Schieb Report

Ausgabe 2024.43

Wo ist der Upload-Status der iOS 18 Foto-App?

Wenn ihr einen Mac und iOS-Geräte nutzt, dann ist der iCloud Fotostream eine wichtige Funktion, um auf all euren Geräten synchron zu sein. Ihr müsst neue Fotos nicht mehr manuell hochladen und verteilen, via iCloud geht das automatisch. Mit iOS 18 allerdings hat Apple einige Änderungen vorgenommen, die wenig intuitiv sind. Wir können helfen!

Aktivieren und nutzen des Fotostreams

Den Fotostream müsst ihr auf jedem Gerät einmal in den Einstellungen der jeweiligen Apple Foto-App aktivieren.

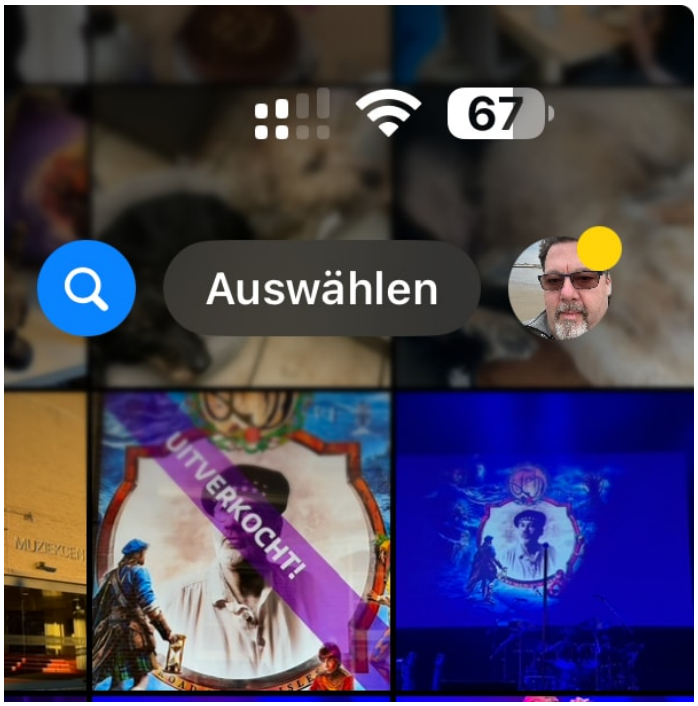
- Dazu aktiviert die Optionen **iCloud-Fotos** und **Mein Fotostream**. Damit werden sowohl die Fotos des aktuellen Geräts in iCloud hochgeladen als auch die Fotos der anderen, mit derselben Apple ID gekoppelten Geräte heruntergeladen. Ihr habt auf allen Geräten denselben Foto-Stand.

- Nun ist die Verfügbarkeit der Bilder auf Ihren eigenen Geräten ja nur der halbe Spaß: Ihr wollt ja auch mit anderen Menschen teilen können. Das ist mit Bordmitteln direkt vom Telefon oder Tablet schnell gemacht: Tippt unter Alben auf **+**, dann auf **Neues geteiltes Album**.

- Benennt dieses Album, dann fügt ihm durch ein Tippen auf **+ Einladen** Personen hinzu, die die Bilder sehen können.

