c't

SICHER EINKAUFEN

Online-Shopping ohne Probleme

Schützen Sie sich vor Betrug

Bankkonten und Kreditkarten schützen
Sicheres Bezahlen auf Kleinanzeigenportalen

Digital bezahlen

PayPal, Giropay, Karte: Womit bezahlen?
Probleme im Ausland vermeiden

Kaufprobleme lösen

Erfolgreich reklamieren
Käuferschutz richtig einsetzen

Frustfrei shoppen

Die wichtigsten Regeln für den Onlinekauf
So machen Sie Schnäppchen ohne Reue
Datenschutzfreundliche Kundenkarten-Apps

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

4 195957 614908 03

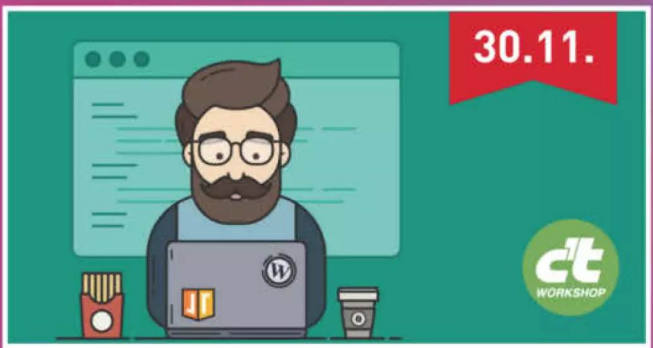
WIR TEILEN KEIN HALBWISSEN
WIR SCHAFFEN FACHWISSEN

ChatGPT und KI-Textwerkzeuge in der Praxis

Das c't-Webinar hilft Ihnen, die neue ChatGPT-Technik zu verstehen und ihren Einfluss auf Ihre Arbeit, Ihre Branche und Ihr Unternehmen einzuschätzen.

Wärmepumpentechnik für Einsteiger

Für Einsteiger: Erfahren Sie grundlegende Einführungen in umweltfreundliches Heizen. In zwei Stunden lernen Sie die Basics kennen und können anschließend Angebote für Ihre persönliche Situation prüfen.



WordPress für Einsteiger

Der praxisorientierte Workshop richtet sich an Neu- und Quereinsteiger in WordPress und bietet eine grundlegende und fundierte Einarbeitung in die aktuelle Version des populären CMS.

Kluge Strukturen für Microsoft 365 entwickeln

Lernen Sie in dem Workshop, wie Sie gemeinsam mit Ihrem Team Leitlinien entwickeln, um in Zukunft das volle Potenzial für die Zusammenarbeit auszuschöpfen.

Sichern Sie sich Ihren Frühbucher-Rabatt:

www.heise.de/ct/Events

Editorial

Liebe Leserinnen und Leser,

digital einkaufen und digital bezahlen gehören zum Alltag. Beides funktioniert bequem, günstig – und sicher. Das setzt jedoch Wissen voraus. Dieses Heft gibt Rat, damit Sie ohne Reue und doch günstig shoppen können, das optimale Zahlungsmittel wählen, im Zweifel Ihr Geld zurückbekommen und Cyberkriminellen nicht auf den Leim gehen.

Den Anfang macht die Einkaufsquelle. Vor allem in der Anonymität des Internets treiben sich viele dubiose Gestalten herum. Zwar können Sie sich auf bekannte Shops meist verlassen. Aber schon auf deren Marktplätzen treffen Sie auf zwielichtige Händler. Unseriöse Angebote lauern auch, wenn Sie mit Preisvergleichern und Schnäppchenportalen sparen wollen. Wir zeigen, wie Sie methodisch vorgehen und wo der Verdacht auf Preis- und Betrugsfallen sowie Datenschleudern angebracht ist.

Es folgt das (digitale) Bezahlen, von Rechnungskauf bis PayPal. Mögen Sie es datenarm? Oder muss es vor allem einfach und billig gehen? Geht alles zusammen und sicher dazu? Wir schaffen Orientierung und haben die drei neueren Trends Giropay, Debitkarte und Wallet genauer analysiert. So können Sie fundiert entscheiden, wie Sie bezahlen; im Laden, im Internet und nicht zuletzt im Ausland.

Doch nicht immer läuft der Kauf wie gedacht. Da hilft es, wenn Sie Ihre Optionen bei Reklamationen und Rückabwicklungen kennen – und wissen, welche Hebel Sie besitzen, wenn Händler, Privatverkäufer oder auch Käufer sich bei Kreditkarten- und PayPal-Zahlungen quer stellen. Ganz anderer Blues droht Ihnen beim Kauf auf Pump und anschließendem Ärger mit der Schufa. Informationen dazu finden Sie daher ebenfalls an dieser Stelle.

Shops und Privatverkäufer, die unter falscher Flagge im Netz segeln, erkennen Sie hingegen besser schon im Vorfeld. Wir haben im letzten Kapitel diverse Betrugsmaschen samt Gegenmaßnahmen zusammengetragen, damit die oft gut organisierten Banden dahinter Ihnen nicht Ihr Konto plündern, ohne jemals Ware liefern zu wollen.

In diesem Sinne wünschen wir Ihnen stets ein zufriedens „Halali“ für die Schnäppchenjagd und nachhaltige Freude an Ihren On- und Offlinekäufen!

Markus Montz

Inhalt

ONLINE EINKAUFEN

Im Internet finden Sie nahezu alles und können in Sekunden Preise vergleichen. Wir zeigen, wie Sie seriöse Shops aufspüren, die Rabattschlacht wohlinformiert führen – und mit digitalen Kundenkarten nicht zur Datenschleuder werden.

DIGITAL BEZAHLEN

Eine digitale Bezahlart wählen Sie im Spannungsfeld von Komfort, Datenschutz und Sicherheit aus. Nach einem Überblick stellen wir mit Debitkarten, Wallets und Giropay drei relativ neue Optionen vor und geben Tipps fürs Ausland.

KAUFPROBLEME LÖSEN

Nicht immer erfüllt ein Einkauf Ihre Erwartungen, manchmal kommt er auch gar nicht an. Wir erklären typischen Ärger, Ihre Rechte und wie Sie Ihr Geld zurückbekommen können – und wie Sie Nachwehen beim Kreditkauf und mit der Schufa vermeiden.

BETRUG VERHINDERN

Im Internet lauern organisierte Banden, die Sie mit raffinierten Maschen abziehen wollen. Wir stellen den „Fakeshop-Finder“ vor, erklären gängige Betrugsmaschen und -muster und was Sie bei Schäden am besten tun.

ZUM HEFT

Digital einkaufen, aber sicher!

Wo viel Geld zu holen ist, sind auch Abzocker und Betrüger nicht weit. In unseren Checklisten zum Onlinekauf zeigen wir, wie Sie Fake Shops meiden, echte Schnäppchen von Lockangeboten unterscheiden, sicher bezahlen und richtig reagieren, falls der Einkauf im Internet schiefläuft.

Von **Ulrike Kuhlmann**

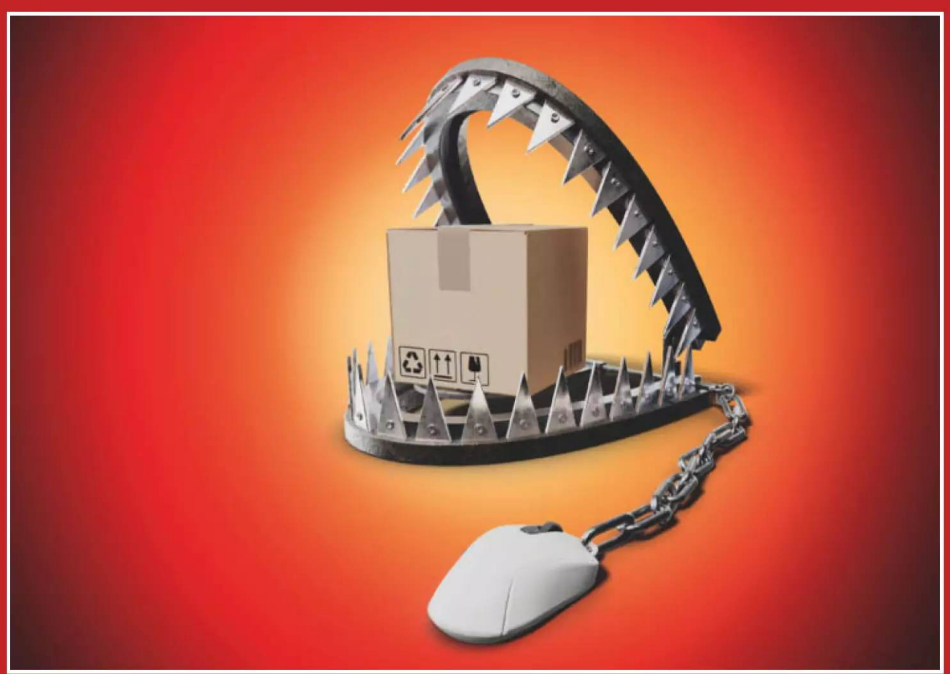


Bild: Andreas Martini

Ein neues Gadget muss her, flugs im Internet gesucht, Superangebot gefunden, ein Klick und schon am nächsten Tag steht der Paketbote mit dem Wunschgerät vor der Tür. Wenn alles gut geht. Oder eben nicht: Das Gerät ist defekt, der Anbieter verschwunden, das Geld futsch.

