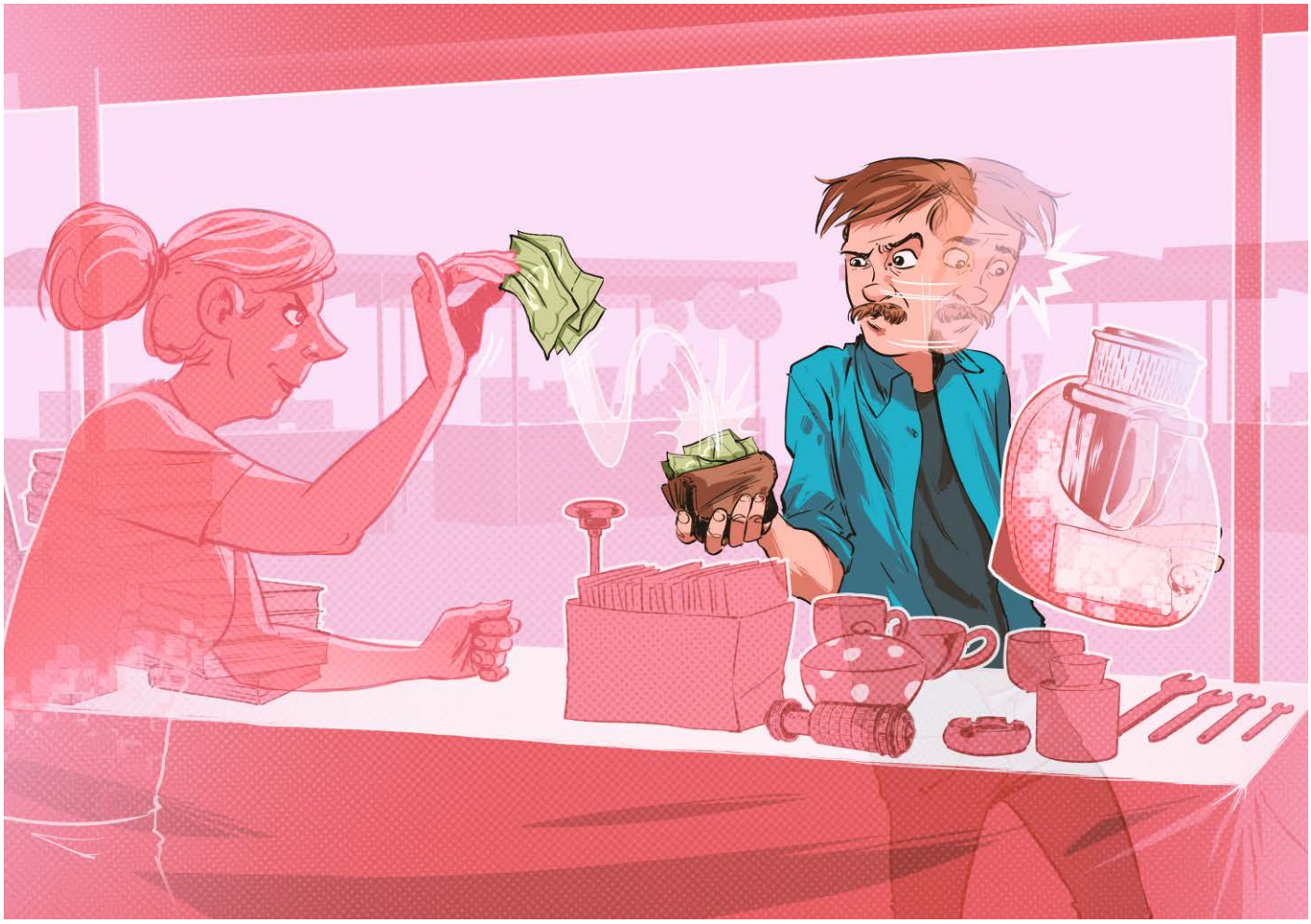


Bild: Albert Hulm

Perfektes Schauspiel

Wie Betrüger mit Fakt und Fiktion Gebrauchtkäufer abzocken

Eine originalverpackte Edel-Küchenmaschine für einen realistischen Preis, glaubwürdige Fotos, eine freundliche Anruferin und eine stimmige Geschichte: Betrüger treiben immer mehr Aufwand, um Nutzer von Kleinanzeigenportalen abzuzocken. Wir erklären, wie Sie sich dagegen wappnen.