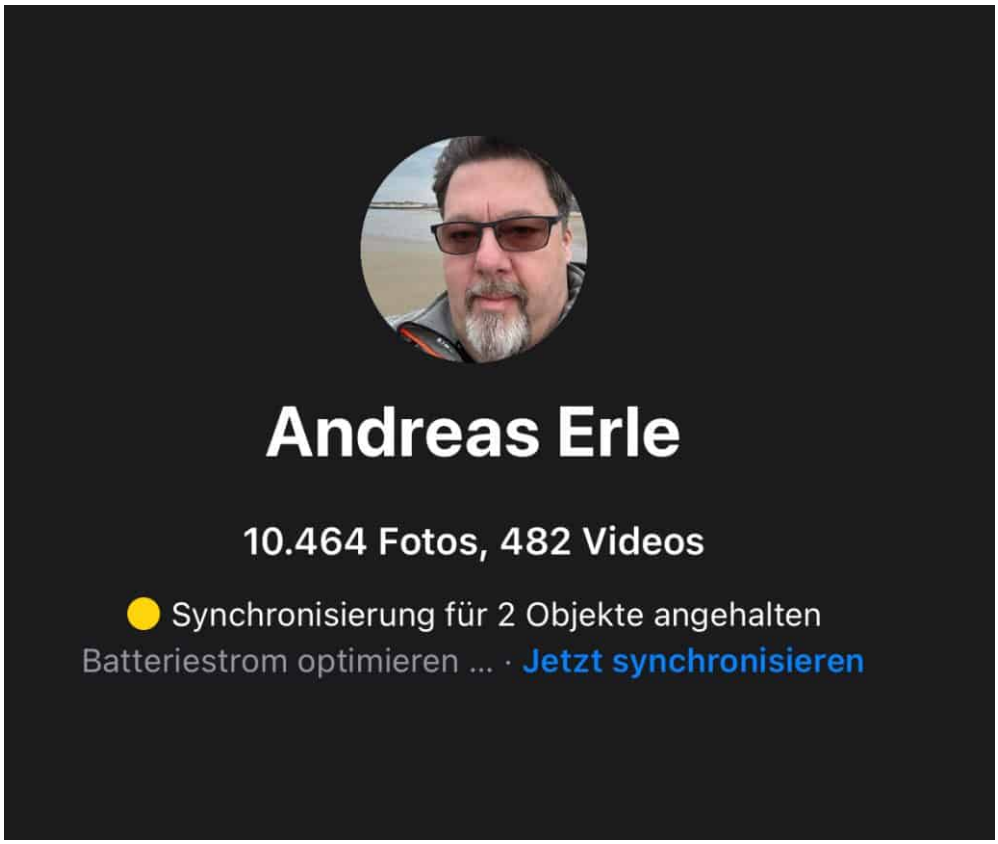
Der Upload-Status unter iOS 18

Eine der vielen Neuerungen bei iOS 18 ist der vermeintlich verschwundene Upload-Status: Wenn ihr ein Foto gemacht habt, dann muss das erzeugende Gerät dieses erst in iCloud hochladen, damit alle anderen Geräte es herunterladen können. Das funktioniert meist ohne manuellen Eingriff. Meist, denn wenn etwa die Netzverbindung schlecht ist oder der Akku leer, dann deaktiviert die Foto-App schnell einmal den Upload. Das war vor iOS 18 schnell zu sehen, war der Sync-Status der Fotos mit iCloud doch direkt unter den letzten Fotos zu sehen. Das hat Apple allerdings in iOS 18 entfernt. Dumm, wenn die Fotos einfach nicht hochladen sollen. Keine Sorge, so findet ihr ihn:

