319.html?utm_source=newsshowcase&utm_medium=gnews&utm_campaign=CDAQ04HZ4ej8opTDARig7YTcoYjsqoIBKhAIACoHCAow-6WICzCZ6YYD&utm_content=bullets&gaa_at=la&gaa_n=AfHvTEvGujrf_Hj0AQbXU3ZqvKgHH6ngPvuWf4Dne9IcJDRUKFQuSpZfyF1IPCc4IFDpLgFrWCi8oF3fc2PXJnjce90P&gaa_ts=64e8656e&gaa_sig=y_9I3D0usZJ5IiwTSEauG0pYep3muRuuJfkbl15dnu5rZEvBUNzTjwQJ-aaKr0H607lWrZDpkkbbA7xGR1ZD0w%3D%3D

7) Amazon: Polizei warnt vor neuer Betrugsmasche – so schützen Sie sich

Betrüger haben es auf Amazon-Kunden abgesehen. Die Polizei erklärt, wie die Cybergangster vorgehen und welche Gefahren dadurch entstehen und wie Sie sich schützen.

Derzeit klingelt bei vielen Menschen das Telefon und wenn man abnimmt, hört man diese Sprachansage: “Hier ist Amazon. In den nächsten 24 Stunden werden von Ihrem Konto 850 € gebucht. Für weitere Informationen drücken Sie die Taste 1”. Drückt man nun tatsächlich auf die “1”, dann wird man offensichtlich zu einem Betrüger durchgestellt. Vor dieser Betrugsmasche warnt jetzt das Landeskriminalamt Niedersachsen.

Wie kommen die Betrüger an die Telefonnummern?

Jetzt stellt sich als Erstes die Frage, woher die Anrufer die Telefonnummer der angerufenen Person haben. Das LKA Niedersachsen geht davon aus, dass die angerufenen Telefonnummern rein zufällig gewählt/generiert werden. Es sei aber auch denkbar, dass eine zufällige vorherige Kontaktaufnahme per SMS mit beigefügtem Link zwecks Kontaktaufnahme erfolgte. Zudem könne es sein, dass die Täter auch auf Datenbanken zurückgreifen, die durch frühere Phishing-Vorfälle erstellt wurden und in denen die Telefonnummern enthalten sind.

So gehen die Täter vor

Zunächst wählen Wählcomputer mehrere Rufnummern gleichzeitig an. Nimmt eine angerufene Person diesen Anruf an, spielt der Computer automatisch eine Sprachansage ab. Drückt das Opfer dann wie aufgefordert die Taste 1, dann stellt das System den Angerufenen zu einem angeblichen Mitarbeiter im Callcenter durch. Mit dieser effizienten Vorgehensweise verhindern die Betrüger Zeitverlust durch langes Klingeln, Anrufbeantworter oder Mailboxen oder durch auch Personen, die den Betrug erkennen und auflegen.

Das ist das Ziel des Betrugs

Der eigentliche Schaden entsteht erst in dem Gespräch mit dem Betrüger. Dieser kann zum Beispiel versuchen, das Opfer dazu zu überreden, eine angebliche Fernwartungssoftware/App zu installieren. Darüber bekommen die Betrüger dann Zugriff auf den Rechner des Opfers. Oder aber der Betrüger überredet das Opfer dazu, seine

Zugangsdaten auf einer gefakten Webseite einzugeben. Ebenfalls denkbar: Das Opfer soll Personalausweis-Bilder hochladen oder sich per Personalausweis und Gesicht via Foto oder Webcam identifizieren. Diese Aufnahmen und Daten können Betrüger dann für Identitätsdiebstahl missbrauchen.

Eine andere Betrugsmasche: Die Opfer sollen Guthabenkarten (z.B. Paysafe) an Kiosken, Tankstellen oder Drogerien kaufen und deren Codes in die Kamera halten. Ebenso ist denkbar, dass die Betrüger Zugriff auf das Onlinebanking oder die Kreditkartendaten erlangen wollen.

So erkennen Sie den Betrug

Amazon ruft grundsätzlich seine Kunden nicht an. Stattdessen kontaktiert Amazon seine Kunden immer per Mail oder Push-Nachrichten in der Amazon-App. Diese Mails und Nachrichten können Sie im offiziellen Kundenkonto unter „Mein Konto“ und dann „Message Center“ nachlesen.

So reagieren Sie richtig

Legen Sie sofort auf, wenn Sie die Bandansage hören. Sollten Sie aber bereits auf den Betrug hereingefallen sein, dann müssen Sie schnell reagieren. Ändern Sie Ihre Zugangsdaten für die betroffenen Online-Konten. Richten Sie, wo immer möglich, die Zwei-Faktor-Authentifzierung ein. Prüfen Sie, welche Geräte/Browser/Computer Sie für die Nutzung freigegeben haben. Löschen Sie unbekannte/unberechtigte Geräte. Fertigen Sie zur Beweissicherung Screenshots an und sichern Sie alle Beweismittel wie zum Beispiel die Guthabenkarten.

Informieren Sie den jeweiligen Kundenservice und gegebenenfalls Ihre Bank. Und erstatten Sie Anzeige bei der Polizei. Das ist auch online in allen Bundesländern möglich, hier beispielsweise in Bayern.

Die Masche ist übrigens nicht ganz neu: Betrüger versuchen auch Paypal-Nutzer mit derartigen Schockanrufen hereinzulegen, worüber wir hier kürzlich berichtetet hatten.

Quelle: https://www.pcwelt.de/article/2037648/amazon-polizei-warnt-betrugsmasche.html?utm_date=20230829140342&utm_campaign=Security&utm_content=Title%3A%20Amazon%3A%20Polizei%20warnt%20vor%20neuer%20Betrugsmasche%20%E2%80%93%20so%20sch%C3%BCtzen%20Sie%20sich&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

8) Telefonbetrug: Das tust du, wenn dich diese Hamburger Nummer anruft

Ein Callcenter versucht vehement neue Opfer für ihren Telefonbetrug anzulocken. Mit diesen Methoden enttarnst du die Masche sofort.

Beim **Telefonbetrug** melden sich oft unscheinbare Callcenter bei den potentiellen Opfern. Aktuell versucht es eine Nummer mit einer Hamburger Vorwahl. Was passiert, wenn du abnimmst und wie du richtig reagierst, verraten wir dir jetzt.

Telefonbetrug mit Internetgewinnspiel

Telefonbetrug kennt viele Facetten. Eine sehr beliebte Masche der zwielichtigen Callcenter-Mitarbeitenden ist, von einem angeblichen Restbetrag eines Internetgewinnspiels zu berichten. Sie melden sich häufig direkt damit, dass sie von der Mahnabteilung abrufen. Das Opfer an der anderen Leitung befindet sich also sofort in einer Stressituation.

Es wird argumentiert, dass die Teilnahme vorerst kostenlos war, aber vergessen wurde, zu kündigen. Entsprechend müssen die Opfer nun zahlen. Doch wie es der Zufall so will, bietet der Anrufer oder die Anruferin mit der 040-Vorwahl auch eine weitere Option an. Man könne stattdessen ein dreimonatiges Abo abschließen und so die Kosten tilgen. Der nächste Schritt bei diesem Telefonbetrug ist es nun, deine IBAN in Erfahrung zu bringen.

Diese Indizien enttarnen den Betrug

Spätestens an dieser Stelle solltest du stutzig werden und auflegen. Die ganze Situation ist nur allzu absurd. Natürlich kann es passieren, dass man vergisst, einen Aboservice zu kündigen. Aber wieso sollte der Kundenservice dir nun ein kostenpflichtiges Abo anbieten, bevor du die angeblichen Schulden beglichen hast?

Doch es gibt noch weitere Indizien, die den Telefonbetrug kennzeichnen. So sollen laut giga die Personen am Telefon nur sehr schlecht deutsch sprechen. In Anbetracht auf die Hamburger Vorwahl ist daher davon auszugehen, dass es sich hierbei um eine getarnte Rufnummer aus dem Ausland handelt. Dies ist ein typisches Anzeichen der betrügerischen Maschen.

Zudem stellen die Mitarbeitenden häufig Fragen, die man zwangsläufig mit „Ja“ beantworten muss, wie etwa „Spreche ich hier mit …?“. Auch auf „Hören Sie mich?“ solltest du niemals antworten. Daraus kann mithilfe von Schnittprogrammen sonst sehr schnell eine gefälschte Vertragszusage entstehen.

Weigerst du dich deine IBAN weiterzugeben, werden die Mitarbeitenden schnell ungeduldig oder gar beleidigend. Oft beenden sie dann das Telefon. Allerdings kommt es durchaus vor, dass wenige Stunden oder Tage später dich dieselbe Rufnummer nochmal versucht zu erreichen.

Blockiere die gesamte Rufnummern-Gasse

Willst du dich vor diesem Telefonbetrug schützen, kannst du die gesamte Rufnummerngasse sperren. Das gelingt kinderleicht am Android-Handy oder bei der FritzBox. Da gebt ihr als blockierte Nummer dann einfach **0402999699*** an. So kann dich das betrügerische Callcenter auch dann nicht anrufen, wenn sich die Endziffern ändern. Beim iPhone musst die Nummern einzeln blockieren.

Quelle: https://www.futurezone.de/digital-life/article483741/telefonbetrug-das-tust-du-wenn-dich-diese-hamburger-nummer-anruft.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

9) Millionen Nutzer betroffen: Daten von Duolingo im Darknet verkauft

Die Daten von 2,6 Millionen Duolingo-Nutzern wurden in einem Hacker-Forum veröffentlicht. Wir erklären, welche Informationen geleakt wurden und wie Sie herausfinden, ob sie betroffen sind.

Ein Hacker hat die Daten von 2,6 Millionen Duolingo-Nutzern veröffentlicht. Die gestohlenen Informationen enthalten sowohl öffentliche als auch nicht-öffentliche Daten, einschließlich **Namen, E-Mail-Adressen und Informationen zur Nutzung** der Sprachlern-App.
Die veröffentlichten Informationen können von Angreifern für **gezielte Phishing-Angriffe** gegen Duolingo-Nutzer verwendet werden.

Informationen von 2,6 Millionen Nutzern veröffentlicht

Wie die IT-Sicherheitsseite Bleepingcomputer berichtet, wurden die Daten durch eine

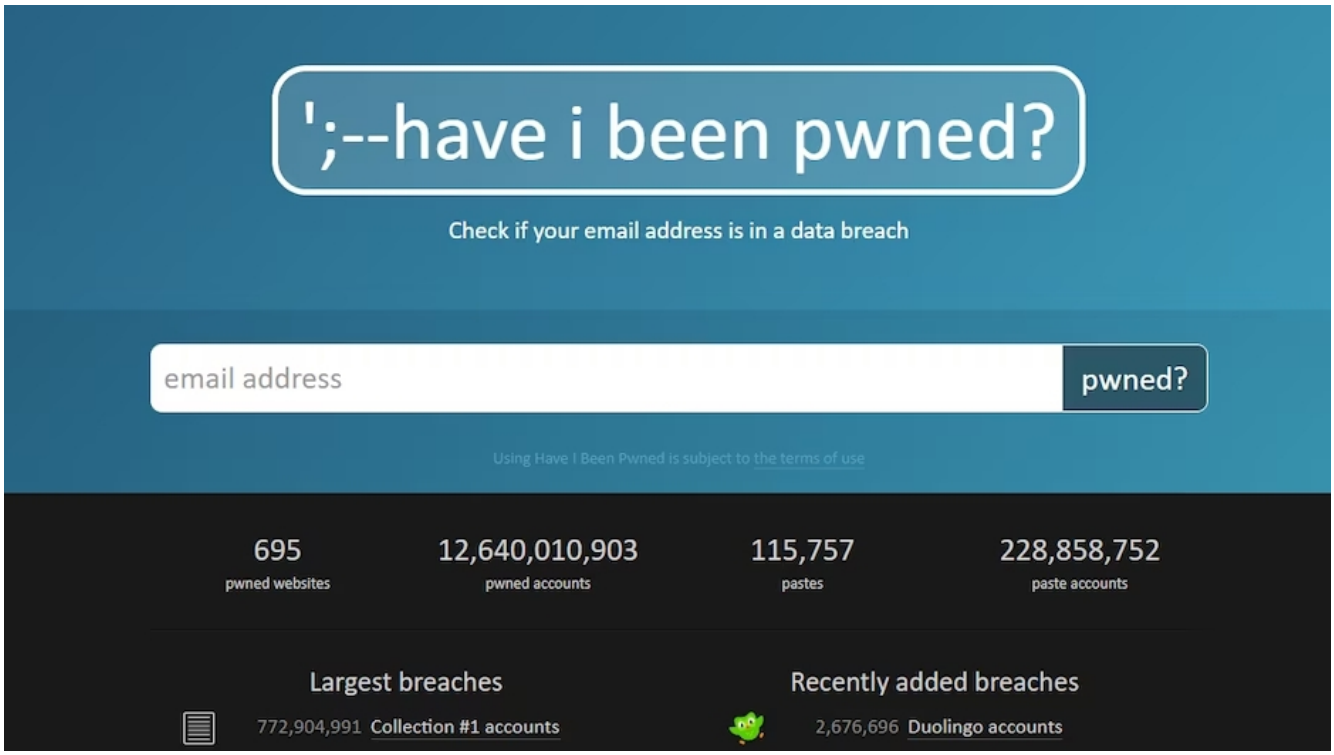
offengelegte Programmierschnittstelle (API) gesammelt, die es jedem ermöglicht, einen Benutzernamen oder eine E-Mail-Adresse einzugeben und die zugehörigen Profilinformationen zu erhalten.

Duolingo habe bereits im Januar bestätigt, dass die Daten aus **öffentlichen Profilinformationen** stammen und weitere Vorsichtsmaßnahmen geprüft. Das Unternehmen hat sich jedoch nicht zu den **E-Mail-Adressen** geäußert, die normalerweise nicht öffentlich zugänglich sind. Die vom Datenklau betroffene API sei **weiterhin öffentlich zugänglich**.

Aus den Daten gehe auch hervor, dass manche Nutzer mehr Berechtigungen haben als andere. So könnten Cyberkriminelle möglicherweise auch **Abonnenten der Premium-Version von normalen Nutzern unterscheiden** und personalisierte Phishing-Attacken starten.

Der Fall könnte für Duolingo ein datenschutzrechtliches Nachspiel haben, ähnlich wie beim riesigen Facebook-Datenleck im Jahr 2021.

Datenleck bei Duolingo: So finden Sie heraus, ob Sie betroffen sind



"Have I been pwned?" zeigt Ihnen, ob Ihr Duolingo-Konto betroffen ist. Screenshot/CHIP

Über die Webapp "Have I Been Pwned" können Sie überprüfen, ob Sie vom Datenleck bei Duolingo oder anderen Diensten betroffen sind. Geben Sie dazu die Mailadresse in die Suchzeile ein, die Sie auch für Ihren Duolingo-Account verwenden.

Da durch das Datenleck **keine Passwörter** gestohlen wurden, besteht für betroffene Nutzer keine akute Gefahr. Sie sollten allerdings wachsam auf gezielte Spam- und Phishing-Mails bleiben.

Quelle: https://www.chip.de/news/Millionen-Nutzer-betroffen-Daten-von-Duolingo-im-Darknet-verkauft_184919227.html?utm_source=chip_1001310&utm_content=29.08.2023&utm_medium=email&utm_campaign=1009832

10) Neue KI-Attacken auf Smartphones: 5 Sicherheits-Tipps vom TÜV

Auch der TÜV schlägt bei Künstlicher Intelligenz Alarm. Die Technik werde genutzt, um Cyber-Angriffe zunehmend ausgefeilter zu gestalten. Nutzer sollten sich dieser 5 Sicherheitstipps annehmen, um KI-Angriffe auf Handys abzuwehren.

Komische Formulierungen, auffällige Tippfehler und krude Links, oft lassen sich Phishing-Mails mit einem kritischen Blick recht einfach entlarven. Doch das könnte bald Geschichte sein.