Der Online-Shopping-Boom der letzten Jahre rief noch mehr Betrüger auf den Plan als zuvor. Die wollen Ihre Daten, Ihr Geld und am liebsten den direkten Zugriff auf Ihr Konto. Selbst versierte Internetkäufer fallen auf die immer raffinierteren Maschen herein. Da werden Fake Shops hochgezogen, wertlose Waren verschickt und mit gekauften Bewertungen und Scheinangeboten manipuliert. Mit unseren Checklisten für den Onlinekauf schaffen Sie es, Fakten von Fakes zu unterscheiden und Fallstricke zu umgehen. Und falls doch mal etwas schiefgeht, zeigen wir Ihnen, wie Sie trotzdem zu Ihrem Recht kommen.

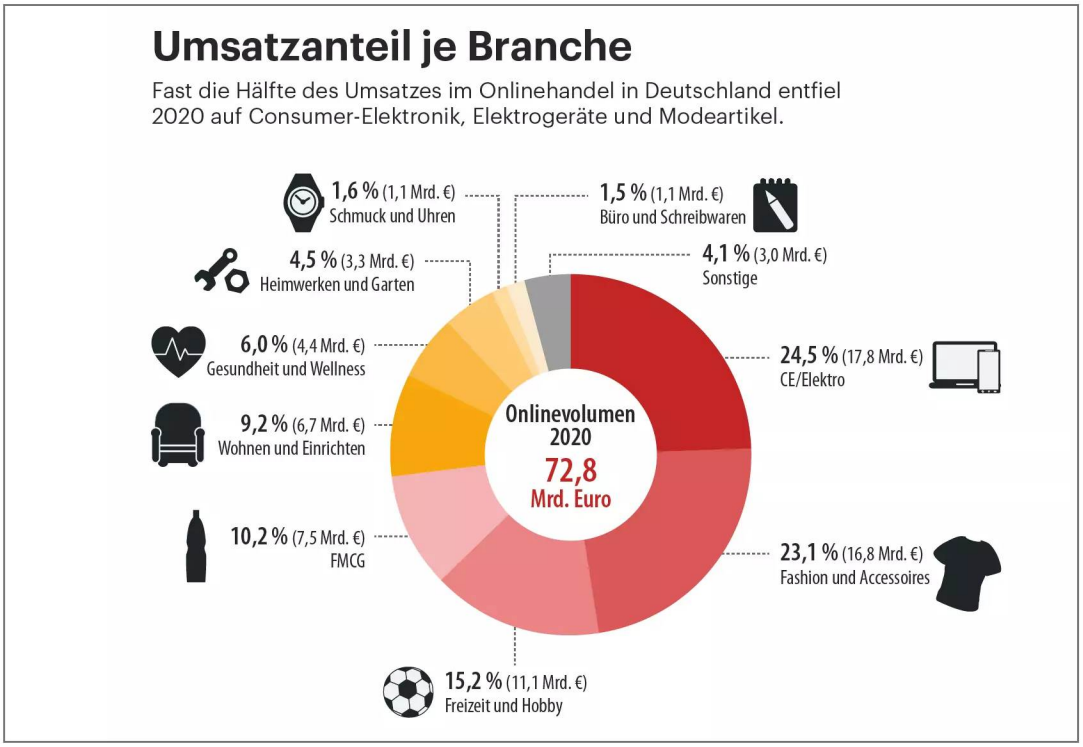
Fake Shops erkennen

Bevor Sie selbst den enormen Umsatz der Onlineanbieter mit einem Klick auf „Kaufen“ weiter in die Höhe treiben, halten Sie besser kurz inne und prüfen, bei wem Sie gerade supergünstig einkaufen wollten. Es gibt betrügerische Shops, die beliebte Ware zum Schnäppchenpreis anbieten, aber nicht beabsichtigen, diese zu liefern. Bei extrem günstigen Angeboten sollten Sie hellhörig werden. Wie Sie gefährliche Fake Shops erkennen und worauf Sie bei der Händlerwahl unbedingt achten sollten, erfahren Sie in unserer Checkliste zur Shop-Auswahl im Artikel „Onlinekauf-Checkliste Shop-Auswahl“ ab Seite 14.

Mehr als die Hälfte der Kunden verlassen sich beim Onlinekauf nach eigenen Angaben auf die Bewertungen anderer Kunden. Das ist nicht ungefährlich, denn solche Bewertungen sind häufig gefälscht. Zudem handelt es sich bei den nach vorn gestellten Kritiken zuweilen um eine Sammlung der besten Bewertungen, die nicht zwingend repräsentativ ist. Hier empfiehlt sich ein kritischer Blick auf die Gesamtzahl der Bewertungen und gerade auch auf die schlechteren Beurteilungen.

Den besten Preis finden

Um die besten Angebote zu finden, nutzen die Hälfte der Onlinekäufer Preisvergleichsseiten. Diese listen



Quelle: Bitkom/Statista

etliche Shops mit den günstigsten Preisen für das gewählte Produkt auf. Allerdings enthalten die präsentierten Ergebnisse womöglich gekaufte Platzierungen, zeigen nicht die Gesamtkosten oder lassen bestimmte Händler außen vor. Was Sie sonst noch über solche Vergleichsportale wissen müssen, fasst unsere Checkliste im Artikel „Onlinekauf-Checkliste Preisvergleich“ ab Seite 10 zusammen.

Wer richtig günstig einkaufen will, nutzt Schnäppchenportale. Wie Sie hier gute Deals finden und vor allem schlechte erkennen und was von Cashback, Gutschein-Codes oder Bonusprogrammen zu halten ist, bringt unsere Schnäppchen-Checkliste im Artikel „Onlinekauf-Checkliste Schnäppchenportale“ ab Seite 12 kompakt auf den Punkt.

Mobil kaufen und bezahlen

Schon 2018 gaben 50 Prozent der Onlinekäufer in einer Bitkom-Studie an, mit dem Smartphone einzukaufen. 2021 waren es bereits 60 Prozent – das Smartphone hat damit erstmals das Notebook (57 %) und erst recht den Desktop-PC (38 %) abgehängt.

Wohl auch deshalb gehörten Online-Bezahldienste wie PayPal zu den bevorzugten Zahlungsarten in Deutschland. Gern wird hierzulande aber auch auf Rechnung gekauft oder per Lastschrift bezahlt. Welche Zahlarten sich für welche Kaufverträge empfehlen, welche sich gegebenenfalls leicht rückgängig machen lassen und worauf Sie beim Bezahlvorgang im Internet unbedingt achten sollten, erfahren Sie in unserer Checkliste zu Bezahlverfahren im Artikel „Onlinekauf-Checkliste Bezahlmethoden“ ab Seite 24.

Reklamieren oder rückabwickeln

Zu den wichtigsten Kriterien für die Shop-Auswahl gehören für Onlinekäufer laut einer Bitkom-Umfrage der günstigste Preis (64 %) und die versandkostenfreie Lieferung (56 %). Das birgt die Gefahr, vor lauter Freude über das Superschnäppchen das Kleingedruckte zur Versandabwicklung zu überlesen. Kommt es dann zum Lieferverzug, ist die Ware unvollständig, defekt oder liegt gar ein falsches Produkt im Paket, gilt es, schnell und richtig zu handeln. In unserer Checkliste zu Versand und Reklamation beim Onlinekauf im Artikel „Onlinekauf-Checkliste Reklamation“ ab Seite 66 finden Sie konkrete Handlungsempfehlungen.

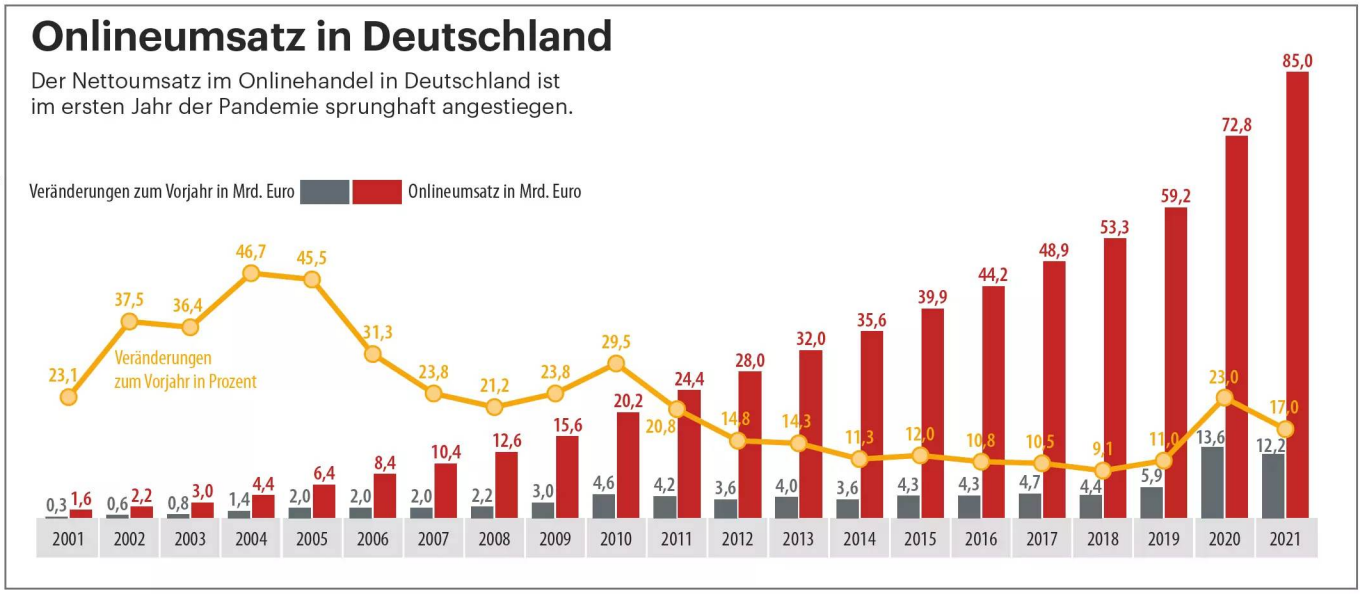
Ein aus Pandemiezeiten bekanntes Vehikel ist Click & Collect: Die Ware wird im Internet bestellt und anschließend vom Kunden im Laden abgeholt. Für diesen zustellungsfreien Onlineverkauf gelten spezielle Regeln – welche das sind, steht ebenfalls in der Reklamationen-Checkliste. Und wer Ware im Ausland bestellt, sollte unbedingt einige Grundregeln zu Zollgebühren, Einfuhrumsatzsteuer oder Servicepauschalen kennen.