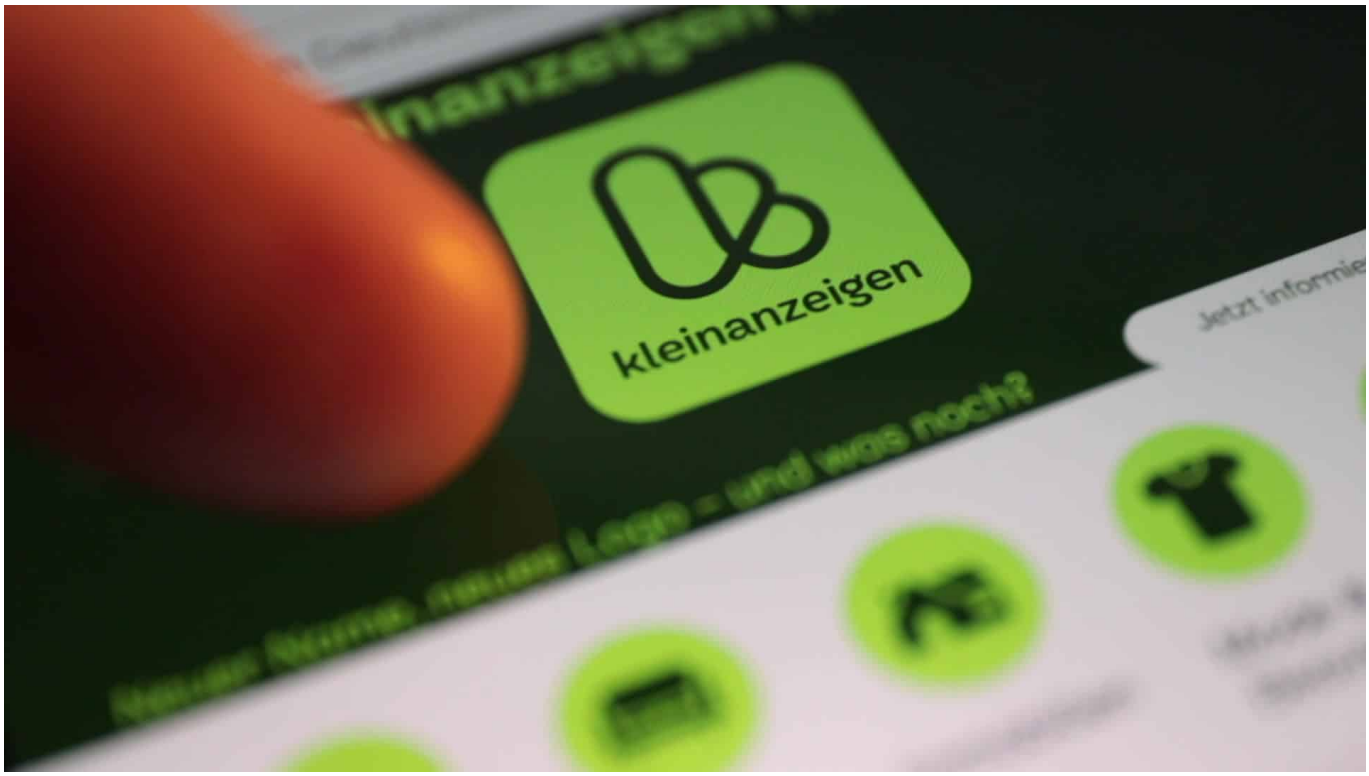


- In der Foto-App habt ihr oben rechts das Kontaktbild eurer Apple ID.
- Wenn der Upload angehalten ist, dann seht ihr daran einen gelben Punkt.
- Läuft er aktuell, dann habt ihr eine gründe, runde Fortschrittsanzeige um euer Kontaktbild.
- Tippt darauf, dann öffnet sich die Übersicht, die in den älteren iOS-Versionen unter den Fotos war.
- Tippt auf **Jetzt synchronisieren**, um die Synchronisation erneut zu starten.

- Kurze Zeit später sind die Bilder auf allen Geräten verfügbar.



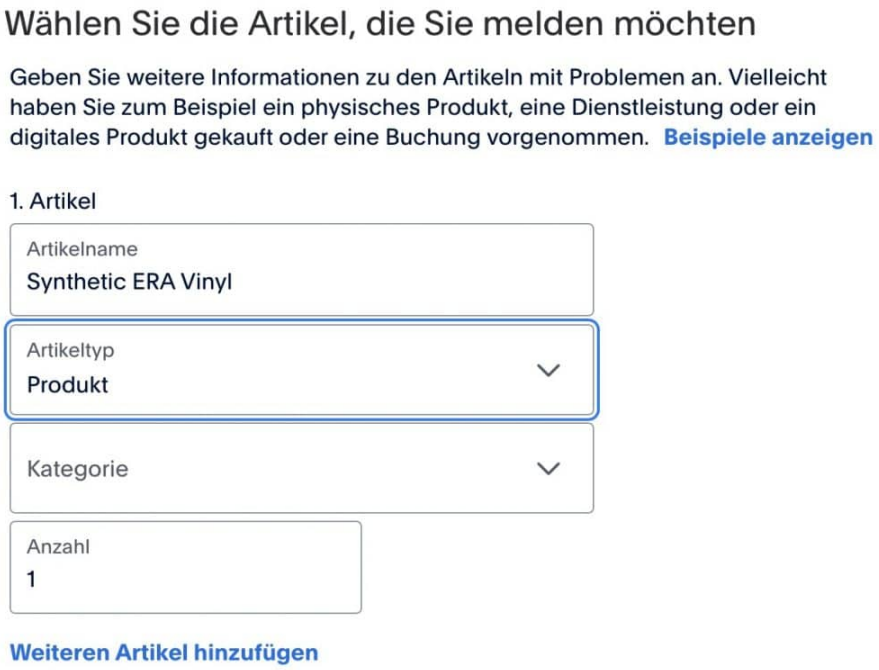
Kleinanzeigen: Der Dreiecks-Betrug



Online-Kauf ist Vertrauenssache. Und wenn das nicht reicht, dann können technische und organisatorische Maßnahmen helfen. Dumm nur, wenn die Bösewichte die dann auch noch umgehen und ihr darauf hereinfallt. Wir zeigen euch, worauf ihr achten müsst.