Laut TÜV-Verband verschärft der vermehrte Einsatz von Künstlicher Intelligenz die Bedrohungslage, denn Angreifer perfektionieren ihre Tarnung. "Dank ChatGPT sind die Nachrichten in geschliffenem Deutsch geschrieben", sagt Marc Fliehe, Leiter Digitales und IT-Sicherheit beim TÜV-Verband.
Vielfach werde die Gefahr unterschätzt und durch die quasi beiläufige Nutzung des Smartphones in Situationen des Alltags ist die Gefahr besonders hoch, von Angreifern überrumpelt zu werden. Der TÜV-Verband gibt 5 Sicherheitstipps.

5 Tipps zur Abwehr von KI-Angriffen

Man muss das Rad nicht neu erfinden, um KI-Angriffe auf Handys abzuwehren. Der TÜV-Verband gibt diese 5 Sicherheits-Tipps:

1. **Regelmäßige Updates:** Updates zeitig einspielen, das ist der wichtigste Tipp für Smartphone-Sicherheit. Das gilt aber nicht nur für das Betriebssystem, sondern auch für die genutzten Apps.
2. **Starke Passwörter:** Für alle Accounts sollten Sie ein eigenes, sicheres Passwort verwenden. Der TÜV-Verband empfiehlt eine möglichst willkürliche Reihenfolge von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Damit Sie sich das nicht alles merken müssen, steht Ihnen ein Passwortmanager zur Seite.
3. **Zusatz-Schutz:** "Wann immer möglich, sollte für die Accounts eine Zwei-Faktor-Authentifizierung eingeschaltet werden", rät Fliehe. "Der Zugriff ist dann nur mit Passwort sowie mit einem Bestätigungscode möglich, der an das Smartphone oder per E-Mail gesendet wird."
4. **Sperre aktivieren:** Damit gestohlene oder verlorene Handys nicht zum Sicherheitsrisiko werden, sollten Sie immer den Sperrbildschirm aktivieren.
5. **Daten verschlüsseln:** Zudem empfiehlt es sich laut TÜV-Verband, Daten auf dem Smartphone oder der Speicherkarte zu verschlüsseln. Wenn Cyberkriminelle darauf Zugriff haben, können sie ihre Opfer im schlimmsten Fall mit den erbeuteten Daten wie Bildern, Videos oder Chatverläufen erpressen.

Schutz in öffentlichen WLANs

Besonders auch in freien WLAN-Netzwerken lauern laut TÜV-Verband Gefahren. "Kriminelle Hacker können an einem Flughafen ein eigenes Netz einrichten, das sie dann zum Beispiel "Free Airport" nennen – wer sich einwählt, wird ausgespäht", erklärt Fliehe die Masche.

Doch selbst in einem offiziellen Netz können Angreifer unterwegs sein und versuchen, auf eingeloggte Smartphones Zugriff zu bekommen. Sie lauern darauf, nicht verschlüsselte Daten abzugreifen. "Im Zweifel sollten Nutzer sensible Anwendungen wie Gesundheits-Apps nur dann verwenden, wenn die Datenverbindung erwiesen sicher ist".

Schutztipp: Wer darauf nicht warten kann, sollte ein Virtual Private Network (VPN) verwenden – entsprechende Programme bauen einen virtuellen Tunnel, der die Kommunikation schützt.
VPN-Empfehlungen finden Sie in unserem Test. Wer kein Geld ausgeben will, kann auch mit einem kostenlosen VPN starten.

Quelle: https://www.chip.de/news/Neue-KI-Attacken-auf-Smartphones-5-Sicherheits-Tipps-vom-TUeV_184917737.html?utm_source=chip_1001310&utm_content=29.08.2023&utm_medium=email&utm_campaign=1009832

11) Perfide Betrugs-Masche betrifft ING: Verbraucherzentrale warnt

Wer ein Konto bei der ING hat, sollte wachsam sein. Die Verbraucherzentrale warnt aktuell vor bestimmten Nachrichten, die Kundinnen und Kunden erhalten könnten.

München – Betrüger lassen sich immer neue Maschen einfallen, um ihr Opfer in die Falle zu locken. Vor allem auf die persönlichen Daten haben es die Betrüger oft abgesehen. Damit versuchen sie, die Konten ihrer Opfer zu leeren. Ein unbedachter Klick kann schnell teuer werden, deshalb wird vor den Betrugs-Maschen immer wieder gewarnt. Aktuell sollten vor allem Kunden der ING vorsichtig sein, denn seit Beginn der Woche erhalten vor allem Kunden dieser Bank verdächtige Mails, wie die Verbraucherzentrale berichtet.

Strategien gegen Spam-Mails

Dringende Warnung an Kunden der ING: Betrüger versenden Phishing-Mails

Mit Phishing-Mails versuchen die Betrüger ihre Opfer in der Regel auf unechte Websites zu locken. Mittel der Wahl sind häufig Betrüger-Mails, wie vor kurzem bei der Sparkasse. Betrüger geben sich für ihre Maschen oft als Bank aus und fordern die potenziellen Opfer zu Handlungen auf, klassische Maschen sind zum Beispiel die Bestätigung der eigenen Identität. Es kommt gelegentlich aber auch zu ungewöhnlichen Betrugsmaschen, so erhielten Kunden der Commerzbank vor kurzem die Benachrichtigung, dass sie Geld zurückerhalten sollten.

Aktuell sind jedoch die Kunden der ING von der Masche betroffen. Die Kriminellen informieren die Bankkunden über „ungewöhnliche Aktivitäten“ auf ihrem Konto. „Um Ihr Konto zu schützen und die Sicherheit Ihrer Gelder zu gewährleisten, bitten wir Sie, sich umgehend in Ihr Konto einzuloggen, um Ihre letzten Transaktionen zu überprüfen,“ heißt es in der Mail. Darunter ist ein Link eingebaut, der zum vermeintlichen Login führen soll.

Besonders perfide: Die Betrüger schreiben sogar, sie würden „alle notwendigen Maßnahmen ergreifen, um sicherzustellen, dass Ihr Konto geschützt bleibt.“ Das ist jedoch nicht der Fall – ganz im Gegenteil. Vor kurzem gingen Betrüger sogar so weit, dass sie Phishing-Mails für angebliche Regierungs-Förderprogramme versendeten.

Phishing-Mails erkennen: Was die ING ihren Kunden rät, um sich vor Betrügern zu schützen

Phishing-Mails sind potenziell gefährlich, lassen sich aber anhand einiger Merkmale in der Regel erkennen. Auf ihrer Website empfiehlt die ING selbst, folgende Dinge zu beachten, um sich vorBetrügern zu schützen:

- **Betreff suchen:** Häufig wurden Phishing-Mails bereits gemeldet. Sollte das der Fall sein, findet man über eine Suche im Internet schnell die entsprechenden Informationen.
- **„Mouse-over-Effekt“ nutzen:** Wird mit der Maus über den eingefügten Link gefahren, erkennt man, ob der Link wirklich zur Website der Bank führt.

- **Nachfragen:** Über offizielle Wege wie die Website oder per Telefon direkt bei der Bank nachfragen. Die Mitarbeiter wissen sicher, ob eine Mail von der Bank versendet wurde oder nicht.

Phishing-Mails an ING-Kunden: Ein falscher Klick kann teuer werden – keine Links öffnen

Weiter informiert die ING auch, dass von der Bank in der Regel nie ein Link zum Login in einer E-Mail versendet wird. Laut der Verbraucherzentrale kann auch eine unpersönliche Anrede ein Anzeichen für eine Betrüger-Mail sein. Zudem versuchen die Betrüger ihre Opfer häufig mit einer angeblichen Gebühr oder einem Zeitlimit unter Druck zu setzen.

Wer eine verdächtige E-Mail erhält, sollte auf keinen Fall einen Link öffnen oder antworten. Stattdessen sollte die entsprechende E-Mail am besten in den Spam-Ordner verschoben oder gelöscht werden. Nicht nur per Mail, sondern auch übers Telefon kontaktieren Betrüger potenzielle Opfer und klingen dabei oft täuschend echt .

Quelle: https://www.fr.de/verbraucher/phishing-mails-von-betruegern-erkennen-betrug-online-geld-bank-warnung-ing-kunden-92476877.html

12) App klaut Bankkonten-Daten: Polizei warnt vor fieser Masche

Eine App, die sich als Scanner tarnt, greift im Hintergrund auf Bankkonten zu. Betroffene sollten schnell handeln.

Die Polizei München warnt derzeit vor einer fiesen Betrugsmasche durch eine Smartphone-App, welche das Smartphone fremd steuern und auf Online-Banking-Apps zugreifen kann. Unter dem simplen Namen "PDF AI" gelangte die App über die App-Stores auf die Geräte der Opfer.

Schadsoftware "PDF AI": Diese App sollten Sie sofort löschen

Der KI-Hype macht sich seit Monaten auch in den App-Charts bemerkbar. Dies machen sich immer häufiger auch Cyberkriminelle zunutze, um Schadsoftware auf die Smartphones der Nutzer einzuschleusen.

So auch im Fall der App "PDF AI", die nur zum Schein als KI-PDF-Assistent funktioniert. Im Hintergrund lädt die Software **weitere Malware** auf das Gerät, **verhindert das Ausschalten und Zurücksetzen** des Smartphones und **greift auf Online-Banking-Apps zu**. Auffällig ist zudem, dass die App im Hintergrund sehr viel Akku verbraucht.

In mehreren Fällen ist es den Betrügern dabei gelungen, Bankgeschäfte über die Konten der Oper zu tätigen und mehrere Tausend Euro abzubuchen. Bei einer Nutzerin eröffneten die Täter sogar ein neues Girokonto, von welchem sie **mehrere Zehntausende Euro** an eine andere Person transferierten. Die Überweisungen konnten jedoch noch durch die Bank gestoppt werden.

Handy-Viren: Polizei gibt Tipps

Mittlerweile wurde die App aus den gängigen App-Stores wieder entfernt, sie könnte sich jedoch bereits unbemerkt auf zahlreichen Smartphones eingenistet haben.

Die Polizei empfiehlt daher, im Zweifel das Bankkonto am besten über ein anderes Gerät auf verdächtige Aktivitäten zu überprüfen. Im App-Store rät die Polizei zu besonderen

Vorsichtsmaßnahmen:

Sie sollten nur Apps von bekannten Herausgebern herunterladen und kritisch überprüfen, ob es sich um originale und legitime Software handelt. Da positive Rezensionen auch gefälscht werden können, sollten Sie zudem Erfahrungen anderer Nutzer recherchieren.

Quelle: https://www.chip.de/news/App-klaut-Bankkonten-Daten-Polizei-warnt-vor-fieser-Masche_184915890.html?utm_source=chip_1001310&utm_content=29.08.2023&utm_medium=email&utm_campaign=1009813

13) Deutsche Rentenversicherung warnt – Zusatzrente gewinnen? Diese Masche steckt dahinter

Das Gewinnspiel eines Privatunternehmens preist eine Zusatzrente an. Es wird in einem Schreiben verschickt, das denen der Deutschen Rentenversicherung ähnelt.

Ein Rubbellos, das zurzeit in vielen deutschen Briefkästen landet, preist eine Zusatzrentenversicherung als Hauptgewinn an. Haben auch Sie einen solchen Brief erhalten? Dann "seien Sie kritisch", warnt die Deutsche Rentenversicherung auf ihrer Webseite.

Das Schreiben des privaten Unternehmens Burda Direct GmbH aus Offenburg sehe den jährlichen Renteninformationen der gesetzlichen Rentenversicherung stark ähnlich, hat mit ihnen aber nichts zu tun. Besonders trügerisch sei das Logo im Briefkopf, das von dem der Rentenversicherung kaum zu unterscheiden ist.

In den Schreiben werde die Chance auf eine Zusatzrente in Höhe von 50.000 Euro in Aussicht gestellt, wenn man an einem Gewinnspiel teilnimmt. Die Empfänger werden aufgefordert, sich telefonisch registrieren zu lassen.

Ziel ist das Einsammeln von Daten

Die Burda Direct GmbH, eine Tochter des Offenburger Burda Verlags, ist ein privates Unternehmen, das sich eigenen Angaben zufolge auf die Daten von Konsumenten spezialisiert hat. "Ziel solcher Gewinnspiele ist es, persönliche Daten einzusammeln, um sie für Werbezwecke zu nutzen", schreibt die Deutsche Rentenversicherung.

Häufig werde im Zuge dieser "Gewinnspiele" dann der persönliche Kontakt am Telefon genutzt, um Produkte oder Abonnements zu verkaufen, heißt es. "Die Deutsche Rentenversicherung rät allen, die nicht möchten, dass ihre persönlichen Daten für Werbezwecke genutzt werden, der Datennutzung aktiv zu widersprechen. Ansonsten könnten große Mengen von Werbemails, weitere Post oder auch Anrufe die Folge sein."

Quelle: https://www.t-online.de/finanzen/ratgeber/altersvorsorge/gesetzlicherente/id_100228758/-zusatzrente-vorsicht-masche-gewinnspiel-gleicht-renten-information.html

14) Temu: Vebraucherzentrale warnt vor Billigplattform

Die Shopping-App Temu erobert derzeit die App-Charts. Doch die Verbraucherzentrale warnt vor der Billigplattform. Wir erklären dir, worauf du beim Einkauf über die App achten solltest.

Mit dem Slogan „Shoppe wie Milliardäre“ wirbt die Plattform Temu in Apples App Store und Googles Play Store. Dabei handelt es sich bei der App in Wirklichkeit um eine Billigplattform mit Schnäppchen und Rabatten.

Doch die niedrigen Preise seien oft verbunden mit einer „geringen Produktqualität und -sicherheit“, warnt nun die Verbraucherzentrale. Deshalb solltest du auf gewisse Aspekte vor einer Bestellung besonders achten.

Das Problem mit der Billigplattform Temu

Bei Temu kannst du so ziemlich alles kaufen. In der App-Beschreibung werden unter anderem Mode, Deko für Zuhause, Kosmetik, Kleidung und Schuhe aufgezählt. Aber auch Smartwatches oder Kopfhörer findest du bei Temu für den kleinen Taler.

Doch laut der Verbraucherzentrale gibt es bereits viele Kund:innen, die die Plattform kritisieren. Demnach seien die schlechte Qualität der Waren, nicht erhaltene Sendungen sowie schlecht verpackte Produkte häufige Probleme bei den Bestellungen.

Wie funktioniert Temu?

Die Verbraucherzentrale vergleicht Temu mit der Shopping-App Wish. Denn die Plattform verkaufe Produkte ebenfalls nicht selbst, sondern über externe Händler:innen. Außerdem gebe es kaum Marken, sondern hauptsächlich No-Name-Produkte.

Die niedrigen Preise bei Temu würden außerdem dazu führen, dass kein Zoll gezahlt werden muss. Jedoch könne es passieren, dass Kund:innen Einfuhrumsatzsteuern sowie Verbrauchssteuern zahlen müssten. Diese würden häufig von Paketdiensten ausgelegt und dann bei der Zustellung eingefordert.

Häufige Kritikpunkte an der Billigplattform

Größter Kritikpunkt an der App und ihren Produkten dürfte wohl die Qualität sein. Laut der Verbraucherzentrale bestehe die Möglichkeit, dass „No-Name-Produkte angeboten werden, deren Qualität und Sicherheit fragwürdig sein könnten“.

Das Verbraucher- und Ratgebermagazin Servicezeit vom *WDR* konnte dies bei einem Probeeinkauf bestätigen. Dabei hätten einige Produkte schlechte Qualität aufgewiesen, andere waren durch en Transport beschädigt oder kleiner als auf den Fotos abgebildet.

Auch könne es laut der Verbraucherzentrale zu längeren Lieferzeiten kommen. Das liege daran, dass die Plattform vor allem Waren aus China anbieten.