Falls gar nichts mehr geht und Sie Ihren Onlinekauf komplett rückabwickeln möchten, stellen sich wichtige Fragen: Kann ich den Kaufvertrag einfach widerrufen, wann darf ich die Zahlung stoppen, was bringt der Käuferschutz und wer trägt eigentlich die Kosten für den Rückversand? Antworten liefert

Tipps für Konsumenten

Unsere Checklisten richten sich an Verbraucher, die im Onlinehandel Waren von Unternehmen beziehen (Business to Consumer, B2C). Gerade im Onlinehandel gelten im Rahmen des Fernabsatzgesetzes diverse Verbraucherschutzregeln, die Verkäufer nicht umgehen dürfen. Auf diese Regeln stützen sich unsere Tipps.

B2B-Verträge zwischen Unternehmen lassen wir bewusst außen vor, denn Firmen untereinander können Verträge deutlich freier aushandeln. Ähnliches gilt für Verkäufe unter Privatleuten.



unsere Checkliste zur Rückabwicklung von Onlinekäufen im Artikel „Onlinekauf-Checkliste Rückabwicklung“ ab Seite 70.

Beliebte Einkaufsmeilen

Die Deutschen shoppen übrigens am liebsten bei Amazon: Der Marktführer im E-Commerce hält hierzulande einen Umsatzanteil von über 50 Prozent. Aber auch stationäre Händler verkaufen online, fast die Hälfte ist inzwischen im Internet vertreten. Das ist folgerichtig, denn der Umsatz im Onlinehandel wächst seit Jahren: Von 1,6 Milliarden Euro im Jahr 2001 stieg er innerhalb von zwanzig Jahren auf stolze 85 Milliarden Euro.

Consumer-Elektronik (CE) und Elektrogeräte sowie Kleidung und Modeartikel lagen in der Gunst der Onlinekäufer weit vorn. Die Elektronikbranche war mit einem Zuwachs von 3,5 Milliarden Euro zugleich der größte Umsatztreiber und erzielte mit Fernsehern, Smartphones und Kleingeräten ähnlich wie die Modebranche fast 40 Prozent ihres Umsatzes online.

Zukunft des Onlinekaufs

Klar, der Zuwachs im Onlinehandel war in den letzten Jahren pandemiegetrieben. Die meisten Kunden wollen aber auch künftig einen Teil ihrer Einkäufe im Internet erledigen – auch die zumeist älteren Erstkäufer. Laut einer Umfrage des Handelsverbands Deutschland (HDE) wollen zwei Drittel derjenigen, die ab 2020 erstmals online shoppen waren, Artikel aus den Bereichen Mode, Gesundheit und Consumer-Elektronik weiterhin im Internet kaufen.

Besonders häufig und besonders viel online kauft in Deutschland die Altersgruppe zwischen 30 und 49 Jahren: Sie gab 2021 pro Kopf monatlich 266 Euro beim Onlineshopping aus. Die über 60-Jährigen beließen es bei 114 Euro pro Kopf und Monat, im gesamtdeutschen Mittel waren es 207 Euro. Männer gaben mit durchschnittlich 230 Euro monatlich 50 Euro mehr aus als Frauen.

Laut einer Studie des Bitkom werden in Deutschland allerdings 11 Prozent aller Onlinekäufe schnell wieder zurückgeschickt. Dabei wurden Waren teilweise bereits in dem Wissen bestellt, sie wieder zu retournieren – etwa, weil ein Kleidungsstück nicht passt oder weil nur ein Teil aus einer Auswahl tatsächlich übernommen werden soll. 56 Prozent der jüngeren Einkäufer bis 49 Jahre gaben an, bestellte Ware hin und wieder zurückzuschicken. Die Retourenquote unter den über 50-Jährigen ist deutlich niedriger; über alle Altersgruppen gemittelt behaupten 83 Prozent, selten oder nie etwas zurückzuschicken. Für die Umwelt wäre das zweifellos besser. (uk) c't

Bild: Andreas Martini

Onlinekauf-Checkliste Preisvergleich

Preisvergleichsdienste im Netz kennen die besten Angebote für viele Produkte. Allerdings drohen Fallstricke bei der Suche. Mit unserer Checkliste landen Sie zuverlässig beim günstigsten Preis.

Von **Jo Bager**

Preisvergleicher auswählen

Welcher Preisvergleichsdienst die besten Angebote liefert, lässt sich immer nur zeitlich begrenzt bestimmen. Tests heben zwar immer mal wieder einzelne von ihnen hervor. Allerdings liefert kein Preisvergleicher für alle Produkte und Produktkategorien zu jeder Zeit die besten Ergebnisse, weil kein Dienst jeden Shop anzeigt und mitunter sogar die großen wie Amazon fehlen. Sicherheitshalber bleibt Ihnen also nichts anderes übrig, als die Preise der Preisvergleicher zu vergleichen.

Amazon betreibt einen Marktplatz, den viele Verbraucher für eine schnelle Preisrecherche nutzen. Preisvergleicher, die Marktplätze berücksichtigen, liefern oft bessere, auf keinen Fall aber schlechtere Angebote, weil sie die Angebote etwa von Amazon in ihre Suche einbeziehen.

Auf exakte Produktnamen achten

Einige Hersteller von PC-Teilen und Elektrogeräten sind sehr kreativ darin, schnell neue Geräte mit ähnlich klingenden Namen, aber unterschiedlicher Ausstattung auf den Markt zu werfen. Achten Sie also auf den genauen, vollständigen Namen. Ein paar zusätzliche, weggelassene oder vertauschte Buchstaben können für ein völlig anderes Produkt stehen. Informieren Sie sich im Zweifelsfall auf der Homepage des Herstellers über die exakte Bezeichnung.

Begriffe wie Refurbished, Recertified oder auch Pullware bezeichnen gebrauchte und wiederaufbereitete beziehungsweise geprüfte Teile, für die kürzere Gewährleistungsfristen gelten können. Sicherheitshalber sollten Sie im Shop des Anbieters vor dem Kauf überprüfen, ob Ihr Treffer auch genau dem Produkt entspricht, das Sie eigentlich suchen.

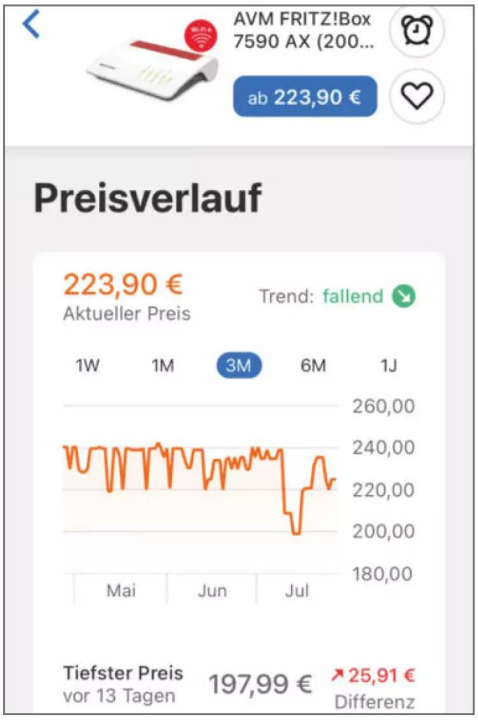
Trefferliste sortieren und filtern

Per Default sortieren viele Preisvergleicher nach dem Produktpreis. Aber Vorsicht: In einem früheren c't-Test hatte ein Preisvergleicher einen festen Platz der Angebotsliste für Produkte eines bestimmten Marktplatzes reserviert, unabhängig vom Preis. Man kann die Angebote auch nach dem Gesamtpreis inklusive der Versandkosten sortieren lassen. Ebenfalls praktisch: Einige Preisvergleicher können nach Angeboten filtern, die sofort lieferbar sind.