Der Käuferschutz bei Paypal

Paypal hat den Ruf, ein sehr sicherer Zahlungsweg zu sein. Vor allem deshalb, weil Zahlungen darüber im Normalfall über den Käuferschutz abgesichert sind. Die Ware kommt nicht? Der sprichwörtliche Backstein ist im Paket statt des Smartphones?



- Wenn ihr eine Transaktion melden wollt, dann meldet euch an euer Paypal-Konto an und sucht in der Liste der Transaktionen die kritische heraus.

- Öffnet sie, dann klickt auf den Link **Ein Problem melden**.

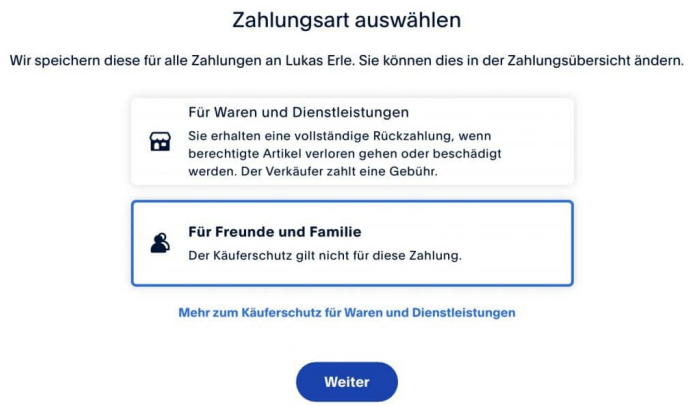
- Gebt nun ein, was ihr hättet bekommen sollen, wann die Lieferung hätte erfolgen sollen und was passiert ist (keine Lieferung, falsche oder defekte Ware etc.)

- Schickt die Meldung ab. Paypal geht jetzt in die Prüfung, kontaktiert den Verkäufer und entscheidet dann irgendwann, meist zu euren Gunsten.

Klingt gut? Ja, aber es gibt einen Haken: Das funktioniert nur dann, wenn ihr nicht per "Freunde und Familie" (Family & Friends) gezahlt habt. Das wollen viele Betrüger gern, angeblich, "weil es euch Gebühren spart". Tatsächlich aber eher, weil ihr dann keinen Käuferschutz nutzen könnt!

Trotz echter Zahlung: Betrug!

Jetzt verkauft ihr eine - meist hochpreisige - Ware aus dem Bereich der Unterhaltungselektronik: Kamera, Smartphone, Laptop, irgendein beliebtes Gerät. Auf Kleinanzeigen kommen in den ersten Minuten alle möglichen Anfragen. Geht getrost davon aus, dass die allermeisten betrügerisch sind.



Was ihr nicht tun solltet:

- Gebt keine Informationen über euch heraus. Namen, Adresse, E-Mail-

Adresse, auch die Kopie der Rechnung dient Betrügern gern dazu, euch auszuspionieren. Das geht bis hin zum Identitätsdiebstahl!

- Verlasst nicht die Kommunikationswege von Kleinanzeigen: Telefonate. WhatsApp, E-Mails, all das versucht euch abzulenken.

- Das Chat-System von Kleinanzeigen ist nachvollziehbar und nicht veränderbar. Wenn ihr später einmal einen Betrugsfall nachweisen müsst, dann hilft es euch.

Jetzt kommt aber ein potenzieller Käufer und will eure Ware kaufen. Und er zahlt per PayPal, ohne auf "Freunde und Familie" zu bestehen. Nach einer etwas längeren Pause geht das Geld per PayPal ein. Alles gut, oder?

- Kontrolliert sehr genau, ob die Daten, die der vermeintliche Käufer euch angibt, mit der PayPal-Zahlung übereinstimmen.