In den App-Bewertungen in den Stores von Apple und Google ist vor allem auch die aufdringliche Werbung der Plattform ein großer Kritikpunkt. Demnach verschicke die App mehrfach am Tag Push-Benachrichtigungen, die zum Kauf verleiten sollen.

Darauf solltest du beim Einkauf achten

Die Verbraucherzentrale rät dazu, sich vor einem Einkauf bei Temu über die geltenden Zollbestimmungen zu informieren. Dies sei bei Bestellungen außerhalb der EU erforderlich, da sonst zusätzlich Steuern oder Zollgebühren anfallen können.

Außerdem solltest du versuchen, eine andere Zahlungsart als Vorkasse zu wählen. So kannst du deine Bestellung bezahlen, sobald du deine Produkte erhalten hast und mit diesen zufrieden bist.

Wie bei vielen Plattformen für Online-Shopping kann es auch bei Temu nicht schaden, einen Blick in die Bewertungen zu werfen. Diese können dir im Zweifelsfall bei deiner Kaufentscheidung helfen.

Quelle: https://www.basicthinking.de/blog/2023/08/21/vebraucherzentrale-warnt-vor-temu/

15) Dringend updaten: Kriminelle nutzen Sicherheitslücke in beliebter PC-Software aus

In einer Software, die weltweit von Millionen Nutzern verwendet wird, wurde eine Sicherheitslücke entdeckt. Diese wird bereits von Kriminellen genutzt.

Der Sicherheitsexperte "goodbyeselene" warnt via "Zero Day Initiative" vor einer gefährlichen Sicherheitslücke. Betroffen ist hier das Tool WinRAR, das viele Nutzer zum Archivieren und Komprimieren von Dateien nutzen.

Die Schwachstelle trägt den Namen CVE-2023-40477. Angreifer können hier potentiell beliebigen Code auf dem Gerät aufspielen. Voraussetzung für die Ausnutzung der Lücke ist, dass der Nutzer zuvor eine bösartige Webseite oder eine bösartige Datei öffnet. Die Gefährlichkeit der Schwachstelle wird mit einem CVSS-Score von 7,8 und dem Schweregrad "hoch" eingestuft.

Wie nun "Techcrunch" berichtet, wurden bereits 130 Infektionen über die Schwachstelle in WinRAR nachgewiesen. Die gute Nachricht: Den Kriminellen ist es bisher offenbar nicht gelungen, über installierte Malware auf die Konten der Nutzer zuzugreifen.

Sicherheitslücke in WinRAR entdeckt: Nutzer sollten Software dringend updaten

Der Forscher hatte dem WinRAR-Hersteller RARLAB die Sicherheitslücke bereits Anfang Juni gemeldet, öffentlich gemacht wurde die Schwachstelle erst am vergangenen Donnerstag. Das liegt voraussichtlich daran, dass man Cyberkriminelle nicht darüber informieren wollte.

Seit Anfang August ist das neue Update 6.23 für WinRAR verfügbar, das die Sicherheitslücke schließt. Haben Sie die Software auf Ihrem Gerät, sollten Sie daher überprüfen, welche Version Sie nutzen und gegebenenfalls ein Update aufspielen. Den zugehörigen Download finden Sie auch bei CHIP unter diesem Beitrag.

Quelle: https://www.chip.de/news/Sicherheitsluecke-in-millionenfach-genutzter-Software-Nutzer-muessen-updaten_184913962.html?utm_source=flipboard&utm_content=other

16) Vorsicht, Betrug – Phishing-Mails werden im Namen von Saturn versendet

Wenn Sie gerade eine Mail vom Elektrohändler Saturn bekommen haben, sollten Sie vorsichtig sein. Betrüger nutzen den Namen der Kette für Phishing-Mails.

Täglich werden Millionen betrügerische E-Mails im Namen bekannter Firmen verschickt. Besonders beliebt bei Betrügern: Phishing-Mails, die mit hochwertigen Gewinnen oder attraktiven Gutscheinen für das jeweilige Unternehmen locken. Letztlich wollen diese Mails aber nur persönliche Daten oder Geld des Empfängers erbeuten. Jetzt sind einem Bericht des Verbraucherportals Biallo zufolge auch Saturn-Kunden betroffen.

Phishing-Mails von Saturn versprechen iPhone 14

Die Nachrichten stammen vermeintlich vom Elektronikhändler Saturn und versprechen Preise oder Gewinnchancen. Die Nachrichten erwecken den Eindruck, dass sie

wirklich von Saturn stammen und verwenden missbräuchlich Firmennamen und Logo.

In den Nachrichten, die nicht nur per Mail, sondern teilweise auch per SMS versandt werden, heißt es beispielsweise, Sie hätten ein iPhone 14 Pro Max gewonnen. In anderen Nachrichten wird behauptet, Sie seien für einen Artikel und Versand nominiert.

Allerdings sollten Sie auf keinen Fall auf die Links in den E-Mails klicken. Dort werden Sie andernfalls wahrscheinlich auf gefälschte Internetseiten geleitet, auf denen Ihre Daten abgefragt werden. Bleiben Sie misstrauisch und löschen Sie verdächtige Mails ungelesen.

Wie erkennen Sie Phishing-Mails?

Auch, wenn die Mails häufig täuschend echt wirken, gibt es ein paar Tipps, wie Sie die Betrüger sofort entlarven können. Folgende Punkte zählen zu den wichtigsten Merkmalen:

- Die Nachricht enthält Grammatik- und Rechtschreibfehler.
- Die Mail ist nicht in deutscher Sprache verfasst.
- Ihr Name fehlt in der Anrede.
- Sie sollen Daten angeben.
- Angeblich haben Sie nur für eine kurze Zeitspanne die Möglichkeit zu handeln.
- Sie sollen eine Datei oder Links öffnen.
- Sie haben zuvor noch nie E-Mails des Absenders (z. B. Saturn) erhalten und sind auch kein Kunde.

Die Verbraucherzentrale rät dazu, verdächtige Mails nicht zu öffnen und direkt zu löschen. Zusätzlich sollten Sie die Absenderadresse sperren. Haben Sie die Mail schon geöffnet und sind sich nicht sicher, ob sie seriös ist, sollten Sie beim Absender direkt nachfragen, nicht jedoch über eine Antwort auf die Mail. Öffnen Sie außerdem keine Links oder Dateianhänge.

Quelle: https://www.t-online.de/digital/aktuelles/id_100227232/phishing-mails-betrueger-versenden-mails-von-saturn-.html

17) Mitten in der Urlaubssaison: Betrüger versuchen an Daten von Booking-Kunden zu kommen

Aktuell machen wieder Phishing-Mails die Runde. Diesmal von der Betrugsmasche betroffen: der Urlaubsanbieter Booking.com.

München – Sommer, Sonne, Strand – auch wenn das Wetter derzeit zu wünschen übrig lässt, ist die Urlaubssaison in vollem Gange. Auch in Bayern und Baden-Württemberg sind nun Ferien und damit in fast ganz Deutschland. Wenn in Deutschland das Regenwetter einfach kein Ende finden will, suchen viele das Weite; und buchen spontan Strandurlaub im Süden. Vor allem viele Kurzentschlossene buchen im Internet auf den letzten Drücker ihr Ticket Richtung Sonne.

Doch auch wer seine Reise schon längerfristig online gebucht hat, sollte sich in Acht nehmen. Hier tummeln sich oftmals Cyber-Kriminelle. Aktuell verschicken Betrüger im Namen von Booking.com Phishing-Mails verschickt, um an die sensiblen Daten – und nicht zuletzt an das

Geld – von Kunden zu kommen.

Phishing-Mails im Namen von Booking.com: Zahlungsinformationen sollen bestätigt werden

In der E-Mail fordern die Betrüger den Kunden dazu auf, die Zahlungsinformationen zu bestätigen. „Wir werden diese Informationen nur einmal erfragen“, steht in der Mail. Grund dafür sei ein neues Update der Booking-App. Der Kunde soll zudem sicherstellen, dass der Verkauf auf digitalem Wege von der neuen Zahlungsmethode unterstützt wird.

Über einen blauen Button sollen Kunden sich einloggen. Tun sie das nicht, werde das Kundenkonto innerhalb von zwei Tagen geschlossen, die gebuchte Reise verfällt. Dafür soll eine Gebühr von 19,99 Euro erhoben werden. Ganz unten findet sich der Hinweis, dass die Mail von künstlicher Intelligenz erstellt wurde, eine Antwort auf die Mail sei daher sinnlos.

Verbraucherzentrale warnt vor Betrugs-Masche: in den Spam-Ordner verschieben

Die Verbraucherzentrale warnt dringend davor, auf das blaue Feld zu klicken. Die Mail soll unbeantwortet in den Spam-Ordner verschoben werden. Versendet wird die Phishing-Mail mit dem Betreff: „Erinnerung: Aktualisierung Ihrer Informationen erforderlich“. Zudem kann Betrug im Namen von Booking.com auch an der E-Mail-Adresse des Senders, erkannt werden, erklärt *partner.booking.com*.

Demnach enden die echten E-Mail-Adressen des Unternehmens immer mit booking.com. Ein klarer Hinweis auf Betrug sind auch Fehler in der Rechtschreibung oder Grammatik. Aber auch dringliche Sprache, oder ein Teil des Textes in einer Fremdsprache, können Anzeichen für eine Betrugsmasche sein.

Betrüger stehlen Daten: So erkennt man eine Phishing-Mail

- Falsche E-Mail-Adresse
- Fehler in der Rechtschreibung oder Grammatik
- Dringliche Sprache oder Drohungen
- Fremdsprache im Text
- Der Verweis auf einen Button oder Internet-Link

Quelle: https://www.merkur.de/verbraucher/mail-masche-betrueger-daten-klau-booking-com-betrug-phishing-92447606.html

18) Hacker verbreiten Schadsoftware über Whatsapp: Android-Smartphones infiziert

Cybergangster verteilen über Whatsapp eine Malware, die Android-Geräte infiziert. Danach haben die Angreifer Zugriff auf die infizierten Androiden. So läuft der Angriff.

Hacker infizieren derzeit mit einer präparierten Android-App Smartphones und stehlen von diesen Geräten Textdateien/SMS, Telefon-Logdateien, Kontakte sowie GPS-Standortdaten und lesen die über Messenger wie Whatsapp, Telegram, Signal, Viber oder den Facebook Messenger ausgetauschte Kommunikation mit. Die erbeuteten Daten sendet die App dann an den Server der Angreifer.

Sicherheitsexperten des Unternehmens Cyfirma vermuten die indische APT-Hackergruppe „Bahamut“ hinter dem Angriff, wie das US-IT-Sicherheitsportal Bleepingcomputer berichtet. Diese Bahamut-Gruppe treibt schon länger ihr Unwesen und versucht Spyware zu verbreiten.

Angreifer nutzen Whatsapp zur Verbreitung ihrer Schadsoftware

Die Vorgehensweise der Angreifer ist dabei immer ähnlich: Die Angreifer überreden die Opfer unter einem Vorwand dazu, die Konversation auf eine angeblich sicherere Plattform zu verlagern. Hierzu müsse das Opfer eine spezielle Chat-App namens „SafeChat“ installieren, die die Angreifer dem Opfer über Whatsapp senden. Diese angeblich sichere Chat-App besitzt eine täuschend echt wirkende Oberfläche und verlangt von dem Opfer einen scheinbar legitimen Authentifizierungsprozess. Das alles soll das Vertrauen der Opfer gewinnen.

Weitreichende Rechte auf dem Androiden

Bei der Installation muss der überrumpelte Benutzer der „SafeChat“-App entscheidende Rechte auf seinem Androiden einräumen. Danach hat die Spyware fast vollen Zugriff auf das Gerät des Opfers. Die App ist nach dem Start selbst dann im Hintergrund aktiv, wenn der Nutzer sie ausdrücklich beendet.

Derzeit suchen die Angreifer allerdings nur Opfer im südasiatischen Raum. Cyfirma hat hier eine ausführliche Analyse der Bedrohung veröffentlicht. Die Sicherheitsexperten vermuten einen Staat hinter dem Angriff, der im indischen Raum angesiedelt ist.

Wieso ist das auch für deutsche Nutzer wichtig?

Zwar sind derzeit nur asiatische Nutzer im Visier dieser Angreifer, doch die Vorgehensweise der Angreifer sollte sich jeder Smartphone-Besitzer vor Augen halten: Über Social-Engineering versuchen die Angreifer ihre Opfer zu überrumpeln. Sie überreden diese dazu, eine andere App zu installieren, die nicht von Google Play stammt. Das ist der entscheidende Fehler. Sie reduzieren Ihr Infektionsrisiko deutlich, wenn Sie konsequent nur Apps von Google Play installieren und sich nicht zur Installation von Apps aus anderen Quellen überreden lassen.

Installieren Sie zudem einen aktuellen Virenscanner auf dem Androiden.

Tipp: Whatsapp-Falle: Hacker locken mit Gratis-Bier – so erkennen Sie den Betrug
Betrüger übernehmen Konten von schlafenden Whatsapp-Nutzern

Quelle: https://www.pcwelt.de/article/2014191/hacker-verbreiten-schadsoftware-uber-whatsapp-android-smartphones-infiziert.html?utm_date=20230830103747&utm_campaign=Security&utm_content=Title%3A%20Hacker%20verbreiten%20Schadsoftware%20%C3%BCber%20Whatsapp%3A%20Android-Smartphones%20infiziert&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

19) Warnung vor falschen PayPal-Anrufen

Schockanrufe im Namen des Zahlungsdienstes PayPal: Kriminelle informieren über eine angeblich anstehende Überweisung eines hohen Geldbetrags. Tatsächlich gibt es die aber nicht.

Das Wichtigste in Kürze:

- Wenn Sie einen Anruf erhalten und eine Computerstimme meint, Sie würden in Kürze mehrere hundert Euro bei PayPal überweisen, legen Sie auf!
- Mit dieser neuen Variante eines Schockanrufs sind Kriminelle derzeit aktiv.
- Welche Ziele sie verfolgen, ist unklar. Allerdings sollten Sie die Behauptungen keinesfalls glauben!

Das Telefon klingelt und eine automatisierte Stimme informiert darüber, dass angeblich eine Zahlung über mehrere hundert Euro bei PayPal veranlasst worden sei. Falls man sie stoppen wolle, soll man eine Taste drücken.

So schildern uns Verbraucher:innen eine offensichtliche Betrugsmasche. Sie erinnert an frühere betrügerische Anrufe, bei denen sich Unbekannte als Interpol, Europol oder Polizei ausgegeben haben. Dabei wurden diejenigen, die nach der Ansage tatsächlich eine Taste gedrückt haben, mit einem Menschen verbunden und im Gespräch zum Zahlen von Geld auf Auslandskonten oder zum Investieren in Kryptowährungen gedrängt.

Keine Zahlungen im PayPal-Konto gebucht

Bislang haben uns alle Betroffenen der PayPal-Masche mitgeteilt, dass sie teils noch während der automatischen Ansage aufgelegt haben. Somit wissen wir nicht, was tatsächlich passiert, wenn man eine Taste drückt. Alle Betroffenen schilderten uns bisher jedoch, dass sie in ihren PayPal-Konten keine Zahlungen gesehen haben. Das ist ein eindeutiger Hinweis darauf, dass der Anruf ein Betrugsversuch gewesen sein dürfte.

Das ist auch unser wichtigster Tipp: Falls Sie so einen Anruf erhalten, **legen Sie auf! Drücken Sie keine Taste**, um mit jemandem verbunden zu werden! Öffnen Sie die PayPal-App oder die echte Internetseite paypal.de, melden Sie sich dort mit Ihren Zugangsdaten an und sehen Sie nach, ob es wirklich eine Zahlungsanweisung über einen hohen Betrag gibt. Falls ja, nehmen Sie über die App oder die Internetseite Kontakt zum echten PayPal-Kundenservice auf!

PayPal-Sprecherin Sabrina Winter stellt klar, dass "PayPal seine Kunden in der Regel nicht anruft – und schon gar nicht mit der Aufforderung, Zahlungen zu leisten".