Von Markus Montz

Stellen Sie sich vor, Sie suchen eine Edelküchenmaschine, die aktuell beliebt und begehrt ist. Auf einem Kleinanzeigenportal finden Sie ein Angebot, bei dem vom Preis bis zur Beschreibung alles vertrauenswürdig aussieht. Ein anschließendes Telefongespräch erzeugt in Kombination mit vermeintlichen Belegen wie Ausweiskopien und Websites genug Vertrauen, dass Sie schließlich in die Falle tappen – und viel Geld verlieren, ohne die Ware je zu Gesicht zu bekommen.

Eine informell organisierte Gruppe von Opfern dieser relativ neuen Betrugsmasche hat sich an c't gewandt. Anhand ihrer Erfahrungen zeigen wir, mit welchen Tricks die gewerbsmäßig organisierten Täter selbst aufmerksame Menschen manipulieren („Social Engineering“) – bis diese unter dem Einfluss von latentem Zeitdruck und subtilen Emotionen teure Fehler begehen. Um es klar zu sagen: „Dumm“ hat sich keines der Opfer angestellt. Alle tappten in Fallen, die nicht auf den ersten Blick erkennbar waren. Außerdem geben wir Tipps, wie Sie die Täter ins Leere laufen lassen.

Seriös wirkende Angebote

Klaus G. suchte auf eBay Kleinanzeigen nach einer Edelküchenmaschine, die beim Hersteller nicht mehr lieferbar war. Ein am selben Tag eingestelltes Inserat einer Lara K. versprach ein neues, noch originalverpacktes Gerät. Der Preis klang realistisch: verhandelbare 1150 Euro, eine kleine Ersparnis gegenüber der unverbindlichen Preisempfehlung, kein unseriöser Knallerpreis.

Ein Foto zeigte den verschnürten Karton. In der Beschreibung hieß es, man habe das Gerät für ein Ferienhaus bestellt, sich aber aus Geschmacksgründen doch

für ein anderes Modell entschieden. Interessenten könnten die Küchenmaschine abholen, Rechnung und Garantie lägen vor. Klaus A. bekundete daraufhin über die Chatfunktion sein Interesse. Um den Prozess abzukürzen, schickte er seine Handynummer mit.

Wenig später erhielt er einen WhatsApp-Sprachanruf, die App zeigte eine deutsche Handynummer an. Eine freundliche Frau stellte sich in bestem Hochdeutsch als „Nina P." vor. Sie sei eine Freundin von Lara K., die in ihrem Auftrag die Anzeige eingestellt habe – sie selbst kenne sich mit eBay Kleinanzeigen nicht aus. Sie wiederholte, dass es sich um eine reine Geschmacksfrage handele und die Maschine schon länger herumstehe.

Klaus G. rief nach kurzer Bedenkzeit über WhatsApp zurück, um das Angebot anzunehmen. Man einigte sich schließlich auf 950 Euro. Nebenbei ließ die angebliche Nina P. fallen, dass sie seit drei Monaten Mutter einer kleinen Tochter sei (im Hintergrund krakeelte passend dazu eine Babystimme) und mit Ferienwohnungen ihr Geld verdiene. Wenn Klaus G. wolle, könne er sich ja mal ihre Homepage anschauen; die Adresse sagte sie gleich mit auf.

Vertrauen erzeugt

Parallel prüfte Klaus G. die Homepage – sie besaß eine .de-Domain und auch die Ferienhausvermietung schien es ausweislich des Impressums zu geben. Es enthielt neben dem Namen der Anruferin auch eine Anschrift und eine Mailadresse, eine Umsatzsteuer-ID sowie die gerade genutzte Handynummer. Zudem verwies es auf ein vermeintliches Mutterunternehmen, inklusive Anschrift und einem Gerd Z. als dessen Inhaber. Ein Instagram-Account mit 1800 Followern komplettierte das Portfolio. Das WhatsApp-Profil der Anruferin schien das Gesagte ebenfalls zu bestätigen: Unter einem Babyfoto befanden sich die Telefonnummer und die Initialen. Klaus G. war sicher, es mit einer seriösen Verkäuferin zu tun zu haben.