- Oft war die Pause keine Kommunikationspause, sondern der Betrüger hat seinerseits eure Ware als Verkäufer eingestellt. Sobald sein Käufer anbeißt, gibt er ihm eure PayPal-Adresse für die Zahlung.

- Das nennt man Dreiecksbetrug: Der Zahlende schickt das Geld und ist es los. Er bekommt aber keine Ware, denn die schickt ihr an den Betrüger, ihr habt ja vermeintlich das Geld. Da ihr aber einen Versand an den Zahlenden nicht nachweisen könnt, werdet ihr es zurückgeben müssen.

- Der lachende Dritte ist der Betrüger: Der hat kein Geld bezahlt und trotzdem die teure Ware bekommen. Versandadressen sind meist gefaked und dienen nur der Warenannahme. Finden werdet ihr - oder die Polizei - den Betrüger da nicht mehr.

Cyberbetrug explodiert: Warum Scamming zur globalen Bedrohung wird

Stell dir vor, du wachst eines Morgens auf und dein Konto ist leer – kein Einbruch, kein Hacker, nur eine gut gemachte Fake-Mail, die deine Welt auf den Kopf gestellt hat. Cyberkriminalität hat eine neue Dimension erreicht, und niemand ist mehr sicher. Ob du es glaubst oder nicht, die nächste Zielscheibe könnten du oder dein Unternehmen sein. Willkommen in der perfiden Welt des Scammings – wo Vertrauen dein größter Feind ist.

Der schockierende Aufstieg von Online-Betrug

Cyberbetrug, auch als "Scamming" bekannt, hat in den letzten Jahren dramatisch

zugenommen und erreicht immer neue Höhen. Der Schaden, der durch Betrügereien weltweit verursacht wird, geht in die Milliarden. Besonders erschreckend: Nicht nur Unternehmen und Institutionen sind betroffen – auch normale Bürger werden regelmäßig Opfer von raffinierten Betrugsmaschen.

Ein besonders drastisches Beispiel ereignete sich im August 2024 in Luxemburg. Ein Mitarbeiter eines Chemieunternehmens wurde von Cyberkriminellen dazu gebracht, 60 Millionen Dollar – die Hälfte des Jahresgewinns – an Betrüger zu überweisen. Und das ohne komplexe Hackerangriffe oder Systemeinbrüche. Der Betrug erfolgte allein durch Fake-Webseiten, gefälschte E-Mails und gezielte psychologische Manipulation.

Scamming – Eine Bedrohung für uns alle

Es ist erschreckend, wie stark sich Cyberbetrug entwickelt hat. Laut Statistiken wurden weltweit Schäden in Höhe von fast einer Billion US-Dollar durch Scamming verursacht, und jeder Vierte war bereits Opfer eines solchen Betrugs. Egal ob per E-Mail, SMS, WhatsApp oder Social Media – die Betrüger sind überall präsent.

Aktuell besonders im Fokus steht die sogenannte "Pig Butchering"-Masche, bei der Kriminelle über Dating-Apps oder soziale Netzwerke Vertrauen aufbauen, um Opfer zu Investitionen in Kryptowährungen zu überreden. Sobald genügend Geld investiert wurde, verschwinden die Betrüger spurlos. Es sind perfide Methoden, die auf emotionaler Manipulation basieren – die Opfer werden wie Schweine gemästet und dann geschlachtet.

CEO-Betrug: Wenn Unternehmen Millionen verlieren

Eine weitere verbreitete Masche ist der "CEO-Fraud". Dabei geben sich Betrüger als Führungskräfte eines Unternehmens aus und veranlassen ahnungslose Mitarbeiter zu Geldtransfers. Im erwähnten Fall in Luxemburg funktionierte diese Taktik so gut, dass 60 Millionen Dollar verloren gingen. Ein weiteres mittelständisches Unternehmen in Deutschland entging nur knapp einem Verlust von 10 Millionen Euro. Der Trick ist simpel, aber äußerst effektiv: Es braucht nur eine E-Mail oder einen gefälschten Anruf, um Schaden in Millionenhöhe zu verursachen.