"Woher haben die meine Nummer?"

Bei solchen Anrufen fragen sich Betroffene, wie die Kriminellen an ihre Telefonnummer gekommen sein mögen. Darauf können wir keine klare Antwort geben. Am wahrscheinlichsten ist es aus unserer Sicht, dass zahlreiche Nummern "auf gut Glück" angerufen werden. Dabei müssen die Betroffenen nicht mal ein PayPal-Konto haben. Bei der großen Verbreitung des Zahlungsdienstes ist es aber sehr wahrscheinlich, dass die Kriminellen einen Treffer landen. Und wer dann eine Taste drückt, gibt ihnen die Bestätigung, über ein PayPal-Konto zu verfügen. Das ist vergleichbar mit Phishing-Mails, die im Namen großer Unternehmen wahllos verschickt werden – auch an Personen, die gar keine Verbindung zu dem Unternehmen haben.

Ihre Nummer könnte zum Beispiel aus öffentlichen Telefonverzeichnissen stammen oder aus früheren Datenlecks verschiedener Firmen. Mit so genanntem Scraping können öffentlich sichtbare Telefonnummern systematisch gesammelt werden. "Da Phishing-Angriffe zunehmend per SMS oder über Messenger-Apps erfolgen", hat z.B. das Online-Portal Kleinanzeigen die Abfrage einer Telefonnummer für private Verkäufe abgeschaltet.

Falls Sie Ihre Nummer mal bei einem Gewinnspiel angegeben haben, könnte sie weiterverkauft worden sein. Eine weitere mögliche Ursache sind schädliche Apps, die vielleicht jemand unbewusst auf seinem Smartphone installiert hat, in dem Ihre Nummer gespeichert ist. Es gibt Apps, die Kontaktdaten auslesen und sammeln. Sie kommen zum Beispiel durch so genanntes Smishing (Phishing per SMS) auf die Geräte, wie etwa über die Paketdienst-Masche oder Sprachnachricht-Masche.

Quelle: https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/warnung-vor-falschen-paypalanrufen-86727

Anwenderinformationen:

1) Darum klingelt am 14. September um 11 Uhr Ihr Handy

Am 14. September 2023 um 11 Uhr lärmt Ihr Handy los. Sogar, wenn Sie es auf lautlos gestellt haben. Und das ist noch nicht alles. Der Grund.

Am 14. September, einem Donnerstag, findet um 11 Uhr wieder der bundesweite Warntag statt. Das teilt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) mit. An diesem Tag testen Bund, Länder und Kommunen die Funktionsfähigkeit ihrer Warnsysteme. Seit dem desaströsen Versagen der Warnfunktionen am Warntag am 10. September 2020, in dessen Folge sogar der Chef des BBK seinen Hut nehmen musste, stehen die in Deutschland vorhandenen Warnsysteme wieder verstärkt in der öffentlichen Wahrnehmung.

Der bundesweite Warntag soll die Funktionsfähigkeit der unterschiedlichen Warnsysteme überprüfen. Außerdem dient der Warntag dazu, die Bevölkerung über die unterschiedlichen Warnmittel zu informieren.

Diese Warnmittel werden am 14.9.2023 um 11 Uhr getestet

Wenn das BBK am Warntag seine Probewarnung in Form eines Warntextes an alle an das „Modulare Warnsystem“ angeschlossenen Systeme verschickt, wird diese Warnung über unterschiedliche Wege an die Bevölkerung weitergegeben.

- Sie sehen die Warnung also am Fernseher und hören Sie im Radio.
- Sie erhalten via Cell Broadcast eine Warnnachricht auf Ihr Handy, sofern dieses kompatibel ist (das ist bei allen halbwegs modernen Geräten der Fall). Deutschland hatte Cell Broadcast anders als viele andere Staaten lange Zeit nicht für notwendig erachtet, doch das Debakel am Warntag 2020 führte zu einem Umdenken und Deutschland zog nach. Mehr zu Cell Broadcast lesen Sie hier. Am bundesweiten Warntag im Dezember 2022 wurde Cell Broadcast erstmals getestet. Dabei zeigte sich, dass die Warnungen nun besser als noch 2020 weitergegeben wurden.
- Sie können sich im Internet über www.warnung.bund.de informieren.
- Öffentliche Sirenen, sofern vorhanden und funktionstüchtig, heulen los. Nachdem der Warntag 2020 den desolaten Zustand des Sirenenwarnsystems offengelegt hatte, werden nun wieder neue Sirenenanlagen in Deutschland aufgestellt: Deutschland bekommt neue Warnsirenen für Katastrophenwarnungen.
- Lautsprecherwagen, sofern vorhanden, geben die Warnung weiter. Auch stationäre Lautsprecher können die Warnung ausgeben.
- Digitale Stadtinformationstafeln sowie Fahrgastinformationssysteme geben die Warnung aus.
- Die diversen Warnapps zeigen eine entsprechende Warnung an. Mehr dazu lesen Sie hier: Die besten Katastrophen- und Terrorwarn-Apps für Android und iOS.

Gegen 11.45 folgt die Entwarnung über alle Warnmittel und Endgeräte, über welche zuvor die Warnung versendet wurde. Mit einer Ausnahme: Über Cell Broadcast wird noch keine Entwarnung verschickt. Derzeit prüfen die Mobilfunknetzbetreiber, ob sie auch für Cell Broadcast eine Entwarnung verschicken können.

Unabhängig vom bundesweiten Warntag gibt es auch auf einzelne Bundesländer begrenzte Warntage: Darum klingeln heute nur in diesen beiden Bundesländern alle Handys.

Sie finden auf dieser Seite des BKK alle Informationen zum bundesweiten Warntag am 14.9.2023 um 11 Uhr.

Quelle: https://www.pcwelt.de/article/2044702/darum-klingelt-am-14-september-um-11-uhr-ihr-handy.html?utm_date=20230829123601&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Darum%20klingelt%20am%2014.%20September%20um%2011%20Uhr%20Ihr%20Handy&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

2) download – Samsung Smart Switch

Samsung bietet mit der Anwendung Smart Switch eine Möglichkeit, Daten auf dem Rechner zu sichern und zum späteren Zeitpunkt wiederherzustellen oder auf ein neues Samsung Smartphone zu übertragen. Bei dem alten Gerät muss es sich dabei nicht zwangsläufig auch um ein Samsung-Gerät handeln.

Mit der Windows-Anwendung Samsung Smart Switch lassen sich Smartphonedaten auf dem Rechner speichern, wiederherstellen und auf ein neues Samsung-Smartphone übertragen. Nachdem das Smartphone per USB-Datenkabel mit dem Computer verbunden wurde wird Smart Switch gestartet. Das Smartphone wird von der Software automatisch erkannt. Um eine Sicherung aller Elemente zu starten, klickt man auf Sicherungskopie. Falls nur bestimmte Gerätedaten gesichert werden sollen, erfolgt dies über die Einstellungen und den Reiter Gesicherte Elemente. Durch das Anklicken einzelner Elemente lassen sich diese gezielt an- und abwählen. Die Datensicherung dient als Quelle für die Wiederherstellung des Smartphones und für die Übertragung der Daten auf ein anderes bzw. neues Samsung-Smartphone.

Alternativ lassen sich Daten direkt von einem Smartphone auf ein anderes mit der Samsung Smart Switch App übertragen. Hier kann zuerst ausgewählt werden, von welchem Handy die Daten übertragen werden und welches die Daten empfängt. Anschließend wird eine Verbindung zwischen dem neuen und dem alten Gerät hergestellt. Dies geschieht kabellos oder per USB-Kabel. Als Nächstes kann man entscheiden, welche Daten übertragen werden sollen. Auf dem Smartphone, welches die Daten übertragt, werden die Daten mit dem Tippen auf “Senden” übertragen. Das Gerät, das die Daten empfängt, muss den Empfang mit dem Tippen auf “Empfangen” bestätigen. Nachdem die Übertragung abgeschlossen wurde kann die Anwendung geschlossen werden und das neue Gerät weiter eingerichtet werden.

Tipp: Datenübertragung, SMS am PC schreiben und Outlook-Synchronisation – die Freeware MyPhoneExplorer eignet sich für Android-Smartphones und fast alle Sony-Ericson-Handys.

Anmerkung der Redaktion: Über den u.g. Link kann die Anwendung heruntergeladen werden.

Quelle: https://www.pcwelt.de/article/1191592/samsung-smart-switch.html?utm_date=20230829124502&utm_campaign=Security&utm_content=Title%3A%20Samsung%20Smart%20Switch&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

3) Feature – Whatsapp-Anrufe vs. normale Anrufe: Was ist besser?

Anrufe über Whatsapp haben viele Vorteile. Aber sind sie den klassischen Anrufen wirklich überlegen? Hier ist die Antwort.

Für Auslandstelefonate ist Whatsapp meine erste Wahl. Warum? Weil Whatsapp-Anrufe über IP-Telefonie laufen, sprich Internet – und ich mich nicht darum sorgen muss, ob ich im nächsten Monat mit horrenden Rechnungen von meinem Telefonanbieter überrascht werde. Viele würden sogar behaupten, dass Whatsapp-Anrufe generell besser und praktikabler sind

als klassische Anrufe. Aber ist das wirklich so? Finden wir es heraus.

Darum sollten Sie öfter über Whatsapp telefonieren

Der wichtigste Grund zuerst: **Whatsapp-Anrufe sind immer kostenlos,** sowohl im Inland als auch im Ausland. Ich zahle also keinen Cent, wenn ich mit einem Freund im australischen Dschungel telefoniere, und das ist schon ziemlich genial.

Davon abgesehen bietet Whatsapp einen **Datenschutzvorteil:** Anrufe über den Messenger sind nämlich Ende-zu-Ende-verschlüsselt und können nicht abgehört werden – normale Anrufe schon.

Besonders praktisch ist Whatsapp auch für **Prepaid-Karten-Nutzer,** denn hier zählt jede Minute. Bevor Sie also Ihr Guthaben für einen Anruf ausschöpfen, telefonieren Sie einfach über den Messenger.

Also haben klassische Anrufe ausgedient?

Nein, natürlich nicht. Internet-Telefonie mag zwar ihre Vorteile haben, doch gibt es auch einen großen Nachteil: In Regionen, in denen kein LTE-Netz verfügbar ist, bleiben Ihnen Whatsapp, Facebook Messenger und Co. leider verwehrt.

Ein normaler Anruf kann zwar auch über LTE/5G laufen, aber eben auch über GSM (also das klassische Mobilfunknetz). Deshalb sind Sie mit solchen Anrufen deutlich flexibler, zumindest bei Inlandsgesprächen.

Ein weiterer Grund, der für klassische Anrufe spricht: Bei einer Telefon-Flatrate können Sie so viel telefonieren, wie Sie möchten. Bei Whatsapp hingegen sind Sie immer auf Ihr monatliches Datenvolumen angewiesen. Ist dieses aufgebraucht, können Sie nur noch über WLAN telefonieren.
Tipp: Wenn Sie viel über Ihre mobilen Daten telefonieren, empfiehlt es sich, die Sparfunktion des Messengers zu aktivieren. Das reduziert zwar die Qualität der Anrufe, aber auch den Datenverbrauch. Zur groben Orientierung:

- Ein 10-minütiger Sprachanruf verbraucht circa 3 MB Datenvolumen (bzw. 1,7 MB mit Sparfunktion).
- Ein 10-minütiges Videotelefonat verbraucht bereits circa 47 MB Datenvolumen (bzw. 10 MB mit Sparfunktion).

Tipp: Noch mehr Whatsapp News & Beiträge gibt es hier:

- “Urlaubsmodus” bei Whatsapp einstellen – so geht’s
- Whatsapp-Nachrichten nachträglich bearbeiten
- 11 Tipps & Tricks für Whatsapp, die jeder kennen sollte

Quelle: https://www.pcwelt.de/article/2029750/whatsapp-anrufe-vs-normale-anrufe-was-ist-besser.html?utm_date=20230829125959&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Whatsapp-Anrufe%20vs.%20normale%20Anrufe%3A%20Was%20ist%20besser%3F&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

4) Apps – Drastischer Schritt: Diese Facebook-App wird im September eingestellt

Wer auf Facebook am Handy chatten will, hat die Wahl zwischen zwei Messengern. Einer von beiden wird jedoch bald abgeschaltet.

Wer Facebook auf dem Handy nutzt, hat auch die passende Messenger-App geladen. Dabei haben Nutzerinnen und Nutzer die Wahl zwischen der herkömmlichen Chat-Anwendung oder dem **Messenger Lite**. Diese abgespeckte Version wird jedoch im September abgeschaltet.

Messenger Lite: Jetzt muss der Umstieg stattfinden

Der Messenger Lite von Facebook ist vor allem auf älteren Android-Geräten oder weniger leistungsfähigen Smartphones installiert. Er stellt eine etwas weniger umfangreiche Version des herkömmlichen Facebook-Chats auf dem Handy dar. Auch Smartphones, bei denen regelmäßig der Speicher voll ist, profitieren vom Messenger Lite, da er auch weniger Speicherplatz einnimmt.

Doch beim Mutterkonzern ist man wohl der Auffassung, dass der Messenger Lite nicht mehr zeitgemäß sei, weiß TechCrunch. Öffnen Nutzerinnen und Nutzer jetzt die App, bekommen sie eine Meldung angezeigt, in der die zur Nutzung des herkömmlichen Facebook-Messengers aufgefordert werden. Spätestens bis zum 18. September sollte der Wechsel vollzogen sein, da an diesem Tag die abgespeckte Version in den Ruhestand geschickt wird – und das obwohl sie über etliche Millionen Downloads verfügt.

So gelingt der Umstieg kinderleicht

Seit dem 21. August soll eine automatische Weiterleitung zum Standard-Messenger von Facebook aktiv sein. Für die Userschaft macht man damit den Umstieg so einfach wie nur irgend möglich. Du musst lediglich den herkömmlichen Messenger laden und dich gegebenenfalls mit deinen Facebook-Logindaten in der App anmelden. All deine Chats und Nachrichten wurden automatisch übernommen.

Sollte dein Handy nicht darauf ausgelegt sein, solltest du über ein neues Smartphone nachdenken. Nicht unterstützte Geräte sind in der Regel so alt, dass sie auch keine Android-Updates mehr erhalten. Bedenke, dass du sich mit einem veralteten Handy gläsern für Hackerinnen und Hacker machst. Günstige Handys findest du vielerlei in passenden Angeboten. Ist das keine Option für dich, kannst du auch einen Trick ausprobieren, um den Facebook Messenger zu umgehen.

Quelle: https://www.futurezone.de/digital-life/apps/article484243/drastischer-schritt-diese-facebook-app-wird-im-september-eingestellt.html?utm_source=browser&utm_medium=push-notification&utm_campaign=cleverpush&utm_term=autofeed

5) How-To – So reinigen Sie Ihre Airpods – und warum Sie das tun sollten

Schmutz auf dem Bügel oder den Polstern der Airpods Max oder Ohrenschmalz an den Airpods (Pro) - das ist zu tun.

Sie kämen sicher kaum auf die Idee, Airpods (Pro) in Ihre Ohren zu stecken, die zuvor in anderen Ohren waren und vorher nicht gereinigt wurden. Doch es ist auch sinnvoll, die eigenen Airpods, die man nie verleiht, regelmäßig zu reinigen.

Den Grund erklärt die HNO-Ärztin Dr. Veronika Wolter im Interview mit unseren Kollegen der MacLife (Ausgabe 9/23): In-Ear-Kopfhörer hätten ein **“enormes Potenzial für Verunreinigungen und sogar Entzündungen”**.

Beim Herausnehmen der Ohrhörer klebt an ihnen immer Ohrenschmalz und “legen Sie die Kopfhörer irgendwo ab, verschmutzen sie zusätzlich und externe Keime siedeln sich an. Desinfizieren Sie die Geräte daraufhin nicht, stecken Sie sich die dieselben Kopfhörer komplett mit allen Keimen wieder ins Ohr und erschaffen damit einen idealen Nährboden für

Bakterien.”