Händler und Angebot überprüfen

Mitunter befinden sich unbekannte Händler unter den günstigsten Anbietern. Das liegt daran, dass kleine Anbieter manchmal nur eine Handvoll Produkte besonders günstig einstellen, um neue Kunden zu gewinnen. Ob so ein Händler zuverlässig ist, darauf geben die Shop-Bewertungen bei den Preisvergleichern Hinweise. Aber Obacht: Unter den Bewertungen könnten sich auch gekaufte befinden; mehr dazu im Artikel „Digital einkaufen, aber sicher!“ auf Seite 6.

Manche Dienste listen nur Produkte von ausgewählten Shops. Daher sollte es dort kein Problem mit Fake Shops geben. Seien Sie bei Marktplatz-Anbietern aber vorsichtig. Bei Google Shopping kann jeder spezielle Anzeigen schalten, die in den Shopping-Ergebnissen landen. Das Verbraucherportal Finanztip.de fand bei früheren Recherchen einen Fake Shop unter den Ergebnissen. Seien Sie außerdem vorsichtig bei Treffern von Privatverkäufern auf eBay, für die andere Gewährleistungspflichten gelten als für den Kauf bei einem Händler.



Ist der aktuelle Preis gut oder wartet man lieber? Preisverläufe wie bei Idealo geben Hinweise.

Den richtigen Moment abwarten

Es kann vorkommen, dass ein Produkt kurzfristig sehr günstig ist, danach aber der Preis wieder steigt. Manche Dienste zeigen die Preisentwicklung in einer Grafik an. Das liefert Hinweise darauf, ob die Gelegenheit günstig ist, oder ob man noch etwas warten sollte. Sie können sich auch mit Preisalarmen per E-Mail informieren lassen, wenn der Preis eine bestimmte Schwelle unterschreitet. (jo) c't

Bild: Andreas Martini

Onlinekauf-Checkliste Schnäppchenportale

Sonderangebote, Cashback, Gutscheine: Im Netz können Sie so manchen Euro sparen – wenn Sie wissen, wo. Bei der Schnäppchenjagd lauern allerdings auch Fallen.

Von **Jo Bager**

Preiskracher-Portale

Überall im Netz günstige Angebote aufzuspüren und aufzulisten ist die Spezialität von Portalen wie mydealz und Dealdoktor. Wer auf konkrete Angebote für ein bestimmtes Produkt wartet, kann sich bei mydealz auch einen Deal-Alarm einrichten.

Bei den Deals des Verbraucherportals Finanztip gibt es viele von der Redaktion geprüfte Schnäppchen. Der Preisvergleicher Idealo weist auf seiner Startseite auf Produkte hin, die vor kurzem deutlich im Preis gefallen sind. TagesAngebote.de und liveshopping-aktuell.de listen zeitlich beschränkt verfügbare Angebote. Dazu zählen auch Amazons Blitzangebote.

Outlets im Browser

Online-Shopping-Clubs offerieren Hunderte bis Tausende Markenprodukte zu stark reduzierten Preisen, aber nur für kurze Zeit. Veepee, BestSecret, Lounge by Zalando, limango und brands4friends sind die bekanntesten Vertreter dieser Zunft. Dort müssen Sie allerdings unter Umständen Lieferzeiten von zwei bis vier Wochen in Kauf nehmen, da die Clubs die Bestellungen zunächst sammeln und erst dann beim Hersteller ordern.

Gutscheine, Newsletter, Apps

Die Welt der Gutscheine ist unübersichtlich. Portale wie Gutscheinpony, sparwelt.de oder mydealz.de geben einen Überblick. Die meisten Angebote dort entsprechen denen auf den Homepages der Anbieter. Nach einem Online-Kauf sollten Sie aber die Augen offen halten: Viele Online-Händler sind in Empfehlungsnetzwerke eingebunden und bieten nach dem Kauf eine Belohnung in Form von Gutscheinen an.

Wer regelmäßig bei bestimmten Supermarktketten einkauft, für den kann es sich lohnen, die jeweilige App zu installieren. Rossmann zum Beispiel versucht Kunden mit Coupons in die Filialen zu locken. 10 Prozent Rabatt auf den gesamten Warenwert sind eigentlich immer drin. Auch Markenhersteller bemühen sich darum, einen direkten Draht zu ihren Kunden herzustellen. Dazu setzen sie zum Beispiel auf E-Mail-Newsletter, in denen sie regelmäßig Rabattaktionen bewerben. Egal, ob Coupon oder Newsletter-Rabatt: Sie erkaufen die Preisnachlässe mit ihren Daten. Der Supermarkt erfährt, wann und was Sie einkaufen, der Markenhersteller, auf welche Links Sie in den Newslettern klicken, für welche Produkte Sie sich also interessieren.

Den Preis drücken

In etlichen Online-Shops erhalten Sie Rückvergütungen, neudeutsch: Cashback. Neben den aus der Offline-Welt bekannten Anbietern Payback und Deutschlandcard gibt es viele weitere, zum Beispiel Shoop.de, Getmore, linkomat und Andasa. Die Provisionen belaufen sich auf bis zu zweistellige Prozentwerte des Einkaufsvolumens, manchmal springen auch Gutscheine von ein paar Euro heraus. Einige Cashback-Anbieter überweisen das Guthaben erst nach einigen Wochen bis Monaten auf das Konto.

Links zu allen erwähnten Diensten
ct.de/w5sg

Vorsicht bei permanentem Zeitdruck und vermeintlich guten Preisen, zum Beispiel bei der Auktionsplattform Snipster. Tatsächlich hat die Plattform für diese Tasche bereits mehr als 700 Euro eingesammelt.

Vorsicht vor Psycho-Tricks

Bei vielen Schnäppchen liegt ein wenig Zeitdruck in der Natur der Sache – was weg ist, ist weg. Dennoch sollten Sie sich immer die Zeit nehmen, ein vermeintliches Schnäppchen mit einem der Preisvergleicher gegenzuchecken (siehe Artikel „Onlinekauf-Checkliste Preisvergleich“ auf S. 10). Manche Dienste nutzen solchen gar nicht mal subtilen Druck auch, um Besucher bei der Stange zu halten. Bei „Countdown“-Auktionsplattformen ohne feste Endzeiten wie Snipster etwa erscheinen die Preise sehr niedrig, weil sie pro Gebot nur um einen Cent steigen. Allerdings kostet ein Gebot 50 Cent und verlängert den Auktionszeitraum. So werden die vermeintlichen Schnäppchenjäger permanent in einem Bieterwettstreit gehalten – den aber nur einer gewinnen kann.

Mit solchen Dark Patterns versuchen Websites, ihre Umsätze zu steigern, indem sie Verbraucher zu Handlungen verleiten, die deren Interessen widersprechen. So werden schon mal unaufgefordert Produkte in den Warenkorb gelegt oder relevante Informationen versteckt. Insbesondere auf Plattformen, die Sie nicht kennen, sollten Sie daher aufmerksam sein. Beim Dark Pattern Detection Project können Sie sich über Dark Patterns informieren.

(jo) c't

Bild: Andreas Martini

Onlinekauf-Checkliste Shop-Auswahl

Sicher oder günstig, das sind die Extrempole beim Onlineshopping. Beides birgt Risiken: Wer alles beim gleichen Shop einkauft, zahlt oft zu viel. Wer stets zum günstigsten Angebot greift, riskiert, in Fallen zu tappen. Wir zeigen, wie Sie online einkaufen, ohne hereinzufallen.

Von **Georg Schnurer**

Mein Kumpel Axel geht beim Online-Einkauf auf Nummer sicher: Er ist Prime-Mitglied bei Amazon und kauft dort alles. Gefällt ihm ein Produkt mal nicht, kann er es problemlos zurückschicken. Angst vor Betrügern oder mangelhafter Ware braucht er nicht zu haben. Andere Onlineshops bieten die Waren allerdings oft günstiger an.

Paul ist ein ganz anderer Shopping-Typ: Er sucht stets das günstigste Angebot. Mit Google, diversen Preisvergleichsportalen und Empfehlungen aus Social-Media durchforstet er das Internet und entscheidet sich für den günstigsten Shop. So kauft er immer wieder bei anderen Händlern ein und spart – wenn alles gut geht – eine Menge Geld.

Allerdings hat die wilde Schnäppchenjagd auch ihre Schattenseiten, denn Betrüger haben längst erkannt, dass Online-Shopper im Jagdfieber leichte Opfer sind. So wundert es kaum, dass Paul auch viel Zeit und Energie in Reklamationen und andere Streitereien mit den stets wechselnden Lieferanten investiert.

Zu schön, um wahr zu sein

Zwischen den Shopping-Verhalten von Axel und Paul gibt es einen goldenen Mittelweg. Die wichtigste Grundregel lautet dabei: Wenn ein Angebot zu gut ist, um echt zu sein, ist es das in der Regel auch nicht. Bietet ein Shop ein Produkt sehr viel günstiger als die Konkurrenz an, kann irgendetwas nicht stimmen.

Was da nicht stimmt, ist allerdings auch für erfahrene Onlinekäufer nicht immer leicht zu erkennen. Die Zeiten, als man Fakes schon an den Schreibfehlern in den Produktbeschreibungen, fehlendem Impressum oder ungültiger Handelsregisternummer erkennen konnte, sind längst vorbei. Die Betrüger kopieren inzwischen komplette Angebote und Webseiten seriöser Anbieter, nebst Impressum, Gütesiegeln und so weiter. Schon länger aktive Fake Shops entlarven Sie dennoch recht zuverlässig mit einer Google-Suche nach dem Shopnamen nebst den Stichwörtern „Betrug“ und „Fake“. Da die Betrüger aber immer wieder neue Fake Shops aus dem Hut zaubern, ist das kein zuverlässiges Mittel.