Es blieb noch die Bezahlart. Mangels eigenem Nutzerkonto sei eine Zahlung über „Sicher bezahlen" bei eBay Kleinanzeigen [1] ja nicht möglich, so die Anruferin, und ein PayPal-Konto habe ihr Unternehmen leider nicht. Das Geld müsse „aus steuerrechtlichen Gründen" aber an ihre Firma gehen. Klaus G. nannte ihr daraufhin seine Kreditkartendaten, der Transfer scheiterte laut Anruferin aber an „3D-Secure". Nun schlug sie eine Überweisung vor, ausweislich der IBAN an ein Institut in Irland – angeblich, weil ihr Unternehmen auch im Ausland Ferienwohnungen vermiete.

Vertrauen missbraucht

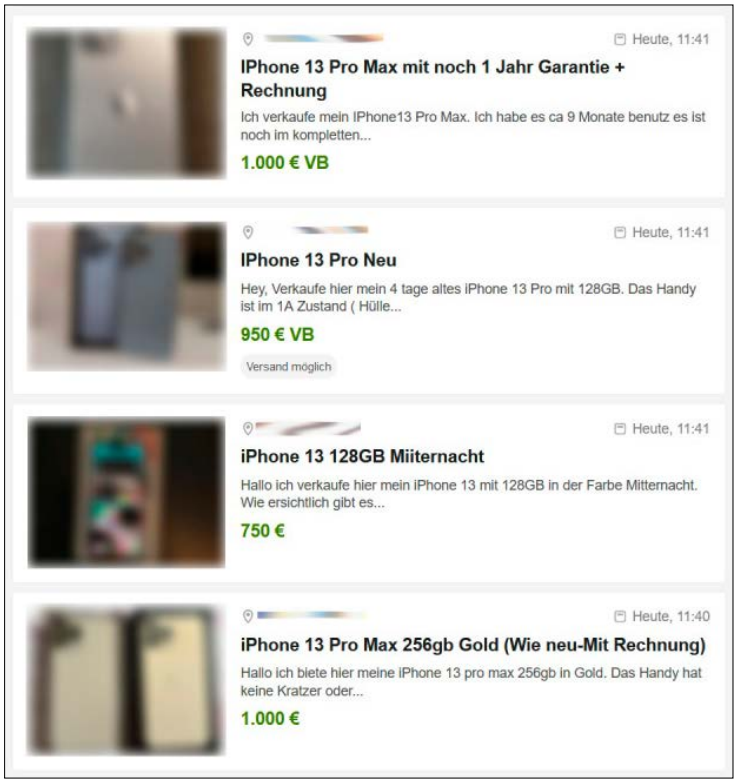
Nachdem ihm Frau P. auch noch die „Originalrechnung" als Bilddatei schickte, überwies Klaus P. das Geld. Wenig später bekam er ein mulmiges Gefühl – zunächst wegen seiner Kreditkarte, die er daraufhin sperren ließ. Auf Nachfrage im WhatsApp-Chat bestätigte ihm die angebliche Nina P. tags darauf, dass das Geld eingegangen sei und sie das Gerät auf den Weg bringen werde. Ihre Nachrichten wurden spärlicher, zwei Tage später schrieb sie ihm, sie sei im Krankenhaus und würde sich später melden. Auf weitere Nachfragen antwortete sie nicht mehr.

Nun versuchte Klaus G. es bei Gerd Z., der ja laut Impressum Inhaber der Muttergesellschaft sein sollte. Die Täter hatten dessen Daten missbraucht. Klaus G. sei allerdings nicht der Erste, der sich mit dieser Frage an ihn wende; er habe bereits Kontakt zur echten Nina P., die mit der Sache aber nichts zu tun habe. Daraufhin erstattete G. Anzeige bei der Polizei und wandte sich an „Modulr", die irische Neobank, bei der laut IBAN das Konto geführt wurde. Die Bank versicherte ihm, der Sache nachzugehen und bereits „Maßnahmen gegen das Konto" ergriffen zu haben. Er solle sich außerdem an seine Bank wenden, damit die Rechtsabteilungen in den Austausch treten könnten; vergeblich, wie sich bald herausstellte.