Da In-Ear-Kopfhörer, insbesondere solche mit ANC wie die Airpods Pro den Gehörgang auch noch gut abschließen, züchte man darin ganze Bakterienkolonien heran.

Das muss nicht sein, In-Ear-Hörer lassen sich leicht reinigen. Apple erklärt ausführlich, wie. Wasser darf dabei nur sehr zurückhaltend ins Spiel kommen. Die äußeren Oberflächen der Kopfhörer kann man auch mit einem mit Isopropylalkohol (70 Prozent) oder Ethylalkohol (75 Prozent) befeuchteten Tuch abwischen – **aber nie die Lautsprechergitter!**

Airpods (Pro) richtig reinigen

- Verwenden Sie ein weiches, trockenes und fusselfreies Tuch, reinigen Sie niemals unter fließendem Wasser.
- Sollten die Airpods (Pro) mit bestimmten Substanzen wie Sonnenmilch oder säurehaltigen Lebensmittel in Kontakt geraten sein, könnten sie fleckig geworden sein. Diese Flecken können Sie mit einem leicht angefeuchteten Tuch wegwischen, dann trocknen Sie die Airpods mit einem fusselfreien, trockenen Tuch und lassen sie noch eine Weile an der Luft trocken, ehe Sie sie zurück in das Ladecase legen.
- Achten Sie darauf, dass keine Flüssigkeit in die Öffnungen eindringt.
- Mikrofon- und Lautsprechergitter können Sie mit einem trockenen Wattestäbchen reinigen
- Das Ladecase können Sie ebenso mit einem trockenen, fusselfreien und weichen Tuch reinigen, etwaige Verunreinigungen in der Lightning-Buchse entfernen Sie mit einem Pinsel mit weichen Borsten.
- Die Ohreinsätze der Airpods Pro können Sie indes abnehmen und mit Wasser abspülen. Danach wie gehabt mit einem trockenen, weichen und fusselfreien Tuch abtrocknen und erst völlig getrocknete Ohreinsätze wieder auf die Airpods Pro setzen.

Airpods Max richtig reinigen

- Auch hier gelten die Grundregeln: Nicht unter fließendem Wasser reinigen, keine Feuchtigkeit in Öffnungen bekommen, ein weiches und fusselfreies Tuch verwenden.
- Die Ohrpolster sind indes abnehmbar und lassen sich mit einem in Seifenlauge getauchten und leicht ausgewrungenem Tuch reinigen. Auf 250 ml Wasser sollte etwa ein Teelöffel (5 ml) Seifenlauge kommen.
- Auch der Kopfbügel lässt sich mit Seifenlauge reinigen, man sollte die Airpods Max aber dabei umgedreht halten, damit kein Wasser in die Befestigung des Bügels rinnt.
- Danach Ohrpolster und Bügel mit einem trockenen, weichen und fusselfreien Tuch abtrocknen
- Ohrpolster und Airpods Max einen Tag flach zum Trockenen an der Luft auslegen, ehe man sie wieder zusammenfügt
- Das Case der Airpods Max kann man bei Bedarf mit Isoporpylalkohol anfeuchten, ehe man es mit einem Tuch säubert.

Quelle: https://www.macwelt.de/article/2028028/airpods-reinigen.html?utm_date=20230829131601&utm_campaign=Macwelt%20Daily&utm_content=Title%3A%20So%20reinigen%20Sie%20Ihre%20Airpods%20%E2%80%93%20und%20warum%20Sie%20das%20tun%20sollten&utm_term=Macwelt%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

6) Ratgeber Webbrowser – Cookies löschen in Chrome – so klappt es auf dem PC und Mobilgeräten

Sie haben in Google Chrome Probleme mit einer Web-App und wollen nun Ihre Cookies löschen? Wir zeigen Ihnen, wie das in nur drei Schritten gelingt.

Cookies sind für Webentwickler ein wichtiges Werkzeug, um temporär Daten im lokalen Speicher der Endgeräte der Benutzer abzulegen. Das führt mitunter dazu, dass Sie sich nicht bei jedem Seitenbesuch wiederholt neu einloggen müssen.

Aber: Wenn eine Webanwendung in Google Chrome nicht ordnungsgemäß funktioniert, kann es helfen, die Cookies zu löschen. Hier erfahren Sie, wie das im Handumdrehen gelingt.

So löschen Sie Ihre Cookies in Chrome auf einem PC oder Mac

Wenn Sie auf einem PC mit Windows 10, 11 oder einem Mac in Google Chrome die Cookies löschen möchten, folgen Sie diesen drei Schritten:

1. Öffnen Sie zunächst das Hauptmenü des Google-Browsers und navigieren Sie zu „Weitere Tools > Browserdaten löschen“. Daraufhin erscheint in Chrome ein kleines Fenster, das sich alternativ auch direkt mit dem Shortcut „Strg + Umschalt + Entf“ öffnen lässt und dass es Ihnen unter anderem erlaubt, ihre Cookies zu löschen.
2. Im oberen Bereich des Fensters sehen Sie den „Zeitraum“, auf den sich der Löschvorgang auswirkt. Wählen Sie „Gesamte Zeit“, um ausnahmslos alle Cookies zu entfernen.
3. Selektieren Sie darunter mindestens die Option „Cookies und andere Websitedaten“ und bestätigen Sie abschließend mit „Daten löschen“.

So entfernen Sie die Cookies unter Android oder iOS

Auch auf einem iPhone, iPad oder einem beliebigen Android-Gerät sind nur drei einfache Schritte erforderlich, um in Google Chrome die Cookies zu löschen:

1. Navigieren Sie im Hauptmenü des Chrome-Browsers auf Ihrem Mobilgerät zu „Verlauf > Browserdaten löschen“.
2. Wählen Sie auch hier oben einen „Zeitraum" aus, wobei die Auswahl des Eintrags "Gesamte Zeit“ zur Entfernung aller Cookies führt. Setzen Sie unten mindestens den Haken neben „Cookies und Websitedaten“.
3. Bestätigen Sie je nach Gerät mit der Schaltfläche „Daten löschen" oder „Browserdaten löschen“.

Beachten Sie, dass viele Webseiten, auf denen Sie zuvor eingeloggt waren, nach diesem Vorgang erneut die Eingabe Ihrer Zugangsdaten anfordern. Das liegt daran, dass die jeweiligen Dienste in Cookies Informationen über den Login-Status Ihrer Benutzerkonten abgelegt haben.

Tipp: Tracking vorbeugen: Warum man Cookies regelmäßig löschen sollte

- Tipps für Ihren Webbrowser: Cookies unter Android löschen: So geht's
- Tipps für den Webbrowser: Firefox Cache löschen – so klappt's

Quelle: https://www.t-online.de/digital/internet/id_100209862/cookies-loeschen-in-chrome-so-klappt-es-auf-pc-und-handy.html

7) Mehr Power --Samsung-Handy schneller machen – mit nur einer Einstellung

Wenn Ihr Samsung-Smartphone ab und zu ruckelt, müssen Sie das nicht hinnehmen. Eine kleine Einstellung verhilft dem Handy zu mehr Schnelligkeit.

Samsung-Smartphones zählen zu den beliebtesten Handys und werden millionenfach gekauft. Doch nicht alle der Smartphones laufen immer einwandfrei. Mal sind es Ruckler, mal störende Verzögerungen, die die Freude am Handy mindern. Doch es gibt eine einfache Lösung, um die Leistung zu steigern – mit nur einer Änderung in den Einstellungen.

Mehr Tempo für Ihr Samsung-Smartphone

Die Erwartung an ein Samsung-Smartphone ist klar: Es soll flüssig und schnell funktionieren. Doch auch bei den leistungsstärksten Spitzenmodellen kommt es gelegentlich zu Beeinträchtigungen – trotz eigentlich ausreichender Leistung. Wenn Sie nicht auf ein Software-Update von Samsung warten möchten oder ein älteres Modell besitzen, das nicht mehr so zügig agiert, können Sie selbst Hand anlegen und die Leistung optimieren.

Samsung-Handys: Animationen machen zum Teil Probleme

Der Knackpunkt bei Samsung-Smartphones sind die Animationen. Solange die Software richtig funktioniert, reagiert das Handy schnell und reibungslos. Doch gelegentlich fangen die Animationen an zu ruckeln und die Funktionen kommen ins Stocken. Ein Beispiel ist das Galaxy A54. Trotz ausreichender Leistung wirkt das Smartphone aufgrund der ruckelnden Animationen beim Öffnen und Schließen von Apps sowie beim Wechseln zwischen Inhalten schwächer als es ist. Aber das Problem können Sie schnell beheben.

So schalten Sie die Animationen bei Samsung-Handys aus

Die Lösung ist simpel: Deaktivieren Sie einfach die Animationen. So können Sie die Leistung Ihres Samsung-Smartphones erhöhen, wenn Sie von ruckelnden Animationen gestört werden.

1. Öffnen Sie die Einstellungen.
2. Scrollen Sie nach unten zum Eintrag "Eingabehilfe".
3. Tippen Sie auf "Verbesserung der Sichtbarkeit".
4. Scrollen Sie nach unten zum Eintrag "Animationen entfernen" und aktivieren Sie den Schalter durch Schieben nach rechts.

Mit dieser Einstellung deaktivieren Sie alle Animationen auf Ihrem Samsung-Handy. Den Unterschied werden Sie sofort bemerken. Ob Sie zurücknavigieren, Apps schließen, die Kamera öffnen oder ein Foto machen – alles geschieht ohne Verzögerung. Die Leistung steigt spürbar, allerdings wird es Ihnen anfangs ungewohnt vorkommen, wenn zum Beispiel beim Auslösen der Kamera die Animation fehlt.

Tipp: Smartphone-Ratgeber: Android Bildschirmaufnahme: So geht's

- Anleitung: So blockieren Sie nervige Spam-Anrufe
- Praktisches Tool: So funktioniert die Android Zwischenablage

Quelle: https://www.t-online.de/digital/smartphone/id_100226148/samsung-handys-schneller-machen-mit-einer-einstellungsaenderung.html

8) So kompliziert ist der Widerspruch gegen neue WhatsApp-Datenschutzrichtlinie

WhatsApp benachrichtigt seine Nutzer zur Zeit über eine neue Datenschutzrichtlinie. Dabei werden personenbezogene Daten unter anderem auch für Direktmarketing erhoben. Wer deshalb von seinem Recht auf Widerspruch Gebrauch machen will, begibt sich auf eine Odyssee aus vielen Einzelschritten und abschreckenden Formulierungen.

Meta und das Thema Datenschutz teilen eine lange, konfliktreiche Geschichte. Über Facebook, WhatsApp und Instagram erhält der Mutterkonzern Zugriff auf eine große Menge Nutzerdaten, deren Umgang eigentlich DSGVO-konform ablaufen muss. Eigentlich. Weil es hier aber immer wieder Mängel gab, musste WhatsApp zuletzt seine Datenschutzrichtlinien überarbeiten. Dies geschah bereits am 17. Juli und seitdem werden die Nutzer schrittweise darüber Informiert. Wer WhatsApps neuen Richtlinien nicht zustimmen möchte, kann nun Widerspruch einlegen. Doch das gestaltet sich komplizierter als gedacht. TECHBOOK verrät, was bei dem Antrag auf Widerspruch zu beachten ist – und warum er sich trotzdem lohnt.

WhatsApp versus DSGVO

Die Datenschutzgrundverordnung (DSGV) ist Teil des EU-Rechts und regelt unter anderem den Umgang von Unternehmen mit den personenbezogenen Daten ihrer Nutzer. TECHBOOK hat bereits im Gespräch mit dem Medienrechtsexperten Christian Solmecke die neueste Anpassung von WhatsApps Datenschutzrichtlinie eingeordnet. Dabei hat Solmecke Bedenken an der aktuellen Richtlinie geäußert, da sie von den Nutzern einen aktiven Widerspruch (Opt-Out statt einer aktiven Erlaubnis (Opt-In) der Datenverarbeitung erfordert.

Konkret möchte WhatsApp mit den neuen Richtlinien die Erlaubnis der Nutzer einholen, um ihre Daten im Rahmen eines „berechtigten Interesses“ verwenden zu dürfen. Daraus ergeben sich zwei Tücken: Nutzer erteilen ihre Erlaubnis passiv, indem nichts tun. Das scheint erst mal bequem zu sein, hat aber zur Folge, dass viele Nutzer sich nicht bewusst sind, welche Rechte sie WhatsApp damit erteilen. Das andere Problem liegt in der schwammigen Formulierung „berechtigte Interessen“. In seinem Hilfebereich konkretisiert WhatsApp die Verwendungszwecke der personenbezogenen Daten folgendermaßen:

- Business Intelligence und Analytics.
- Das Speichern und Teilen von Informationen mit anderen, einschließlich Strafverfolgungsbehörden, und um auf rechtliche Anfragen zu reagieren.
- Das Speichern und Teilen von Informationen, wenn wir juristischen Rat suchen oder uns selbst im Kontext von Gerichtsverfahren oder anderen Streitigkeiten schützen müssen.
- Zur Förderung von Sicherheit und Integrität außerhalb der Erfüllung unseres Vertrags mir dir.
- Zur Verbesserung des WhatsApp Customer Supports.
- Zur Verbesserung des WhatsApp Services durch die Entwicklung neuer Funktionen oder die Aktualisierung vorhandener Funktionen.

Das klingt zunächst nicht weiter ungewöhnlich. Doch etwas versteckt in einem Absatz unter diesem Listicle steht nun der eigentlich interessante Teil: „Du hast außerdem jederzeit die Möglichkeit, der Verarbeitung deiner personenbezogenen Daten zu widersprechen, die mit dem Zweck des Direktmarketings erfolgt – und zwar unabhängig von der der Verarbeitung zugrunde liegenden Rechtsgrundlage.“ Wer diesem Aspekt nicht widerspricht, dessen Daten sammelt Meta, um personalisierte Werbung schalten zu können.

Opt-Out-Methode bei Datenverarbeitung nicht rechtens

Solmecke verweist gegenüber TECHBOOK auf ein Urteil des Europäischen Gerichtshof (EuGH) vom 04. Juli 2023, das „die Personalisierung der Werbung nicht als berechtigtes Interesse [für] die Datenverarbeitung“ anerkennt. (Az. C-252/21). „Stattdessen wird Meta eine freiwillige und aktive Einwilligung seiner Nutzer einholen müssen“, meint der Medienrechtsexperte. Es ist daher wahrscheinlich nur eine Frage der Zeit, bis WhatsApp seine aktuelle Datenschutzrichtlinie erneut an die DSGVO anpassen muss. Bis dahin aber können Nutzer Widerspruch gegen die Richtlinie einlegen.

Der lange Weg zum Widerspruch

Um WhatsApps Datenschutzrichtlinie zu widersprechen, muss man entweder auf den Benachrichtigungsbanner klicken oder die FAQ-Website von WhatsApp aufrufen. Von hier aus gelangt man zu einem Formular – nachdem man die obligatorischen Cookies erlaubt oder verboten hat. Hier kann man nun aus verschiedenen Optionen auswählen, unter anderem: „Wie kann ich meine Informationen löschen?“ oder eben „Wie kann ich der Verarbeitung meiner Informationen widersprechen?“

Klickt man letzteres an, öffnet sich ein Reiter, in dem erneut die verschiedenen Bereiche der Datenverarbeitung aufgeführt sind. Und auch hier steht der problematische Aspekt – die Datenverarbeitung für personalisierte Werbung – versteckt und separiert von den anderen Aufzählungen.

Bevor man nun final auf „Ich möchte Widerspruch einlegen“ klickt, versucht WhatsApp, einen erneut auf die ursprüngliche FAQ-Seite umzuleiten. Hier kann man sich nochmal über die einzelnen Schritte zum Widerspruch informieren. Außerdem kündigt WhatsApp an dieser Stelle an, dass man genau angeben soll, gegen welche Datenverarbeitung man Widerspruch einlegt. Laut eigenen Angaben kann WhatsApp den Widerspruch nämlich immer dann ablehnen, wenn er sich nicht auf das Direktmarketing bezieht, sondern auf einen der anderen genannten Aspekte.