Damit der Schnäppchenjäger nicht zu viel Zeit für Recherchen aufwendet, erhöhen die Anbieter gezielt den Druck auf den Käufer: Mal ist plötzlich nur noch ein Produkt zum Superpreis auf Lager, mal läuft der Zähler für die verfügbaren Schnäppchen langsam ab oder das Angebot gilt nur für einen engen Zeitraum. Beliebt sind hier auch zeitlich begrenzte Eröffnungs- oder Einführungsangebote.

Von solchen – leider auch bei so manchem seriösen Shop üblichen – Drängeleien sollten Sie sich nicht unter Druck setzen lassen. Suchen Sie vor dem Kauf gründlich und in Ruhe nach Fallen. Erster Warnhinweis ist der eingangs genannte zu günstige Preis. Bietet der Shop ausschließlich „Vorkasse“ als Bezahlmethode an, ist Alarmstufe Rot. Wer hier vorab bezahlt, ist sein Geld los. Tückisch ist auch PayPal als Zahlmethode bei eBay. Sie sollten für Onlinekäufe keinesfalls die sogenannten „Zahlungen an Freunde“ verwenden. Diese PayPal-Variante bietet nämlich keinerlei Käuferschutz – mehr zum sicheren Bezahlen im Artikel „Onlinekauf-Checkliste Bezahlmethoden“ ab Seite 24.

Ganz raffinierte Betrüger bieten auf den ersten Blick neben Vorkasse weitere Bezahlmethoden an. Versucht man dann, etwa Kauf auf Rechnung, Last-

„Bezahlung per PayPal als Freund“ – ein klarer Hinweis auf eine Falle. Hier sind es gefälschte Apple-Lautsprecher.

Shopping-Regeln

Wer die folgenden Regeln beachtet, kann günstig, aber dennoch sicher einkaufen:

- Fake Shops erkennen und meiden: Ist ein Angebot unverschämt billig und bietet der Händler ausschließlich Vorkasse an, müssen die Alarmglocken laut schrillen.
- Gebrauchtware und kastrierte Produkte erkennen: Nur wer die Produktbeschreibung sorgfältig studiert, schützt sich vor ärgerlichen Reinfällen.
- Sichere Bezahlvariante wählen: Sie sollten nur in Ausnahmefällen per Vorkasse zahlen. Diesen Vertrauensvorschuss haben nur Händler verdient, die Sie bereits genutzt und als zuverlässig eingestuft haben.
- Immer die Gesamtkosten beachten: Versteckte Kosten, etwa für den Versand oder die Zahlungsabwicklung, können aus einem Schnäppchen schon mal einen teuren Reinfall machen.
- Lieferzeiten prüfen: Gibt der Händler keine klaren Lieferzeiten an oder hält er sich hier mit schwammigen Formulierungen bedeckt? „Lieferung üblicherweise in 1–2 Tagen“ ist keine feste Zusage! Nachfragen vor dem Kauf schützt hier vor Überraschungen.
- Vorsicht bei Angeboten auf Social Media: Verkäufer sind keine Freunde! Prüfen Sie Angebote genau und vergleichen Sie die Preise. Nur weil da jemand „Schnäppchen“ brüllt, muss das noch lange kein attraktives Angebot sein.

schrift oder Kreditkartenzahlung zu wählen, lassen sich diese Optionen nicht aktivieren. In solchen Fällen sollten Sie den Kauf abbrechen.

Gebrauchtes statt Neues

Bei auffällig günstigen Angeboten sollten Sie prüfen, ob Sie wirklich Neuware erwerben. Mancher Händler versucht, Widerrufsware oder reklamierte Produkte weiterzuverkaufen, ohne deutlich darauf hinzuweisen, dass es sich hier um gebrauchte Ware handelt. Irgendwo steht dann zwar, dass es „neuwertige“ Produkte sind, aber neuwertig ist halt nicht neu!

Beliebt sind auch Angebote mit leicht abgewandelten Produktbezeichnungen. Oft verbergen sich hinter kleinen Abweichungen in der Typenbezeichnung abgespeckte oder nur eingeschränkt nutzbare Produkte. Hier schützt ein Vergleich mit der Produktbeschreibung auf der Herstellerwebseite vor ärgerlichen Reinfällen.

Ein besonders lukratives Umfeld für Betrüger sind Shopping-Angebote in sozialen Netzwerken. Da viele Nutzer hier mehr Vertrauen in vermeintlich neutrale Empfehlungen von „Freunden“ haben, werden solche Plattformen gern mit vermeintlichen Schnäppchenangeboten geflutet.

Mal verweisen diese Angebote auf Fake Shops, mal bieten die Bauernfänger dort minderwertige Waren mit allzu verlockenden Beschreibungen und geschönten Fotos an. Kommt nach dem Kauf tatsächlich etwas an, entpuppt sich die Ware häufig als Billigprodukt von minderwertiger Qualität. Eine Reklamation (siehe auch Artikel „Onlinekauf-Checkliste Reklamation“ ab S. 66) ist oft nicht möglich, weil der Anbieter plötzlich im EU-Ausland sitzt oder als Vermittler auftritt. Mitunter ist der Verkäufer nach dem Kauf auch einfach nicht mehr zu erreichen.

Auch im vermeintlich sicheren Hafen von Amazon tummeln sich Betrüger. Um die Schutzmechanismen von Amazon zu umgehen, versuchen diese, den Käufer zur Zahlung außerhalb des Amazon-Zahlungssystems zu drängen. Lassen Sie sich nicht darauf ein und melden Sie solche Angebote möglichst sofort bei Amazon. Die Plattform entfernt unseriöse Offerten in der Regel recht schnell und sperrt die Händler. Leider dauert es meist nur wenige Tage, bis ähnliche Angebote wieder auf der Plattform auftauchen. Hase und Igel lassen grüßen.

eBay-Käuferschutz

Die am häufigsten anzutreffende Betrugsmasche bei eBay sind Produktfälschungen. Zwar bietet eBay

ähnlich wie Amazon ein Käuferschutzsystem, doch das greift nur, wenn die Bezahlung über eBay abgewickelt wird. Deshalb drängeln betrügerische Verkäufer auch hier mitunter zur direkten Zahlung per Vorkasse oder per PayPal-Freundschaftsüberweisung. In beiden Fällen gibt es keinen Käuferschutz, also Finger weg!

Doch auch wer die vermeintlich sichere Zahlung über das Bezahlsystem von eBay wählt, kann nach Erhalt mangelhafter oder gefälschter Ware noch im Regen stehen. Der eBay-Käuferschutz setzt nämlich voraus, dass die Ware nachweislich an den Händler zurückgesendet wurde. Sitzt der etwa in China, können die Rücksendekosten schnell die von eBay zu erwartende Erstattung auffressen. Hier haben manche Händler vor allem aus China ein perfides System entwickelt, um zu verschleiern, wo der tatsächliche Firmensitz ist. Da wird mit „Versand aus Deutschland“ und „Artikelstandort: Hamburg“ geworben und nur wer sich bis zum eBay-Impressum des Händlers durchklickt, erfährt, dass er im Begriff ist, mit einem Händler aus dem EU-Ausland Geschäfte zu machen. EU-Käuferschutzregeln gelten dann nicht und Sie sind bei Problemen auf die Kulanz des Händlers und der Plattform angewiesen.

China-Shopping

Gerade Elektronikkomponenten oder ähnlichen Bastelbedarf bekommt man über Plattformen wie Aliexpress inzwischen recht komfortabel. Da die Plattform mittlerweile beim Versand nach Deutschland eine Verzollung gemäß den neuen EU-Regeln vornimmt, sind Sie weitestgehend vor Überraschungen in Form von unerwarteten Abgaben verschont. Alipay arbeitet bei Käufen aus Deutschland neuerdings mit Klarna zusammen. Damit können Kunden aus Deutschland nicht nur per Kreditkarte zahlen, sondern auch auf Rechnung einkaufen. Nach Erhalt der Ware können sie diese so in Ruhe prüfen und dann die Zahlung via Klarna veranlassen.

Ganz frei von Fallstricken ist der Kauf bei Aliexpress damit freilich nicht: Viele Händler bieten dort zwar auf den ersten Blick sehr günstige Produkte an, doch oft kommen teils recht hohe Versandkosten hinzu. Anders als etwa bei Amazon oder eBay summieren sich die Versandkosten aber bei Aliexpress, selbst wenn Sie mehrere Produkte beim gleichen Händler ordern. Hier gilt es also, stets den Gesamtpreis – also Warenpreis plus Versandkosten – im Auge zu behalten.