Außerdem meldete Klaus G. das Konto von Lara K. bei eBay Kleinanzeigen. Der Kundendienst antwortete, man habe das Nutzerkonto „des Anbieters, mit dem Du Kontakt hattest, eingeschränkt". Man gehe davon aus, dass es „missbräuchlich durch Dritte" verwendet worden sei, während der „eigentliche Kontoinhaber" die Anzeige nicht geschaltet habe und auch nicht hinter den Nachrichten stecke.

c't kompakt

- Betrüger ködern Schnäppchenjäger auf Kleinanzeigenportalen mit seriös wirkenden Inseraten.
- Mit einem Geflecht aus gestohlenen Identitäten, gefälschten Websites und emotionalen Geschichten schaffen sie bei den Interessenten Vertrauen, bis diese sich auf unsichere Zahlungswege einlassen.
- Mit den richtigen Vorsichtsmaßnahmen vermeiden Sie, in die Falle zu tappen, und können im Schadensfall vielleicht noch etwas retten.



Vorsicht auf Kleinanzeigenportalen: Seriöse Angebote sind von Fakes kaum zu unterscheiden.

Ein WhatsApp-Profil lässt sich leicht fälschen. Das Foto haben die Täter einfach auf Facebook kopiert und die Nummer ist nicht mehr vergeben, auch wenn WhatsApp sie weiterhin anzeigt.

Kein Einzelfall

Klaus G. recherchierte weiter. Über die im Impressum angegebene Adresse erreichte er schließlich die echte Nina P. Sie zählte ebenfalls zu den Geschädigten: Bei ihr hatte die gleiche Tätergruppe auf ein Gesuch nach einem teuren Smartphone reagiert. Auf die Überweisung hatte die echte Nina P. sich am Ende zwar nicht eingelassen, dafür hatte sie den Tätern auf Nachfrage Fotos ihres Ausweises geschickt. Nun missbrauchten die Täter ihre Identität, um den Opfern damit eine falsche Geschichte aufzutischen und ihre Spuren zu verwischen. Die Familie hatte deshalb bereits Anzeige erstattet.

Allein der c't bekannte Schaden beträgt zwischen 15.000 und 20.000 Euro. Ungefähr die Hälfte davon entfällt auf hochpreisiges DJ-Equipment. Nur wenige Geschädigte hatten Glück und bekamen ihr Geld zurück. Die gefakte Website, die ausweislich der Nameserver-Angaben beim Website-Dienstleister Jimdo gehostet war, ist mittlerweile immerhin offline. Gerd Z. hatte wegen der unerlaubten Nutzung seiner Daten einen Anwalt beauftragt. Jimdo bestätigte auf Nachfrage von c't, die Website gehostet und „auf Aufforderung einer ermittelnden Behörde" abgeschaltet zu haben; weitere Angaben seien aus Datenschutzgründen nicht möglich.

Köder und falsche Nummern

Den Ausgangspunkt bilden in diesem und allen anderen Fällen Nutzerkonten auf eBay Kleinanzeigen, die die Täter entweder gekapert oder unter falscher Identität eröffnet haben. Die Täter bieten dort meist schwer erhältliche, höherpreisige Waren an, die einen subtilen Kaufdruck bei Interessenten erzeugen. Die Preise bewegen sich im realistischen Rahmen. Zur Illustration verwenden die Betrüger anderswo kopierte Fotos. Die Beschreibungstexte samt „Hintergrundgeschichte" sind frei erfunden und sollen Vertrauen aufbauen.

Unser Rat: Denken Sie stets daran, dass betrügerische Konten auf Kleinanzeigenportalen allgegenwärtig sind. Die Schilderung eines Betroffenen, der nach dem Reinfall weitere Angebote für die gesuchte Kamera prüfte („neun von zehn waren Fake"), hat uns nicht überrascht. Lassen Sie daher besonders bei höherwertigen und womöglich besonders begehrten Produkten Vorsicht walten – in den uns bekannten Fällen ging es nicht nur um teure Küchengeräte, sondern auch um Kameras, High-End-Grafikkarten, Smartphones, Playstations und DJ-Ausrüstung.

Im zweiten Schritt erfragen die Täter eine Mobilfunknummer, um die Interessenten vom Portal herunter zu locken. Das hebelt die Schutzmechanismen aus, die beispielsweise eBay Kleinanzeigen mit „Sicher bezahlen" bietet. Im aktuellen Fall riefen die Betrüger die Interessenten über WhatsApp an und nutzten zusätzlich den WhatsApp-Chat (zu anderen Wegen wie Call-ID-Spoofing mehr in [1]). WhatsApp hat aus Sicht der Betrüger den Vorteil, dass sie die App nur einmal über eine SMS an die Rufnummer freischalten müssen, die SIM-Karte anschließend aus dem Gerät nehmen und abmelden können. Dem Empfänger wird sie trotzdem weiterhin angezeigt.