Nicht nur Unternehmen sind betroffen – auch Privatpersonen werden durch falsche Paketbenachrichtigungen oder gefälschte Kleinanzeigen auf Plattformen wie eBay Kleinanzeigen um ihr Geld gebracht. Die Kreativität der Betrüger scheint keine Grenzen zu kennen.

Warum fallen Menschen auf Scams herein?

Trotz zahlreicher Warnungen fallen Menschen immer wieder auf die Tricks der Betrüger herein. Warum? Es liegt an der gezielten Manipulation von Emotionen. Betrüger spielen mit Gefühlen wie Liebe, Angst oder Gier, um ihre Opfer zu täuschen. Besonders perfide sind Betrüger, die sich über WhatsApp als Kinder oder Enkel ausgeben und dringend Geld für eine vermeintliche Notlage verlangen. Die Opfer handeln oft aus dem Reflex heraus, einem geliebten Menschen sofort helfen zu wollen, ohne die Situation zu hinterfragen.

Die Dunkelziffer der Opfer ist hoch, da viele sich schämen, über den Betrug zu sprechen. Es braucht mehr Aufklärung und Schutzmaßnahmen, um diesen emotionalen Angriffen entgegenzuwirken.

Was tun große Unternehmen gegen Cyberbetrug?

Zahlungsdienstleister wie PayPal oder Kreditkartenunternehmen haben mittlerweile fortschrittliche Systeme entwickelt, um verdächtige Transaktionen zu erkennen und zu stoppen. Doch oft sind die Betrüger schneller. Ein besonders krasses Beispiel ist eine Frau in Deutschland, die über Monate hinweg hohe Summen an Betrüger überwies, weil sie glaubte, in ein lukratives Krypto-Geschäft investiert zu haben – trotz der Warnungen ihres Zahlungsanbieters.

Auch Online-Marktplätze wie Amazon und eBay arbeiten daran, Betrugsfälle zu reduzieren. Die Betrüger passen sich jedoch schnell an, indem sie ganze Webseiten klonen oder gefälschte Zahlungsaufforderungen verschicken. Trotz aller Bemühungen der Plattformen sind die Nutzer am Ende die Leidtragenden.

Künstliche Intelligenz: Eine neue Waffe der Betrüger

Ein besonders beunruhigender Trend ist der Einsatz von Künstlicher Intelligenz (KI) durch Cyberkriminelle. Betrüger verwenden KI, um täuschend echte Deepfake-Videos und -Stimmen zu erstellen, die dann für CEO-Betrügereien oder Fake-Anrufe genutzt werden. Kürzlich wurde ein Fall bekannt, bei dem ein Live-Zoom-Call mit einem KI-generierten Avatar durchgeführt wurde, der sich als Chef eines Unternehmens ausgab und Mitarbeiter zu Geldtransfers aufforderte.

Noch gefährlicher sind automatisierte Phishing-Kampagnen, bei denen ChatGPT-ähnliche Technologien verwendet werden, um personalisierte E-Mails in perfektem Deutsch zu erstellen. Diese E-Mails sind so überzeugend, dass die Empfänger kaum Verdacht schöpfen. Die Reichweite solcher automatisierten Betrugsversuche ist enorm, und es wird zunehmend schwieriger, sich zu schützen.

Ein Wettrennen zwischen Angreifern und Verteidigern

Während die Betrüger ihre Methoden ständig weiterentwickeln, arbeiten IT-Sicherheitsexperten und Unternehmen daran, ihre Systeme zu verbessern und den Schaden zu minimieren. Doch es ist ein ständiges Wettrennen. Für den Schutz im persönlichen Umfeld kann es hilfreich sein, einen Geheimcode mit engen Verwandten oder Kollegen zu vereinbaren. So kann man im Zweifelsfall sicherstellen, dass man es wirklich mit der echten Person zu tun hat.

Der Schlüssel zur Bekämpfung von Scams liegt jedoch nicht nur in der Technik, sondern auch in der Sensibilisierung und Aufklärung der Nutzer. Jeder sollte sich der Risiken bewusst sein und lernen, wie man betrügerische E-Mails, Anrufe oder Nachrichten erkennt. Denn eines ist klar: Cyberkriminalität wird uns auch in Zukunft begleiten – und nur durch Wachsamkeit und technologische Innovation können wir uns schützen.