Diesen Gesamtpreis vergleichen Sie dann am besten mit dem, was Sie in deutschen Shops für das gleiche oder ein ähnliches Produkt bezahlen müssten. Ist der Unterschied nicht signifikant, lohnt der Kauf in China kaum, denn bis Sie die Ware letztlich in Händen halten, vergehen schon mal mehrere Wochen oder gar Monate. Zudem ist eine Reklamation hier komplizierter, vor allem wenn die Gerätschaften erst nach einiger Zeit Fehler aufweisen. (gs) c't

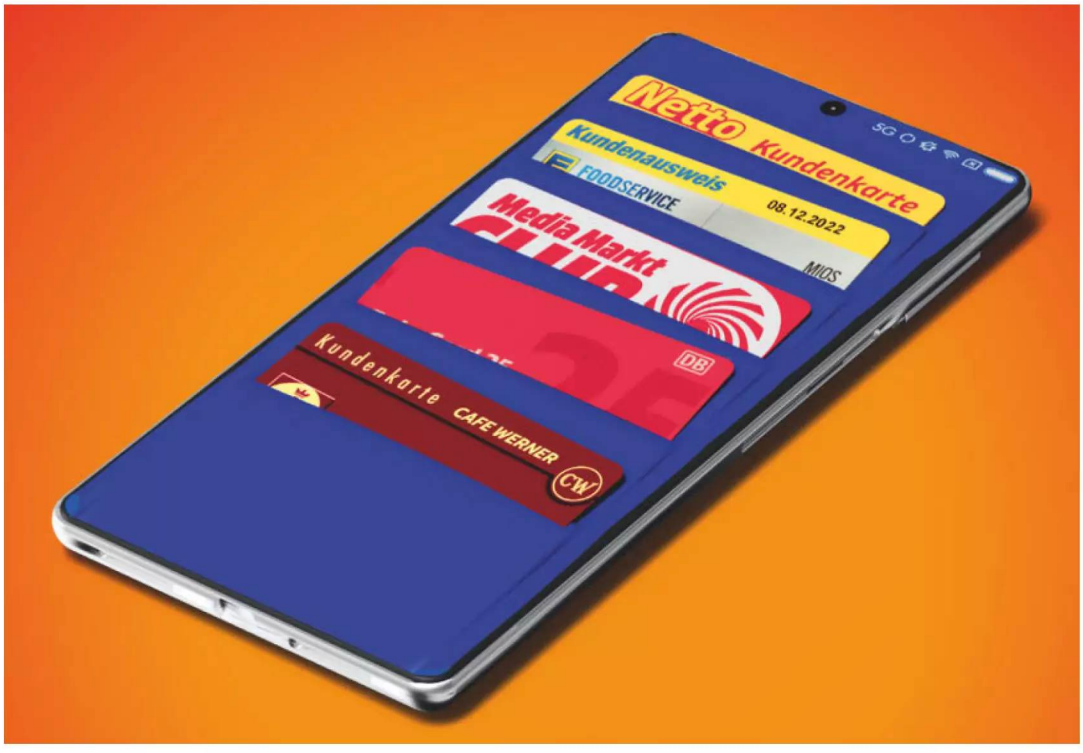


Bild: Andreas Martini

Kundenkarten via App digitalisieren

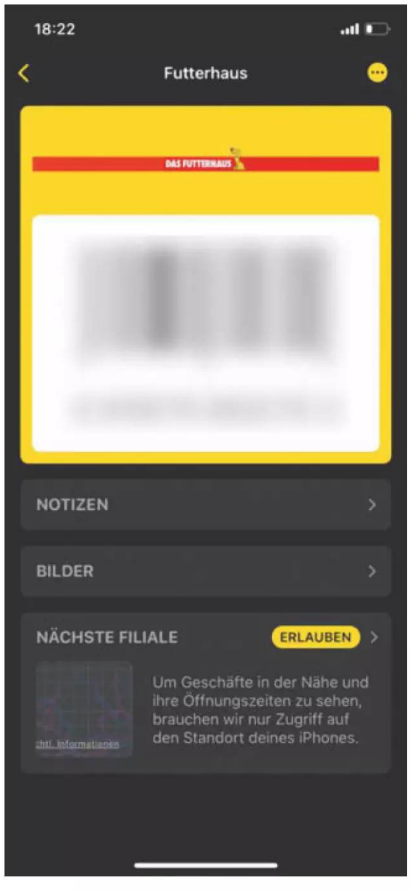
Nichts füllt ein Portemonnaie so schnell auf wie Kundenkarten. Mithilfe von Apps können Sie diese bequem digitalisieren, doch Vorsicht: Manche bereichern sich an Ihren Daten, daher stellen wir datenschutzfreundliche Alternativen vor.

Von **Wilhelm Drehling**

Möchten Sie eine Kundenkarte haben? – der Rabatt beim Einkauf wäre schon schön. Ein schneller Blick ins Portemonnaie verheißt jedoch nichts Gutes: Schon jetzt dehnt sich das Leder gefährlich über die Plastikkarten. Eine Zerreißprobe bahnt sich an – vielleicht passt ja oben noch eine rein oder ganz hinten, drei Karten in einem Fach sind doch machbar. Jede neue Karte könnte die letzte Stunde des Portemonnaies einläuten.

Auch wenn die meisten Geldbörsen deswegen nicht gleich zerreißen, stört es im Alltag schon gewaltig, wenn sich zu viele Kundenkarten ansam-

meln. Abhilfe schaffen Apps, die diese digitalisieren. Sie funktionieren alle ähnlich: Man scannt den Barcode oder nimmt ein Foto der Karte auf, vergibt anschließend einen Namen und speichert die virtuelle Karte ab. Manche der Apps setzen noch eins drauf, indem sie ein Logo oder den Firmenschriftzug automatisiert dazulegen. Die digitalen Karten liegen dann innerhalb der App bereit zum Abruf. Beim nächsten Einkauf holen Sie nur noch das Handy heraus, wählen die korrekte Karte aus und zeigen den Barcode beziehungsweise das Foto auf dem Bildschirm vor.



Kundenkarten-Apps wie Stocard kommen geschickt an Nutzerdaten heran: Kurz mal die Öffnungszeiten checken und (zack!) gibt man seine Standortdaten ab.

Sieht man sich die Ranglisten der beliebtesten Kundenkarten-Apps genauer an, tauchen meistens die gleichen Namen ganz oben auf. Häufig sind das Apps, die viele Funktionen enthalten, mit digitalen Bezahlmöglichkeiten gekoppelt sind und allerhand Anpassungsmöglichkeiten anbieten. Viele davon schalten aber Werbung, sammeln Daten und verdienen sich damit eine goldene Nase. Für die Nutzer ist das meist kein sonderlich guter Deal.

Kundenkarten sind per se wahre Datensammler [1], Sie müssen aber Ihre Daten nicht noch großen Werbenetzwerken in den Rachen werfen. Im Folgenden nennen wir zwar die üblichen Favoriten und gehen ein Stück auf sie ein, werden im Anschluss daran aber datensparsame und bessere Apps für iOS und Android vorstellen.

Populäre Favoriten

Das erste Ergebnis für „Kundenkarten-Apps“ in der Google-Suche ist Stocard (siehe ct.de/wrew). Die für iOS und Android erhältliche App steht auf den meisten Ranglisten an erster Stelle. Kein Wunder: Stocard bringt eine Palette von Funktionen mit, die von Punkteabfragen bei Payback und DeutschlandCard über Werbeprospekte bis hin zu vorgeschlagenen Gutscheinen reicht. Es ist kein Account oder Registrierung nötig und das Einscannen von Karten geht mit der ansprechend simpel gestalteten App denkbar leicht.

Die App erfreut sich großer Beliebtheit: Stocard verzeichnet einen Benutzerstamm von weltweit fast 49 Millionen aktiven Nutzern. Das gefiel auch dem Bezahldienst Klarna, der die App im Sommer 2021 für 113 Millionen Euro übernahm. Mittlerweile kann man auch seine Mastercard digitalisieren und über die App benutzen.

Trotz der gerade aufgezählten Funktionen möchten wir die App nicht empfehlen. Die ganzen Annehmlichkeiten kommen nicht umsonst: Stocard sammelt Daten und finanziert sich durch Werbeanzeigen, die kreisrund wie Instagram-Stories oben am Bildschirmrand kleben. Sollten Sie zum Beispiel versehentlich die Standortdaten für die App freigegeben haben, dann darf Stocard die Daten verwenden, um zielgerichtete Werbung zu schalten oder Markt- und Meinungsforschung zu betreiben.

Die Schnüffelei dokumentiert das Unternehmen offen und ehrlich in der Datenschutzerklärung. Daraus geht außerdem hervor, dass Stocard bestimmte Daten von Diensten wie Mixpanel, Firebase Analytics, AppsFlyer Software Development Kit (SDK) und dem

Facebook SDK verarbeiten lässt. Die Firmen hinter den Diensten sitzen alle in den USA, garantieren aber angeblich eine Datenverarbeitung nach EU-Recht. Dabei verweisen die Anbieter auf das Privacy-Shield-Abkommen, das aber wegen Unvereinbarkeit mit dem europäischen Datenschutz gekippt wurde und derzeit neu verhandelt wird. So erfasst zum Beispiel Firebase Analytics sämtliche Ereignisse wie „das erstmalige Öffnen der App, Deinstallation, Update, Absturz oder Häufigkeit der Nutzung der App“ und erstellt daraus Nutzerprofile, die Stocard für „zugeschnittene Werbehinweise“ verwendet.

Das unabhängige Open-Source-Tool Exodus Privacy (siehe ct.de/wrew), das Android Apps auf Tracker und Erlaubnisse scannt, kommt zu einem ernüchternden Ergebnis: Die App enthält sieben Tracker und verlangt 29 Berechtigungen. Das ist ganz schön viel, vor allem wenn man nur ein paar Kundenkarten auf dem Handy abladen will. Im Zweifel machen Sie sich selbst ein Bild der Datenschutzerklärung, die wir Ihnen unter ct.de/wrew verlinkt haben. Wollen Sie bestimmten Diensten die Weiterverarbeitung der Daten untersagen, finden Sie dort die jeweiligen Links dazu, die zu Widerspruchserklärungen führen. Für Apps dieser Art ist es ohnehin eine gute Idee, die Zugriffe auf persönliche Daten weitestgehend zu unterbinden.