Darüber hinaus soll man laut Leitfaden seinen Widerspruch auch noch begründen und erklären, „wie sich die Verarbeitung auf dich auswirkt (welche Rechte und Freiheiten deiner Meinung nach durch die Verarbeitung beeinträchtigt werden und warum).“ WhatsApp hat sich also große Mühe gegeben, die Instruktionen so aufwendig und abschreckend wie möglich zu gestalten. Wer nämlich Widerspruch gegen die Datenverarbeitung zur Direktwerbung einlegen, muss diesen nach Art. 21 Abs. 2 DSGVO gar nicht begründen.

Nicht abschrecken lassen

Klickt man nun endlich auf „Ich möchte Widerspruch einlegen“, muss man in einem Formular eine E-Mail-Adresse und die Handynummer des WhatsApp-Accounts angeben. Anschließend erhält man eine E-Mail, mit der gleichen Aufforderung wie schon auf der Website: Man solle angeben, welcher Datenverarbeitung man widersprechen möchte und den Widerspruch begründen. Theoretisch sollte der Widerspruch gegen die Datenverarbeitung zum Direktmarketing ohne Begründung möglich sein. Wer bei der Formulierung auf Nummer sicher gehen will, kann sich am Musterbrief der Verbraucherschutzzentrale orientieren.

Ist die E-Mail abgesendet, heißt es warten. WhatsApp prüft im nächsten Schritt den eingelegten Widerspruch, behält sich aber vor, die Prüfung zu unterlassen, wenn der Nutzer „keine ausreichenden Informationen“ vorgelegt hat. Auch von dieser Formulierung sollte man sich nicht abschrecken lassen. Wird dem Widerspruch gegen die Datenverarbeitung zum Direktmarketing stattgegeben, beendet WhatsApp die Datenverarbeitung.

Quelle: https://www.techbook.de/mobile-lifestyle/apps/whatsapp-widerspruch-datenschutzrichtlinie

9) Neue Funktion – WhatsApp verschickt Fotos jetzt in HD-Qualität

Wer Fotos und Videos auf WhatsApp verschickt, liefert den Freunden bisher überschaubare Qualität. Eine neue Funktion macht nun Schluss damit.

Auf dem eigenen Smartphone glänzen sie scharf und brillant, doch teilt man Fotos und Videos per WhatsApp mit seinen Kontakten, lässt die Qualität eher zu wünschen übrig. Doch

das ändert sich gerade. Ab sofort kann der Messenger zumindest Fotos auch in hoher Auflösung verschicken – und das weiterhin mit Ende-zu-Ende-Verschlüsselung.

Um die neue HD-Funktion nutzen zu können, müssen Sie allerdings selbst aktiv werden. Voreingestellt ist weiterhin die "Standardqualität", wie aus einer offiziellen Erklärung der WhatsApp-Mutterfirma Meta hervorgeht. Möchten Sie zur HD-Qualität wechseln, gehen Sie wie folgt vor:

- Öffnen Sie den Chat, in dem Sie das Foto teilen möchten.
- Tippen Sie auf das Kamera-Symbol im Chat-Eingabefeld.
- Wählen Sie wie gewohnt das gewünschte Foto aus.
- Tippen Sie im oberen Bereich auf das neue HD-Symbol.
- Bestätigen Sie, dass Sie das Bild in HD-Qualität verschicken wollen.

Neue WhatsApp-Funktion: Update nötig

Die Funktion ist derzeit noch nicht für alle WhatsApp-Nutzer verfügbar. Sie wird im Laufe der kommenden Wochen flächendeckend ausgerollt. Um darauf zugreifen zu können, benötigen Sie ein Update der App. Zudem kündigte Meta an, bald auch HD-Videos möglich zu machen.

HD entspricht bei WhatsApp einer Bildgröße zwischen 9 und 16 Megapixeln, was in etwa einer 4K-Auflösung entspricht. Das ist zwar eine deutliche Verbesserung, bedeutet aber nicht, dass Sie Fotos in Originalqualität verschicken können, wie es etwa WhatsApp-Konkurrent Signal anbietet.

HD-Qualität erhöht das Datenvolumen

Nutzer müssen sich zudem auf eine weitere Einschränkung einstellen: Ist die Internetverbindung des Empfängers schwach, zeigt WhatsApp die HD-Bilder zunächst weiter in Standardqualität. Der Kontakt muss dann aktiv die bessere Qualität auswählen, um sie in höherer Auflösung sehen zu können.

Dass WhatsApp bisher automatisch die Bildqualität beim Senden herabsetzt, hat einen durchaus nützlichen Hintergedanken. So werden weniger Daten übertragen, die Ihren Handyspeicher oder Ihr Mobilfunk-Konto belasten.

Quelle: https://www.t-online.de/digital/whatsapp/id_100227780/whatsapp-fotos-endlich-in-hd-qualitaet-versenden-neue-funktion.html

10) Merkwürdige Spam-Anrufe: Deshalb bleibt es am Hörer stumm

Auf dem Telefon-Display prangt eine unbekannte Nummer. Doch sobald man rangeht, meldet sich niemand zu Wort. Was hinter diesen Anrufen steckt, verraten wir hier.

Spam-Anrufe kennt sicher jeder. Ob es sich um hartnäckige Werbung handelt oder man dich das fünfte Mal zur selben Umfrage überreden will – Fakt ist: es nervt. Es kann jedoch auch sein, dass dich eine unbekannte Nummer kontaktiert und dann gar nichts passiert. Was dahinter steckt und wie du diese Anrufe los wirst, verraten wir jetzt.

Spam-Anrufe: Das passiert, wenn „030/ 499 189 …“ anruft

Besonders kuriose Spam-Anrufe vermeldet man gerade unter drei Berliner Nummern. Bei 030/499 189 778, 030/499 189 771 und 030/499 189 770 handelt es sich um ein und dasselbe Callcenter. Daher weichen auch nur die letzten drei Ziffern ab. Der vordere Teil, also 030/499 189 ist die sogenannte Rufnummerngasse, die mit dem Center verknüpft ist.

Doch obwohl es dort vor Mitarbeitenden wimmeln muss, kommt es durchaus vor, dass am Telefon erst einmal gar nichts passiert. Auch auf Nachfragen hin meldet sich niemand auf der anderen Seite. Meldet sich die Nummer ein zweites Mal einige Zeit später, hat man plötzlich einen Mitarbeiter oder eine Mitarbeiterin am Telefon. Selbes passiert beim Rückruf.

Erster Anruf dient als Ping

Doch was steckt hinter diesem ersten, ominösen Kontaktversuch, der sich durch durchgängiges Schweigen auszeichnet? Hierbei handelt es sich um einen Ping-Anruf. Das bedeutet, dass ein Wählcomputer unzählige Rufnummer durchprobiert und anklingelt. Damit will man lediglich in Erfahrung bringen, ob die Handynummer überhaupt vergeben ist. Da am anderen Ende der Leitung jedoch niemand sitzt, sondern nur ein PC die Rufnummern durchprobiert, meldet sich auch keiner, falls du rangehen solltest.

Doch das Klingeln alleine reicht, damit deine Telefonnummer auf der Liste des Callcenters landet. Später wird also ein Mitarbeiter oder eine Mitarbeiterin dich kontaktieren, um eine Umfrage mit dir durchzuführen. Laut giga.de sind die Personen höflich und bedrängen dich nicht, wenn du kein Interesse hast.

Mit diesem Trick wirst du die Anrufe los

Jedoch kann das Cellcenter schnell zu Spam-Anrufen bei dir führen, falls die Auftraggeber und damit die Umfragethemen wechseln. In diesem Fall kannst du dich jedoch einer simplen Methode bedienen.

Hinter den Spam-Anrufen steckt die Info GmbH, die wiederum im Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. als Mitglied gemeldet ist. Mit der Mitgliedschaft gehen auch strenge Verhaltensregeln einher. Wenn du also von „030/499 189 …“ kontaktiert wirst, kannst du jederzeit den Wunsch äußern, dass deine Rufnummer für künftige Umfragen gesperrt wird. Alternativ kannst du eine Email mit deinem Anliegen an kontakt@infogmbh.de senden. Zu guter Letzt hast du die Option die Rufnummerngasse oder die einzelnen Nummern zu blockieren.

Quelle: https://www.futurezone.de/digital-life/article479134/merkwuerdige-spam-anrufe-deshalb-bleibt-es-am-hoerer-stumm.html

11) Mit diesem Trick findet niemand mehr Ihr WLAN

Trotz aller Sicherheitsvorkehrung gelingt es immer wieder, dass sich Unbefugte Zugriff auf den heimischen Router und somit das Netzwerk verschaffen. Das wird aber schwieriger, wenn das eigene WLAN-Netzwerk quasi unsichtbar für Außenstehende ist. Um das zu erreichen, hilft eine einfache Einstellung.

In der Regel sind Router von Haus aus bereits gut abgesichert. Wer sich aber etwas mit dem Menü seines Gerätes beschäftigt, wird die ein oder andere Einstellung entdecken, die durchaus hilfreich sein kann. Denn fernab der Werkseinstellungen bieten die meisten Router allerlei Funktionen um den Schutz vor Datenverlust und kostspielige Telefongespräche zu erhöhen oder Maßnahmen gegen Hacker und Malware einzurichten. Wer sein WLAN zum Beispiel vor unberechtigtem Zugriff schützen möchte, kann es ganz einfach unsichtbar machen. TECHBOOK erklärt in wenigen Schritten, wie das bei der Fritzbox oder aber den Speedport-Routern der Telekom funktioniert.

WLAN auf der Fritzbox unsichtbar machen

Die Fritzbox von AVM ist für ihr übersichtliches Menü und die vielen Einstellungsmöglichkeiten für Nutzer bekannt. Dabei hält AVM die Hürden möglichst niedrigschwellig, damit sich auch diejenigen zurechtfinden, die technisch nicht so versiert

sind. Um das Menü der Fritzbox aufzurufen, müssen Nutzer in die Adresszeile ihres Internet-Browsers **fritz.box** oder wahlweise **192.168.178.1** eingeben. Dann öffnet sich die Anmeldemaske, auf der sie sich mit ihrem Nutzernamen und Passwort anmelden.

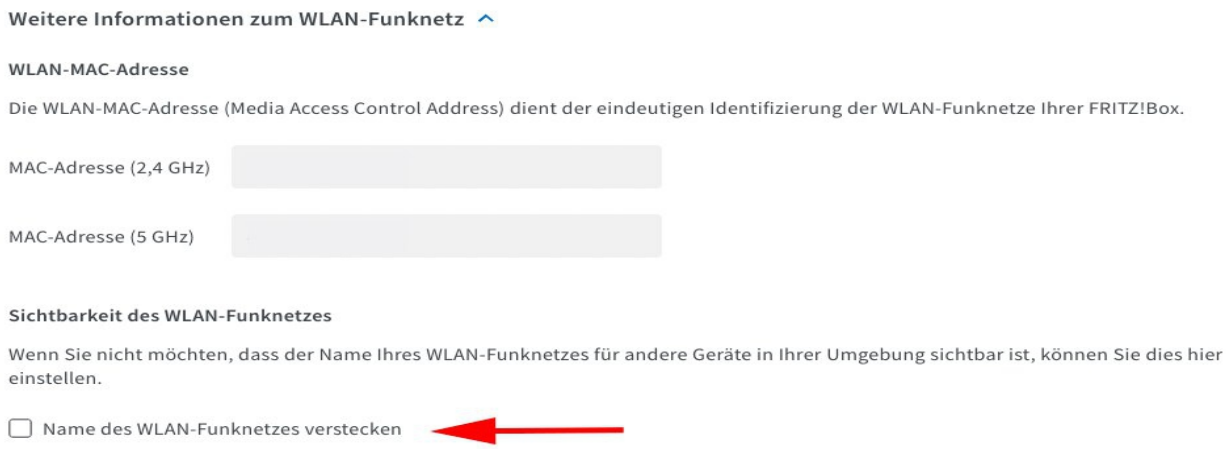
Schritt 1: WLAN-Einstellungen der Fritzbox öffnen

Die notwendigen Einstellungen, um das WLAN auf der Fritzbox unsichtbar zu machen, finden sich allesamt in der linken Menüleiste. Wer noch ein älteres Fritz!OS auf seinem Router installiert hat, muss dort unter Umständen zunächst die erweiterte Ansicht aktivieren. Läuft die Fritzbox allerdings mit einer aktuellen Firmware wie dem Fritz!OS 7.50 oder höher, entfällt dieser Schritt.

In diesem Fall können Nutzer direkt auf den Menüpunkt „WLAN“ und anschließend auf „Funknetz“ klicken.

Schritt 2: WLAN-Sichtbarkeit deaktivieren

Innerhalb der WLAN-Einstellungen der Fritzbox muss man nun herunterscrollen, bis fast ans Ende der Ansicht. Hier findet sich ein eingeklapptes Feld mit der Bezeichnung „Weitere Informationen zum WLAN-Funknetz“. Mit einem klappt sich dieses aus und Nutzer finden weitere Angaben und Einstellungsmöglichkeiten. Dazu gehört auch der letzte Punkt „Name des WLAN-Funknetzes verstecken“. Setzt man hier ein Häkchen, wird das Netzwerk nach Außen nicht mehr angezeigt.



Quelle: Um das WLAN auf der Fritzbox zu verstecken, muss man in diesem Feld ein Häkchen setzen. Foto: TECHBOOK

Nutzer sollten beachten, dass sie bei Aktivierung der Einstellung selbst das dann unsichtbare WLAN ihrer Fritzbox auch nicht mehr in der Liste der verfügbaren Netzwerke finden. Das ist kein Problem, soweit Geräte bereits im Heimnetz eingebunden sind und die Verbindung abgespeichert ist. Möchte man jedoch neue Geräte ins Netzwerk aufnehmen, muss die Unsichtbar-Einstellung kurzzeitig deaktiviert werden.