Unser Rat: Geben Sie Ihre Telefonnummern grundsätzlich nicht preis. Ist es doch passiert, lassen Sie sich nicht vom Portal weglocken oder bestehen Sie bei Anrufen oder SMS- respektive Messengernachrichten darauf, spätestens zum Bezahlen wieder in den Chat des Kleinanzeigenportals zu wechseln. Vertrauen Sie keiner angezeigten Rufnummer. Einige Interessenten wendeten Schlimmeres ab, als sie versuchten, die Nummer über das normale Mobilfunknetz zu erreichen – das ein „nicht vergeben" zurückmeldete.

Theatervorstellung

Im dritten Schritt wollen die Täter das Vertrauen der Interessenten gewinnen und erfinden Erklärungen, zum Beispiel dafür, dass die Namen von Kontoinhaber und Anrufer voneinander abweichen. Also konstruieren sie geschickt Figuren samt Hintergrundgeschichten und vermischen Fiktion und Realität. Real (aber von Dritten gestohlen) sind die Namen, persönlichen Daten und eventuell Fotos. Letztere – beispielsweise das Babyfoto – kopieren die Täter aus sozialen Medien wie Facebook. Die Namen und Adressdaten stammen von Personalausweiskopien, die die Betrüger sich unter Vorwänden von den eigentlichen Inhabern besorgt haben (siehe Kasten). Zu diesen Menschen denken sie sich eine Geschichte und einen Verkaufsgrund aus, subtil mit Emotionen angereichert und von akzentfrei deutsch sprechenden Menschen geschauspielert.

Ihre Geschichte untermauern die Täter oft mit Rechnungskopien, die sie sich ebenfalls von Dritten besorgt oder einfach gefälscht haben. Das Kernstück in diesem Fall war die falsche Website der Ferienhausvermietung, die sie mit anderswo kopierten Fotos und Texten sowie den ergaunerten Identitäten bestückt hatten. Solche Websites sollen die Interessenten in Sicherheit wiegen und gehören mittlerweile zum gängigen Instrumentarium von Betrügern [2]. Dabei kommt den Tätern zupass, dass Webhoster die Identität von Website-Betreibern nach deutschem Recht nur in Verdachtsfällen prüfen müssen. Häufig verschicken die Betrüger außerdem Kopien der Ausweise, die sie ergaunert haben – und bitten die Interessenten subtil darum, im Gegenzug ebenfalls Ausweisfotos zu senden.

Unser Rat: Bleiben Sie auf Distanz und glauben Sie nichts. Sie wollen etwas kaufen und verhandeln mit Unbekannten in der Anonymität des Internets; eine Hintergrundgeschichte können Sie nicht überprüfen. Seien Sie extrem misstrauisch, wenn die Namen von Kontonutzer und Anrufer voneinander abweichen. Selbst Ausweiskopien belegen keine Identitäten, denn Identitätsmissbrauch ist allgegenwärtig – verschicken Sie daher auch selbst

nie Ausweiskopien an Unbekannte. Websites sind ebenfalls kein Beleg für ehrbare Absichten: Betrüger buchen Domains (auch mit .de) einfach mit gestohlenen Zahlungsdaten und klicken falsche Inhalte im Handumdrehen zusammen.

Weg ist das Geld

Haben die Täter Vertrauen aufgebaut, verleiten sie die Interessenten im letzten Schritt zu einer Banküberweisung. Zunächst erfinden die Täter vermeintlich plausible Gründe, weshalb eine Bezahlmethode mit Käuferschutzoptionen wie „Sicher bezahlen“ auf eBay Kleinanzeigen, PayPal oder Kreditkarte nicht möglich sei. Geben Interessenten Kreditkartendaten preis, missbrauchen die Täter diese unter Umständen ebenfalls für illegale Zwecke.

Um den Geldtransfer für das Opfer einfach zu machen und zugleich ihre Spuren zu verwischen, wählen die Täter gern ausländische Banken in der Eurozone als Ziel. Dabei nutzen sie gezielt Kreditinstitute mit Schwächen bei der Identitätsprüfung – meist haben ahnungslose Strohleute die Konten eröffnet und den Tätern die Zugangsdaten überlassen. Für die ausländische IBAN denken sie sich Erklärungen aus, wie die „steuerlichen Gründe“ bei Klaus G. In einem anderen Fall erfanden sie für die IBAN der irischen „Prepaid Financial Services“ (mit voranstehendem IE) eine Bank mit deutschem Namen – zupass kam ihnen dabei, dass dieses unauffällig auftretende Institut nur schwer im Netz zu finden ist.