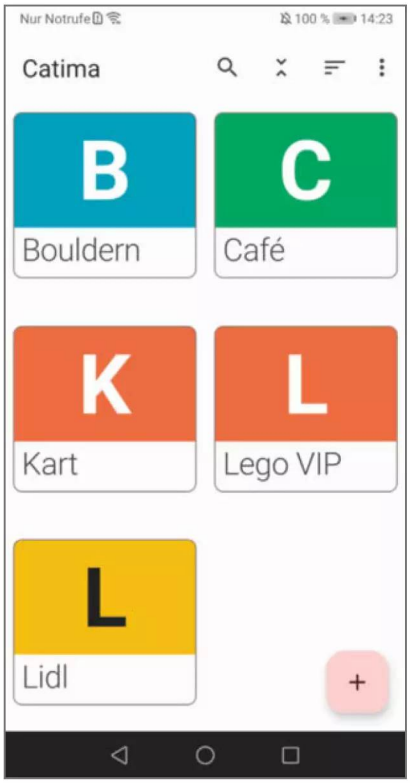
Eine weitere beliebte App ist Fidme. Die vor allem in Großbritannien verbreitete iOS- und Android-App zählt alleine im Google Play Store mehr als eine Million Downloads. Ähnlich wie Stocard greift sie großzügig Daten ab. Laut Exodus Privacy enthält Fidme 11 Tracker und fordert 26 Berechtigungen, weshalb wir sie ebenfalls nicht empfehlen möchten. Was also tun?

Kartenetui

Wir haben uns Kundenkarten-Apps sowohl für iOS als auch für Android angeschaut und geprüft, welche davon gar keine Daten verarbeiten – und wurden fündig. Im Folgenden stellen wir für jedes System jeweils unseren Favoriten vor. Beide benötigen nur die zum Betrieb notwendigen Berechtigungen und kommen komplett ohne Internetverbindung aus. Sie schalten außerdem keine Werbung, sind anmeldefrei und sichern die Karten lokal ab.

Für Android heißt der Kandidat Catima, eine quelloffene App der Entwicklerin Sylvia van Os (siehe ct.de/wrew). Die App können Sie aus dem Open-Source-App-Store F-Droid oder dem Google Play Store herunterladen. F-Droid bekommen Sie nur von der Seite f-droid.org. Den alternativen App-Store sowie seine Installation haben wir unter [2] schon genauer beschrieben. Alternativ können Sie Catima auch als APK-Installationsdatei von der F-Droid-Seite herunterladen und selbst installieren. Wir empfehlen aber den Download aus einem der App-Stores, weil sich diese automatisch um Updates kümmern.

Beim Scannen steht die App der spionierenden Konkurrenz in nichts nach: Über das Plus-Symbol unten rechts fügen Sie eine neue Karte hinzu. Ein Klick darauf öffnet die Kamera, mit der Sie nun den Barcode oder QR-Code scannen. Schlecht lesbare Karten digitalisieren Sie manuell, indem Sie die Nummer abtippen. Zum Schluss ergänzen Sie noch



Die datenschutzfreundliche Android-App Catima zeigt die Karten übersichtlich an. Ein Klick auf einen der Kästen ruft den entsprechenden Barcode beziehungsweise QR-Code auf.

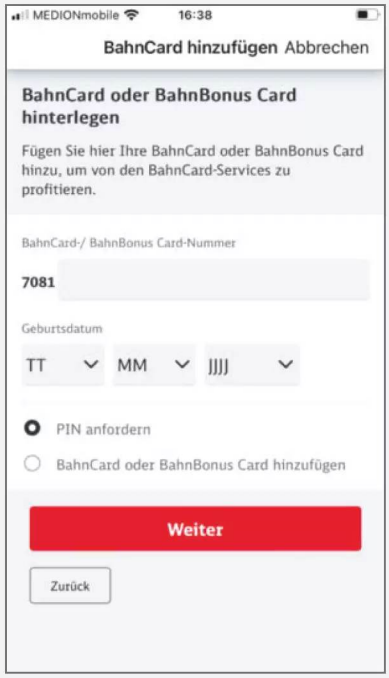
Deutsche Bahn

Wenn Sie Ihre Bahncard aus dem Portemonnaie verbannen möchten, speichern Sie sie am besten in der hauseigenen App „DB Navigator“ der deutschen Bahn. Die gibt es sowohl für Android als auch für iOS (siehe ct.de/wrew).

Damit Sie Ihre Karte in der App hinterlegen können, brauchen Sie einen Account bei der Deutschen Bahn. Melden Sie sich mit diesem an und bestätigen Sie Ihre E-Mail-Adresse, falls noch nicht geschehen. Öffnen Sie nun per Klick auf das App-Menü, wählen dort „BahnCard & BahnBonus“ und unten dann „BahnCard hinzufügen“ aus. Sobald Sie Ihre Karte eingefügt haben, erscheint die Karte unter „Meine Bahncards“.

Abgesehen davon, dass Sie unterwegs nicht mehr die Bahncard mitnehmen müssen, bringt die App ein paar bequeme Extras mit: So können Sie Ihre Tickets verwalten, selber in den Zug einchecken (Komfort-Check-In) und Informationen zu Ihren Fahrten abrufen. Eine Übersicht aller Funktionen haben wir unter ct.de/wrew verlinkt.

Nie wieder Bahncard vergessen: Mit dem DB Navigator der Deutschen Bahn digitalisieren Sie im Handumdrehen Ihre Plastikkarte, ohne Daten an Dritte abtreten zu müssen.



einen Namen oder ein Vorschaubild, fertig. Die digitalen Karten landen schließlich auf dem Hauptbildschirm der App.

Dass sich die App nicht an Kundendaten bedient, beweist auch der Exodus-Privacy-Bericht (siehe ct.de/wrew). Laut diesem verwendet die Version aus dem Google Play Store keine Tracker und braucht gerade mal drei Berechtigungen (Schreiben, Lesen und Kamera).

Catima hat zwar weniger Funktionen als der Marktführer Stocard, muss sich aber keineswegs verstecken: Es gibt zum Beispiel einen praktischen Import, um Karten aus anderen Apps wie Stocard umzuziehen. Aufgrund der großen Community ist die App mittlerweile in mehr als 46 Sprachen verfügbar und wird stetig aktuell gehalten. Den gesamten Funktionsumfang sowie das GitHub-Projekt haben wir unter ct.de/wrew verlinkt.

Kartentresor

Für iOS haben wir uns für die zu Unrecht unbekannte App Card-Safe des Entwicklers Nils-Ole Bickel entschieden (siehe ct.de/wrew). Bis dato zählt die App gerade mal 500 Bewertungen. Card-Safe ist wie Catima anmelde- und kostenfrei. Die App laden Sie wie gewohnt aus Apples App-Store herunter.

Nach dem ersten Start zeigt Ihnen die App zunächst, wofür die einzelnen Symbole stehen und wie man neue Karten anlegt. Der Hauptbildschirm ist schon mit ein paar Beispielkarten gefüllt, die Sie leicht löschen können.

Anders als Catima scannt Card-Safe nicht die Barcodes, sondern speichert lediglich Fotos der Karten. Der Nachteil dieser Methode liegt darin, dass Sie Karten mit einem schlecht lesbaren Barcode nicht digitalisieren können, dafür aber Visitenkarten. Mit einem Klick auf das Plus-Symbol können Sie Karten fotografieren und zurechtschneiden – das geht auch beidseitig. In der Theorie brauchen Sie zwar nur die Rückseite, weil der den Barcode enthält, aber Card-Safe zeigt die Vorderseite hübsch als Preview an.

Um die besten Ergebnisse zu erzielen, sollten Sie die Fotos bei gutem Licht auf einer ebenen Fläche schießen. Die App erkennt die Umrisse der Karte automatisch und schneidet sie aus dem Foto aus. Bei Karten mit einem Magnetstreifen müssen Sie den Ausschnitt manuell anpassen, weil die App den schwarzen Streifen häufig als Rand interpretiert. Alternativ können Sie Bilder der Karten extern mit der Kamera aufnehmen, zuschneiden und anschließend en bloc importieren.

Auf Wunsch können Sie die Karten per Face ID, PIN oder Touch ID wegsperren. Diese Option können Sie beim Start der App oder nachträglich in den Einstellungen (Zahnrad-Symbol) aktivieren.

Die Datenschutzerklärung besteht aus drei kurzen Sätzen, in denen der Entwickler klarstellt, dass die App keinerlei Daten sammelt, keine automatische Übermittlung erfolgt und alle Karten lokal auf dem Gerät abspeichert (siehe ct.de/wrew). Kurzum: Die App tut, was sie soll, und kein Stück mehr. Die Vorschau der Karten macht die App zu einem aufgeräumten Hingucker.

Card-Safe zeigt als Vorschau die Vorderseite der fotografierten Karten an. Größere Sammlungen kann man in Ordnern kategorisieren.