Auch bei Speedport-Routern lässt sich das WLAN unsichtbar machen

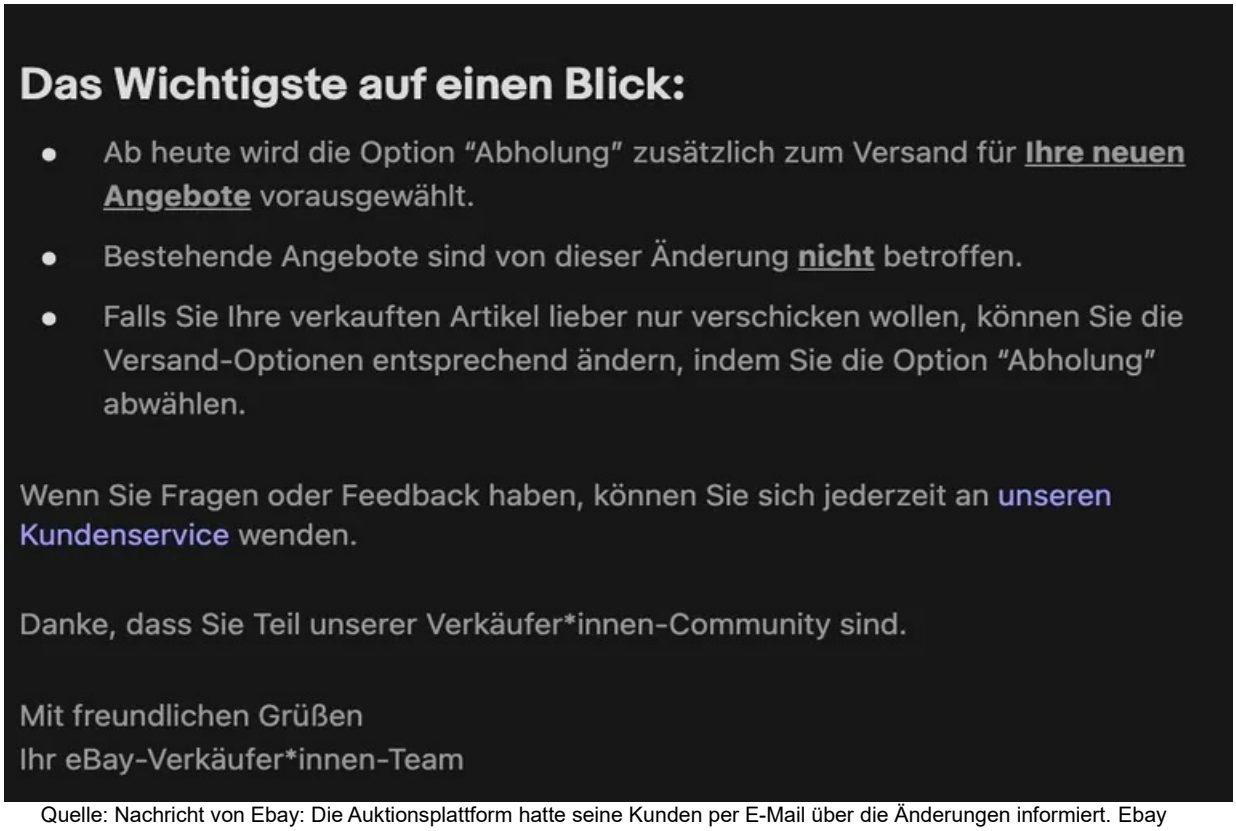
Dieser Tipp lässt sich im Übrigen auch auf vielen Speedport-Routern der Telekom anwenden. Dazu wählt man in der Übersicht den Menüpunkt „Konfiguration“ und dann „Sicherheit“ aus. Im Anschluss müssen Nutzer auf der nun geöffneten Sicherheitsseite zur Kategorie „WLAN Sicherheitseinstellungen“ navigieren. Hier klicken sie dann auf „SSID & Verschlüsselung“.

Es öffnet sich eine Setup-Seite, auf der sich neben anderen Optionen wie zum Beispiel „Netzwerkname (SSID)“, „Verschlüsselung und Kennwort zur Verschlüsselung“ auch der Punkt „Netzwerkname“ befindet. Hier interessiert die Einstellung direkt darunter: „SSID unsichtbar“. Wird sie mit einem Häkchen aktiviert, ist das WLAN künftig unsichtbar.

Quelle: https://www.techbook.de/connectivity/wlan-fritzbox-unsichtbar-machen

12) Versandkosten sparen – Ebay bietet neue Funktion für Verkäufer an

Ebay hatte kürzlich die Gebühren für Privatverkäufe gestrichen. Jetzt gibt es eine weitere Neuerung, die privaten Verkäufern mehr Reichweite bringen soll.
Ebay will Privatverkäufe weiter ankurbeln und setzt deshalb stärker auf das persönliche Abholen der Waren vor Ort. Beim Erstellen neuer Angebote von privat wird ab sofort die Option Abholung zusätzlich zur Option Versand vorausgewählt sein, teilt das Unternehmen mit. Bestehende Angebote seien nicht betroffen.



Quelle: Nachricht von Ebay: Die Auktionsplattform hatte seine Kunden per E-Mail über die Änderungen informiert. Ebay

Durch die Neuerung sollen demnach mehr potenzielle Käuferinnen und Käufer erreicht sowie Versandaufwand und -kosten gespart werden. "Sollten Sie einen Artikel lieber versenden wollen, können Sie in den Versandoptionen nach wie vor eine Versandmethode angeben und 'Abholung' abwählen", heißt es weiter.

In Konkurrenz zur Kleinanzeige

Ziel der Neuerung sei es zudem, das "Handeln in der Nachbarschaft zu erleichtern", heißt es weiter. Damit tritt der Online-Marktplatz stärker in Konkurrenz zur klassischen Kleinanzeige, bei der das persönliche Abholen der Ware vor Ort beim Verkäufer die Regel und ein Versand die Ausnahme ist.

Seine eigene Kleinanzeigensparte "Ebay-Kleinanzeigen.de" hat das Unternehmen im Sommer 2020 an den norwegischen Portalbetreiber Adevinta verkauft. Dieser hat den Ebay-Namensteil erst Mitte Mai endgültig gestrichen und tritt seither mit neuem Logo als "Kleinanzeigen" oder "Kleinanzeigen.de" auf.

Im vergangenen Februar hat Ebay die Gebühren für das Verkaufen und Einstellen von Artikeln für private Anzeigen gestrichen. Vorher hatten Verkäufer rund elf Prozent ihrer Erlöse als Provision an Ebay abtreten müssen. Dazu kamen 35 Cent als Einstellgebühr.

Erlöse waren gesunken

Mit der Geschäftsentwicklung insgesamt konnte die Ebay-Führung damals nicht zufrieden sein. Im Februar berichtete die Handelsplattform für das vorangegangene Quartal schwache Zahlen.

Die Erlöse im Jahresvergleich waren um vier Prozent auf 2,5 Milliarden Dollar (2,4 Mrd. Euro) gesunken. Der bereinigte Gewinn aus dem fortgeführten Geschäft fiel um zehn Prozent auf 581 Millionen US-Dollar.

Im vergangenen Quartal konnten die Gewinnerwartungen zwar wieder übertroffen werden, aber die Umsatzprognose wurde verfehlt.

Quelle: https://www.t-online.de/digital/aktuelles/id_100233700/ebay-bietet-neue-funktion-fuer-verkaeufer-an-versandkosten-sparen.html

Allgemeines:

1) Aktuelle Rückrufe: Verdacht auf Kunststofffremdkörper in Gut&Günstig-Salami

So sorgfältig die Herstellung und Verarbeitung von Lebensmitteln und Produkten auch überwacht wird, manchmal kommt es dennoch zu Fehlern oder Verunreinigungen. Im Normalfall können betroffene Artikel im Markt auch ohne Kassenbon zurückgegeben werden, der Kaufbetrag wird erstattet oder das Produkt ersetzt. Aktuelle Rückrufe: Rückruf von Käse bei Kaufland und Lidl, Aldi-Gewürz kann Glasfremdkörper enthalten.

Gut&Günstig-Salami: Verdacht auf Kunststofffremdkörper

Update vom 29. August: Verbraucherinnen und Verbrauchern wird dringend vom Verzehr einer Salami der Marke GUT&GÜNSTIG abgeraten. Der Hersteller The Family Butchers Germany GmbH kann nicht ausschließen, dass in Produkten mit einem bestimmten Mindesthaltbarkeitsdatum blaue Kunststofffremdkörper enthalten sind.

Durch diese kann es beim Verzehr zu ernsthaften Verletzungen im Mund- und Rachenraum sowie zu inneren Verletzungen oder Blutungen kommen. Erhältlich ist die Salami bei Edeka und Marktkauf. Betroffene Kundinnen und Kunden können das Produkt auch ohne die Vorlage eines Kassenzettels in den Märkten zurückgeben und bekommen den Kaufpreis erstattet.

Folgendes Produkt ist betroffen:

- **Das Produkt**: GUT&GÜNSTIG Hauchfeine Delikatess Salami geräuchert, 200-g-Packung
- **Mindesthaltbarkeitsdaten:** 10.09.2023, 11.09.2023 und 12.09.2023 (mak)

Bertolli Pesto enthält Senf: Gefahr für Allergiker

Update vom 24. August: Die bekannte Pesto-Marke Bertolli ruft ihr Pesto Calabrese zurück. Das Produkt enthält Senf, ist aber nicht entsprechend gekennzeichnet. Für Personen mit einer Senf-Allergie kann das gefährlich werden. Kundinnen und Kunden können die betroffene Charge auch ohne Vorlage des Kassenbons im Laden zurückgeben und erhalten den vollen Kaufpreis zurück. Das Pesto ist bei Rewe, Edeka, Real, Marktkauf, Metro, Penny und eventuell weiteren Supermärkten erhältlich.

Betroffenes Produkt: Bertolli Pesto Calabrese 185G

- **Mindesthaltbarkeitsdatum:** 29.02.2024
- **Charge:** F043 oder LF043
- **EAN:** 8712247232978
- **betroffene Länder:** Bayern, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Schleswig-Holstein, Thüringen

Listerien-Verdacht in Käse bei Kaufland und Lidl

Up vom 16. August: Bei gleich zwei großen Supermärkten gibt es aktuell Rückrufe von Käse.

Die Käserei Studer ruft ihr gesamtes Sortiment an gereiftem Käse zurück. Grund dafür ist eine festgestellte Kontamination mit Listerien bei einer der Käsesorten. Das Schweizer Unternehmen kann nicht ausschließen, dass die Kontamination im Reifekeller auch auf die anderen Käsesorten übertragen wurde.

Die Produkte sind über diverse Händler und Handelsketten verfügbar, weshalb vor allem Urlauber und Reiserückkehrer ihren Käse auf eine mögliche Betroffenheit prüfen sollten. Studer-Käse ist aber auch in Deutschland bei Kaufland und online erhältlich.

Betroffene Käse-Sorten der Marke Studer sind:

- Alter Schweizer
- Bergjuwel
- Bio Alter Schweizer
- Bio Bodenseekäse
- Bio Der scharfe Maxx
- Bio Die zarte Klara
- Bio Familienkäse
- Bio Sternenkäse
- Bio Wellenkäse
- Bodenseekäse (konventionell)
- Der edle Maxx 365
- Der freche Maxx
- Der scharfe Maxx
- Die zarte Klara
- Familienkäse (konventionell)
- Füürtüfel
- Käsermeister
- Landchäs
- Le Baron
- Meister-Chäs
- Raclette carré
- Rahmkäse
- Rapsody
- Reibkäse
- Seemerzler
- Sternenkäse
- Wellenkäse mild
- Wellenkäse mittel
- Wellenkäse rezent
- Wilhelm-Tell

Käse-Rückruf auch bei Lidl

Auch bei Lidl gibt es aufgrund des Verdachts einer Listerien-Kontamination einen Rückruf von Käse. Der Lieferant Züger Käsevertrieb GmbH warnt vor dem Verzehr des Artikels "Milbona Seemerzler" in der 200g-Packung.

Folgendes Produkt ist betroffen:

- **Artikel:** Milbona Seemerzler Käse, 200g
- **Identitätskennzeichen:** CH 5417
- **Mindesthaltbarkeitsdaten:** alle bis einschließlich 10.10.2023
- **Betroffene Länder:** Bayern, Berlin und Brandenburg

In beiden Fällen können Verbraucher das Produkt ohne Vorlage eines Kassenzettels zurückgeben und erhalten den Verkaufspreis wieder.

Darum sind Listerien so gefährlich

Vor dem Verzehr von mit Listerien kontaminierten Produkten wird gewarnt, da das Bakterium zu Übelkeit, Erbrechen, Fieber oder Durchfall sowie grippeähnlichen Symptomen führen kann. Bei gesunden Personen verläuft eine Listeriose meist harmlos, Kleinkinder oder Menschen mit geschwächter Immunabwehr, wie frisch Operierte, Aids- oder Krebspatienten, sowie Diabetiker können hingegen erkranken.

Bis die Krankheit ausbricht, kann es bis zu acht Wochen dauern. Meist kann eine durch Listerien verursachte Sepsis (Blutvergiftung) oder Meningitis (Hirnhautentzündung) durch Antibiotika behandelt werden, eine Todesfolge ist jedoch nicht auszuschließen. Bei Schwangeren kann Listeriose zu einer Frühgeburt, schweren Schädigungen oder sogar zum Absterben des Fötus führen. (mak)

Aldi-Gewürz wegen möglicher Glasfremdkörper zurückgerufen

Update vom 7. August: Die BLM Produktions- und Vertriebsgesellschaft mbH & Co. KG ruft den Artikel "Le Gusto Bolognese Gewürz (35g)" zurück. Aus einer Mitteilung des Lebensmittel-Großhändlers geht hervor, dass in dem Produkt möglicherweise Glasfremdkörper enthalten sein können.

Das Gewürz wurde im Rahmen eines Aktionsangebotes bei Aldi Nord sowie Aldi Süd verkauft.

Dieses Produkt ist betroffen:

- **Produkt:** Le Gusto Bolognese Gewürz (35g)
- **Mindesthaltbarkeitsdatum (MHD):** 01.06.2025

Wer das Gewürz gekauft hat, kann es den Angaben zufolge auch ohne Kassenbon in seiner Filiale zurückgeben und bekommt den Kaufpreis erstattet. (ff/dpa)

Erhöhte Aflatoxin-Gehalte in dm-Reiswaffeln

Update vom 7. August: Die Drogeriemarktkette dm hat den Artikel "dmBio Himbeer-Reiswaffeln ab dem 8. Monat (35 g)" zurückgerufen und umgehend aus dem Verkauf genommen. Das geht aus einer Pressemitteilung hervor.

Einzelne Packungen können demnach erhöhte Aflatoxin-Gehalte aufweisen. Werden diese Stoffe über einen längeren Zeitraum aufgenommen, könnten sie die Gesundheit beeinträchtigen.

Folgendes Produkt ist betroffen:

- **Produkt:** dmBio Himbeer-Reiswaffeln ab dem 8. Monat (35 g)
- **Mindesthaltbarkeitsdatum (MHD):** 04.06.2024
- **Charge:** NL 157

Quelle: https://www.gmx.net/magazine/ratgeber/finanzen-verbraucher/aktuelle-rueckrufe-gutguenstig-salami-kunststofffremdkoerper-enthalten-37472242

Rückruf wegen Listerien – Räucherlachs von Gut&Günstig mit Bakterien belastet

Der Artikel "Gut&Günstig Norwegischer Stremel Lachs heiß geräuchert Natur" wird zurückgerufen. Verkauft wurde das Produkt vor allem von zwei Händlern.

Bei einer Qualitätskontrolle des Räucherlachses von Gut&Günstig wurde das Bakterium Listeria monocytogenes nachgewiesen. Die Norfisk GmbH ruft deshalb das Produkt zurück. Listerien können grippeähnliche Symptome auslösen, vom Verzehr des Produktes wird dringend abgeraten.

Informationen zum betroffenen Artikel

Betroffen ist konkret der Artikel "Gut&Günstig Norwegischer Stremel Lachs heiß geräuchert Natur" in der 125-g-Packung mit dem Verbrauchsdatum 02.09.2023, der Losnummer L34232531/20 und der Veterinärkontrollnummer PL 20031801 WE. Verkauft wurde der Räucherlachs vorwiegend bei Edeka und Marktkauf.

Wer ein vom Rückruf betroffenes Produkt erworben hat, kann dieses auch ohne den Kassenbeleg in der Filiale zurückgeben. Der Kaufpreis wird erstattet.

Quelle: https://www.t-online.de/leben/aktuelles/id_100233544/raeucherlachs-mit-bakterien-belastet-dringender-rueckruf.html

2) Auf Plastikstreifen achten – Polizei warnt vor raffinierter Einbruchsmasche

Die Polizei warnt vor einem Trick von Einbrechern. Ein unscheinbares Utensil verrät, dass Ihr Heim im Visier der Täter ist. Das sollten Sie wissen.

Um festzustellen, ob das Haus verwaist ist, klemmen Einbrecher an Eingangs- und Terrassentüren Plastikstreifen zwischen Türblatt und Rahmen. Die Plastikstreifen sind durchsichtig, unscheinbar und maximal vier Zentimeter lang. Immer wieder stoßen Ermittler an Tatorten auf die Kunststoffstücke.

Aber auch Zahnstocher oder gar Laub beziehungsweise Blätter können Zeichen dafür sein, dass Ihr Haus von Kriminellen beobachtet wird.