Unser Rat: Überweisen Sie niemals Geld auf Girokonten von Unbekannten, egal ob deutsche oder ausländische IBAN – Sie haben so gut wie keine Chance, es zurückzubekommen. Am besten holen Sie die Ware selbst ab und zahlen bar. Bei Versand bestehen Sie auf eBay Kleinanzeigen auf „Sicher bezahlen“, auch wenn die Treuhandfunktion teuer für Käufer ist. Alternativ schlagen Sie PayPal vor; dort zahlt der Verkäufer das Entgelt. Nutzen Sie ausschließlich die Option „Waren und Dienstleistungen“ und beachten Sie die Regeln für den Käuferschutz [2]. Geben Sie Kreditkartendaten nie an Unbekannte weiter.

Die echte Nina P. handelte an dieser Stelle umsichtig: Vor der vorgeschlagenen Überweisung forderte sie die Täterin auf, über WhatsApp spontan ein Foto des Handys zu schicken, neben das sie als Echtheitsbeweis einen Löffel legen sollte. Als die Täterin nach Ausflüchten suchte, brach Nina P. die Verbindung ab.

Reingefallen – was nun?

Hat es Sie doch erwischt, kontaktieren Sie sofort Ihre Bank. Vielleicht besteht noch eine (Rest-)Chance, die Überweisung aufzuhalten. Erstatten Sie im nächsten Schritt Anzeige bei der Polizei. Zwar ist deren Chance gering, die Täter zu fassen; völlig ausgeschlossen ist dies aber nicht – und nur die Polizei kann organisierte Banden überhaupt aufspüren. Wenn Sie Ausweiskopien verschickt haben, erstatten Sie ebenfalls Anzeige: Zumindest weiß die Polizei dann in Verdachtsfällen, dass Ihre Identität wahrscheinlich von Dritten missbraucht wird.

Melden Sie dem Kleinanzeigenportal außerdem das betrügerisch genutzte Profil. Zwar dürften die Täter weitere in petto haben, aber zumindest dieses wird so hoffentlich gesperrt. Auch eine Website mit gestohlenen Daten und Copyrightverletzungen bei Bildern und Texten können Sie beim Hoster melden – ausschlaggebend ist der Nameserver, den Sie für .de-Domains mit dem WhoIs der DENIC (ct.de/yesb) finden. Jimdo versicherte uns auf Nachfrage, entsprechenden Meldungen zu prüfen und betrügerische Seiten samt der Nutzerkonten zu sperren. Kommen Sie nicht weiter, können Sie auch einen Anwalt beauftragen. Zudem lohnt es sich, die Bedingungen der Hausratversicherung zu prüfen. Manche zahlen auch bei Schäden durch Cyberkriminalität. *(mon@ct.de)* c't

Eine Website mit falschen Daten wie diese einer „Ferienhausvermietung“ ist leicht gebaut – und das Impressum keine Garantie für die Echtheit.

Keine Ausweiskopien verschicken

Schicken Sie niemals Fotos Ihres Ausweises an Unbekannte, auch nicht im „Gegenzug“ – die Gefahr eines Missbrauchs Ihrer Identität ist viel zu hoch und Sie geraten in Verdacht, wenn jemand Straftaten in Ihrem Namen begeht. Bedenken Sie auch: Sind die Fotos einmal im Netz, bekommen Sie diese dort nicht mehr heraus. Es gibt einige wenige Ausnahmen, in denen seriöse Dienstleister eine Kopie Ihres Ausweises benötigen, zum Beispiel zur Identitätsprüfung. Auch dann haben Sie mitunter Möglichkeiten, Teile des Dokuments zu schwärzen. Damit wollen wir uns in einem der nächsten Hefte beschäftigen.

Literatur

[1] Markus Montz, Ausgeplündert, Wie Betrüger „Sicher bezahlen“ auf eBay Kleinanzeigen aushebeln, c't 16/2022, S. 120
[2] Markus Montz, Schutzlos ausgeliefert, PayPal-Betrugsmaschen auf Kleinanzeigenportalen, c't 25/2020, S. 150

DENIC-WhoIs: ***ct.de/yesb***