So funktioniert die Einbruchsmasche

Die Methode ist denkbar einfach: Die Einbrecher biegen die Kunststoffstreifen in U-Form und klemmen sie zwischen Haustür und Rahmen oder fixieren sie an Garagentoren und Terrassentüren. "Mit diesem Trick soll festgestellt werden, welche Häuser jetzt in der Urlaubszeit leer stehen", heißt es in einer Mitteilung des Polizeipräsidiums Rheinpfalz. Sind die Plastikstücke noch Tage später unverändert da, haben die Einbrecher freie Bahn.

Die Polizei Mühlheim berichtet von weiteren Methoden: So werden beispielsweise Blätter von Bäumen oder Zahnstocher in die Türzagen oder Fensterläden geklemmt. Wenn der derart angebrachte Gegenstand nach einigen Tagen unberührt geblieben ist, schließen die Kriminellen daraus, dass sich niemand im Haus befindet, und so können sie ihren Einbruch entsprechend unbehelligt verüben.

Die Polizei fordert Bürger zu besonderer Wachsamkeit auf. Wer solche Plastikstreifen an seinem Haus entdeckt, solle unverzüglich die nächste Polizeidienststelle informieren. Auch verdächtige Personen in der Nachbarschaft sollten Sie sofort über den Polizeiruf 110 melden.

Einbruchsschutz im Urlaub

Einbrecher achten auf alle Anzeichen dafür, ob sich die Bewohner einer Wohnung im Urlaub befinden. Dazu gehören auch die Fußmatten vor der Eingangstür. Oft legen die Reinigungsdienste in einem Mehrfamilienhaus die Matten beim Putzen des Treppenhauses zur Seite – und belassen sie auch so. Der Immobilienverband IVD in Berlin rät daher, diese vor einem Urlaub in die Wohnung zu räumen, um keinen Verdacht zu erregen. Alternativ kann auch der Wohnungssitter, der den Briefkasten regelmäßig leert, oder der Nachbar die Matten wieder in Position bringen.

Ein weiterer Trick sind Zeitschaltuhren. Diese können Sie beispielsweise für das Licht im Wohnzimmer und der Küche verwenden, um so eine mögliche Anwesenheit vorzutäuschen. Wenn möglich, sollten Sie Ihre elektrischen Fensterläden ebenfalls zeitsteuern.

Neben diesen kleinen Punkten sollten während Ihres Urlaubs auch Nachbarn, Freunde oder Verwandte regelmäßig nach dem Rechten sehen. Dabei sollten nicht nur die Rollläden bewegt und die Briefkästen geleert, sondern auch auf Plastikstreifen an Terrassentüren, Garagentoren und Haustüren geachtet und gegebenenfalls die Polizei verständigt werden. Die Polizei rät davon ab, auf frei zugänglichen öffentlichen Kanälen – zum Beispiel auf Facebook oder Instagram – Urlaubsbilder zu posten.

Haus und Wohnung einbruchsicher machen

Generell lohnt sich die Investition in mechanische Sicherheitstechnik. Die Kosten für wirksamen Einbruchsschutz sind überschaubar. In Einfamilienhäuser dringen die Täter meist durch ungesicherte Fenster oder Terrassentüren ein. Vor allem im Erdgeschoss sollten Sie daher Fenster und Terrassentüren einbruchsicher machen, indem Sie Pilzkopfzapfenbeschläge oder Aufschraubsicherungen nachrüsten lassen. Achten Sie bei der Nachrüstung auf eine Zertifizierung der Produkte nach DIN 18104.

Einbruchhemmende Fenster und Türen sind gemäß der DIN 1627 geprüft. Achten Sie auch auf die VdS-Zertifizierung. Die Kennzeichnung weist auf die Qualität und Zuverlässigkeit des Einbruchsschutzes bei dem jeweiligen Produkt hin. Je höher diese ist, desto besser schützt die Tür oder das Fenster vor einem Einbruch. Zusätzlich sollten die Fenster, damit sie einen ausreichenden Schutz liefern, von einem Fachmann eingebaut werden.

Im Mehrfamilienhaus dringen Einbrecher meist durch Erdgeschossfenster oder durch die Wohnungstür ein. Letztere lässt sich mit Türsicherungen effektiv sichern. Über gute Einbruchsschutzprodukte und qualifizierte Handwerker für die Montage berät die Kriminalprävention der örtlichen Polizeibehörde kostenlos und oft sogar vor Ort beim Verbraucher.

Lesetipp:

- Sicheres Zuhause: Einbruchschutz für Fenster und Türen im Test
- Einbrecher abschrecken: Diese Überwachungskameras sichern für Sie Haus und Garten
- Richtiges Verhalten laut Polizei: Was tun, wenn Einbrecher im Haus sind?

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

Quelle: https://www.t-online.de/heim-garten/bauen/einbruchschutz/id_74895066/einbruch-polizei-warnt-vor-uebler-masche-mit-plastikstreifen-an-der-tuer.html

3) Alkoholmessgerät im Angebot – als Oktoberfest-Party-Gag oder zur Selbstkontrolle

Meinen Sie, dass Sie nach ausgelassenem Feiern auf dem Oktoberfest am nächsten Morgen fahrtüchtig sind? Diese Frage müssen Sie sich in Zukunft nicht mehr stellen – dank des Alkoholtesters von ACE Instruments. Sichern Sie sich jetzt unser exklusives Angebot von 129 Euro (UVP 199 Euro) mit dem Gutscheincode "Chip23". Der Versand ist inklusive!

Praktisches Alkoholmessgerät für sicheres Feiern

Alkoholtestgeräte kennt man hauptsächlich aus Polizeikontrollen. Es gibt allerdings eine schnelle und einfache Lösung, wie Sie Ihre Blutalkoholkonzentration selbst bestimmen können – ohne erst von der Polizei angehalten werden zu müssen: den ACE X, das Atemalkoholmessgerät von ACE Instruments. Durch seinen elektrochemischen Premium-Sensor hat der Tester eine **erstklassige Messgenauigkeit und nur minimale Messabweichungen von höchstens ± 0,05 Promille.** Auch deshalb wurde der ACE X in einer umfangreichen Studie der TU Wien als Testsieger ausgezeichnet!
Greifen Sie jetzt zu und sichern sich den Alkoholtester ACE X von ACE Instruments zu unserem unschlagbaren Angebotspreis von 129 Euro! Mit dem **Gutscheincode "Chip23"** reduziert sich der Preis im Shop um 70 Euro.

Das Atemalkoholtestgerät von ACE Instruments im Detail:

- **Atemalkoholtester mit elektrochemischem Premium-Sensor für 129 Euro**
- Sie sparen 35 Prozent im Vergleich zur unverbindlichen Preisempfehlung von 199 Euro. Geben Sie einfach den **Gutscheincode "Chip23"** im Warenkorb ein.
- Hier geht's zum Angebot
- **Polizeigenaue Werte:** präzise Messungen mit einer Messtoleranz von maximal ± 0,05 Promille
- **Testsieger einer Studie der TU Wien: 99,1 Prozent Testgenauigkeit**
- Digitale Anzeige der Testergebnisse auf großem OLED-Display
- Integrierter Speicher für bis zu 100 Messergebnisse
- Einfache Bedienung
- Ideal für den privaten Einsatz dank handlicher Größe (128 x 60 x 24 Millimeter) und kompaktem Gewicht (130 Gramm, inklusive Batterien – im Lieferumfang enthalten)
- Lieferumfang: Alkoholtester, 6 hygienisch einzeln verpackte Mundstücke (weitere Mundstücke können separat erworben werden), Hartschalen-Transporttasche und Bedienungsanleitung
- Kostenlose Lieferung

Der ACE X – federleicht und einfach zu bedienen

Das **Atemalkoholtestgerät** von ACE Instruments ist vielleicht nicht ganz so leicht wie eine Feder – aber fast: Mit einem Gewicht von nur 130 Gramm (inklusive Batterien) und einer handlichen Größe von 128 x 60 x 24 Millimeter ist der Tester ideal für den persönlichen Einsatz. Auch zum Ermitteln des Restalkohols am Morgen danach ist das Gerät hervorragend geeignet.
Die Bedienung ist selbst für ungeübte Benutzer kinderleicht: Über einen einzigen Knopf, der sowohl für Rechts- als auch Linkshänder gut zu erreichen ist, können Sie den Test durchführen. Das Ergebnis können Sie anschließend sofort auf dem OLED-Display ablesen, **der Wert ist dabei 1:1 interpretierbar.** Sie sollten allerdings die im Lieferumfang enthaltenen

Mundstücke nicht mehrmals verwenden – auch nicht bei sich selbst.

Testsieger einer Studie der TU Wien

Die Technische Universität Wien hat im Rahmen einer umfangreichen Studie im Jahr 2019 eine Reihe von Alkoholmessgeräten getestet. Das Ergebnis: **Mit einer Genauigkeit von 99,1 Prozent ist der ACE X Testsieger!**
Als CHIP Leser sparen Sie mit unserem Angebot 70 Euro auf den ACE X und bekommen ihn für nur 129 Euro – inklusive Versandkosten. Der Gutscheincode "**Chip23**" wird einfach im Feld "Gutschein-Code" eingelöst, dann erhalten Sie den exklusiven Vorteilspreis.

Alkoholtester vom Marktführer ACE Instruments

ACE wurde vor 20 Jahren im schönen Bayern gegründet. Heute sind sie der führende Fachdistributor für Atemalkoholmesstechnik im deutschsprachigen Großraum.
Sie beliefern Apotheken, Fachhändler und Verbraucher der öffentlichen Hand, Medizin, Industrie und Gewerbe, sowie auch Privatpersonen mit erstklassigen und leistungsfähigen Alkoholtestgeräten.
**Unser Deal-Team bietet jeden Tag beste Angebote für ein gelingendes Leben. CHIP erhält für jeden Verkauf eine Provision. Die Shopping-Deals werden von unseren Deal-Experten ausgewählt und unabhängig von der Redaktion gestaltet.*

Quelle: https://www.chip.de/news/Polizeigenaues-Alkoholtestgeraet-im-Angebot_184422802.html?utm_source=&utm_medium=chip-newsletter&utm_campaign=27-08-2023%2B09%253A43%253A13&utm_content=nl_chipn-wy&utm_term=

4) Hochwasser-Echtzeitkarte: Sind Sie bedroht? Die Antwort!

In Bayern droht aktuell immer noch Hochwasser. Eine offizielle Karte der Bundesländer zeigt für ganz Deutschland immer die aktuelle Hochwasserlage.

In Bayern droht immer noch Hochwasser und auch in Teilen der Schweiz und in Österreich kämpfen die Menschen mit den Wassermassen. Auf hochwasserzentralen.de sehen Sie jetzt sofort, wie in ganz Deutschland die Hochwasserlage ist.

Die Webseite zeigt eine Karte von Deutschland. Mit unterschiedlichen Farben wird der Pegel der Flüsse dargestellt. Klickt man die Punkte an, bekommt man Detailinformationen. Außerdem kann man sich die Hochwasserlage nach Bundesländern getrennt anzeigen lassen.

Derzeit sieht man überwiegend grüne Punkte: Dort ist derzeit kein Hochwasser. Ein gelb eingefärbter Punkt signalisiert „kleines Hochwasser“ und ein oranger Farbtupfer steht für „mittleres Hochwasser“.

Bedrohlich wird es, wenn der Punkt rot eingefärbt ist. Das signalisiert „großes Hochwasser“. Leuchtet der Punkt sogar in dunkelviolett, dann handelt es sich um ein „sehr großes Hochwasser“. Was das konkret bedeutet, ist von Bundesland zu Bundesland leicht verschieden, die genaue Interpretation finden Sie hier.

Aktuelle Lage in Bayern angespannt

Derzeit springen zwei rote Tupfer aus Bayern ins Auge. Einer davon ist Ingolstadt und der Landkreis Neuburg-Schrobenhausen. Der andere ist der Landkreis Kelheim.

Für die Drei-Städte-Stadt Passau, traditionell eine von Hochwasser oft heimgesuchte Grenzstadt im Freistaat Bayern, gibt es dagegen eine weniger starke Hochwasserwarnung. Für Passau heißt es aktuell: „Das Hochwasser aus dem Inneinzugsgebiet hat die Stadt Passau passiert. Die Pegel Passau/Donau und Ilzstadt/Donau sind rückläufig und haben

bereits die Meldestufe 3 verlassen.“

Auf der Donau hat sich zwar aufgrund der Niederschläge eine kleine Hochwasserwelle aufgebaut, doch für die ebenfalls von Zeit zu Zeit von Hochwasser heimgesuchte Donaustadt Regensburg wird allenfalls die Meldestufe 2 erwartet.

Für das übrige Deutschland sind keine großen Hochwasser gemeldet.

Woher die Daten stammen

Die Seite hochwasserzentralen.de wird von den deutschen Bundesländern betrieben: „Jedes teilnehmende Bundesland stellt hierfür laufend aktuelle Daten einer Auswahl von Hochwassermeldepegeln und eine Kurzinformation zur aktuellen Hochwasserlage zur Verfügung. Weitere Pegeldaten werden von der Wasser- und Schifffahrtsverwaltung des Bundes (WSV) sowie den zuständigen Behörden der Nachbarländer bereitgestellt“.

Schweiz und Österreich

In der Schweiz haben die Regenmassen zu Erdrutschen geführt. In Österreich hat es vor allem Sölden hart getroffen.

Quelle: https://www.pcwelt.de/article/1196910/hochwasser-karte-deutschland-echtzeit.html?utm_date=20230830094314&utm_campaign=Best-of%20PC-WELT&utm_content=Title%3A%20Hochwasser-Echtzeitkarte%3A%20Sind%20Sie%20bedroht%3F%20Die%20Antwort%21&utm_term=PC-WELT%20Newsletters&utm_medium=email&utm_source=Adestra&tap=39de1e7cd48826bafbe65379a817dcc8&eh=64bc18f05aa8fc98b946a260057eddd57f800a8db1ca4e20d8a3858ac410c4c4

5) Dringend – Rückruf: Fahrradhelme sitzen nicht fest

Ein Fahrradhelm, der im Fall eines Sturzes keinen echten Schutz für den Kopf bietet: Smyths Toys ruft dieses Kinderprodukt zurück.

Der Spiel- und Sportwarenhändler Smyths Toys informiert über einen "dringenden Rückruf" von Kinderfahrradhelmen des Herstellers MV Sport Hong Kong Ltd. Es habe sich herausgestellt, dass die Helme aufgrund des unzureichenden Befestigungssystems nicht richtig auf dem Kopf sitzen. "Die Wirksamkeit der Trageeinrichtung kann nicht eingehalten werden", schreibt Smyths Toys. Dies könne im Falle eines Sturzes zu Verletzungen führen.

Um diese Helme handelt es sich:

Mit diesem Warnhinweis informiert Smyths Toys über den Rückruf von fehlerhaften Kinderfahrradhelmen des Herstellers MV Sport Hong Kong Ltd. Smyths Toys

SKU 206073 Fahrradhelm LOL Surprise 48-52 cm

SKU 206074 Fahrradhelm Disney Princess 48-52 cm NR

SKU 206075 Fahrradhelm Paw Patrol 48-52 cm

SKU 127003 Fahrradhelm Batman 48-52 cm

SKU 209551 Fahrradhelm Disney Frozen 2 48-52 cm

SKU 173294 Fahrradhelm Spiderman 48-52 cm

Modellnummer: YX-041

Aus der Beschreibung von Smyths Toys wird nicht klar, was bei den Kinderhelmen genau mit "unzureichendem Befestigungssystem" (Kinnriemen, Spannrad zur Größenanpassung oder Verschlussschnalle) gemeint ist. "Kunden sollten das Produkt nicht mehr verwenden", rät der Händler. Kunden könnten sich an die nächste Filiale wenden, um eine Rückerstattung des Kaufpreises zu erhalten, heißt es. Außerdem stehe ein Kundenservice unter dieser Telefonnummer zur Verfügung: Telefon: +49 (0)221 5972 454.

Quelle: https://www.t-online.de/leben/aktuelles/id_100222638/rueckruf-fahrradhelme-fuer-kinder-vom-smyths-toys-schuetzen-nicht.html