Big Player

Im Artikel „Sicher mit dem Smartphone bezahlen“ auf Seite 40 haben wir unter anderem erklärt, wie Sie Bezahlkarten bei Google Pay und Apple Wallet digitalisieren. Beide verwalten theoretisch auch Kundenkarten: Konkrete Anleitungen haben wir für beide Apps unter ct.de/wrew verlinkt, gestalten das Ganze aber deutlich umständlicher als Card-Safe oder Catima und unterstützen nur bestimmte Karten.

In Google Wallet erreichen Sie das zuständige Menü mit Klick auf „+ Zu Wallet hinzufügen“ und danach auf „Treuepunkte“. Daraufhin erscheint eine Liste, in der Sie Ihre Kundenkarte erst mal finden und auswählen müssen, bevor Sie sie einscannen dürfen. Weil Wallet allerdings nur die Kundenkarten großer Firmen wie Media Markt oder Netto kennt und Anwender die Liste nicht selbst ergänzen können, bleibt das kleine Café um die Ecke außen vor.

Apple Wallet ist ein mächtiges Werkzeug, in dem man Codes für Tickets oder Gutscheine hinterlegen und eigene erstellen kann [3]. In Sachen Kundenkarten sieht es jedoch eher düster aus: Sie selbst können im Wallet gar keine Karten per Scan anlegen. Nur wenn der Anbieter einen personalisierten Link generiert hat, der zur Wallet-App führt, können Sie Ihre Karte hinzufügen.

Bildergalerie

Wenn Ihnen die Idee gefällt, Sie aber keine der hier aufgezählten Apps anspricht, dann können Sie Ihre Karten auch einfach fotografieren und in der Fotogalerie Ihres jeweiligen Geräts als Favoriten hervorheben. Unter iOS klappt das auch in der hauseigenen App „Notizen“. So haben Sie diese in der Warteschlange vor der Kasse mit wenigen Klicks parat. (wid) c't

Literatur

[1] Stefan Wischner, Auf Schnäppchenjagd, Sieben Supermarkt-Apps im Nutzwert-Check, c't 3/2023, S. 116

[2] Andreas Itzchak Rehberg, Android-Apps ohne Google, Der App-Store F-Droid mit Privatsphäre, c't 25/2018, S. 182

[3] Jan Mahn, Taschenticketautomat, Apple Wallet: Handytickets für iOS erzeugen, c't 18/2022, S. 152

Apps und Anleitungen
ct.de/wrew

// heise devSec()

Die Konferenz für sichere Software- und Webentwicklung

11.–13. September 2023 in Karlsruhe

Sichere Software beginnt vor der ersten Zeile Code

Security ist fester Bestandteil der Softwareentwicklung – vom **Entwurf** über den **Entwicklungsprozess** bis zum **Deployment.**

Die **heise devSec** hilft Ihnen dabei mit Vorträgen zu den wichtigsten Themen wie Software Supply Chain, Kryptografie und der Auswirkung von KI auf die Sicherheit.

Aus dem Programm:

// Das ABC sicherer Webanwendungen
// Software Supply Chain Security mit dem SLSA
// Multifaktor-Authentifizierung in der Praxis
// Skalierung von Sicherheit in Kubernetes
// Erweiterung des Secure Development Lifecycle um Privacy by Design
// Wie man mit Mathematik eine Bank übernehmen kann

JETZT **TICKETS** SICHERN!

www.heise-devsec.de

Workshops am 11. September
OAuth 2.1 und OpenID Connect | DevOps und der API-Lebenszyklus | Legacy-Software

Veranstalter: iX Magazin für professionelle IT · dpunkt.verlag · heise Security

Gold-Sponsoren: Contrast Security · opentext | Cybersecurity · Rohde & Schwarz Make ideas real · R&S · sysdig · veeam · WIBU SYSTEMS

Silber-Sponsor: INNOQ

Bronze-Sponsor: andrena OBJECTS

Onlinekauf-Checkliste Bezahlmethoden

Bei der Wahl des Zahlungsweges müssen Sie zwischen Komfort, Sicherheit vor Kostenfallen und Betrug sowie Privatsphäre abwägen. Wir zeigen, wo Fallen lauern und wie Sie sich schützen können.

Von **Markus Montz**

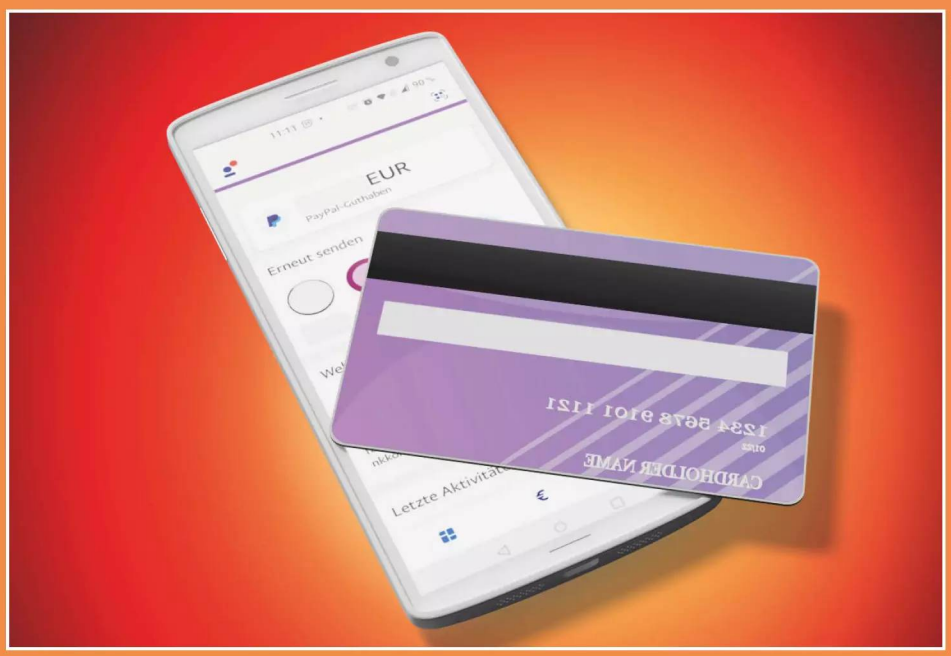


Bild: Andreas Martini

Sichere Bezahlverfahren

Den Datenstrom zwischen den an einer Zahlung beteiligten Parteien könnten Kriminelle höchstens mit enormem Aufwand manipulieren oder belauschen. Dazu tragen Verschlüsselung und die ausgeklügelten Prüfungsroutinen von Zahlungsdiensten und Banken bei. Als Endkunde müssen Sie allerdings dafür sorgen, dass Ihr PC oder Smartphone frei von Schadsoftware ist und sich Betriebssystem und Software mindestens auf dem vom Zahlungsdienst vorgeschriebenen Stand befinden.

Durch die Vorgaben der Zweiten Europäischen Zahlungsdiensterichtlinie ist außerdem eine Zwei-Faktor-Authentifizierung (zum Beispiel TAN) Pflicht bei Kreditkartenzahlungen – auch mit Apple Pay, Google Pay, Klarna und Amazon Pay. Das Gleiche gilt für Überweisungen einschließlich Sofortüberweisung und Giropay sowie PayPal- und Paydirekt-Transaktionen. Die Lastschrift fällt nicht unter die PSD2-Vorgaben, dafür können Sie diese zurückbuchen, wenn jemand Ihre Kontodaten missbraucht hat. Schadensbegrenzung bringt eine Prepaid-Karte von Mastercard oder Visa. Damit verlieren Sie maximal den darauf befindlichen Betrag, allerdings akzeptieren zum Beispiel Hotels solche Karten oft nicht.

Hinterlassen Sie Karten- oder Kontodaten umsichtig. Nutzen Sie im Zweifel Dienste wie PayPal, Paydirekt / Giropay, Apple Pay, Google Pay, Amazon Pay oder Klarna / Sofortüberweisung. Mit ihnen erhält der Händler niemals Konto- oder Kartendaten. Diese Dienste können Ihre Daten zudem besser schützen als ein Händler, vorausgesetzt, Sie nutzen ein starkes Passwort und wo möglich Zwei-Faktor-Authentifizierung.

Phishing-Fallen umgehen

Die meisten Kriminellen versuchen, mit Tricks Ihr Verhalten zu manipulieren, das sogenannte Social Engineering. Die bekannteste Variante im Onlinehandel ist Phishing: Ein Fake Shop oder ein falscher Verkäufer auf einer Auktionsplattform versucht, Sie zur Preisgabe von Zahlungskarten- oder Kontodaten und Passwort sowie zur Zwei-Faktor-Authentifizierung zu bewegen. Dafür nutzen Betrüger raffiniert gefälschte Links in Mails oder Kurznachrichten sowie wohlpräparierte Websites, die eine Datenabfrage durch Ihre Bank oder Kreditkartenmarke vortäuschen. Achtung: Haben Sie eine Zahlung per Zwei-Faktor-Authentifizierung ausgelöst, können Sie im Schadensfall nicht auf die Kulanz Ihrer Bank hoffen.

Seien Sie daher wachsam. Bleiben Sie in Shops, aber insbesondere auf Marktplätzen, Kleinanzeigenportalen und Auktionsplattformen für die Kommunikation und Zahlung stets auf der jeweiligen Website. Gehen Sie nicht auf Bezahl- oder Überweisungslinks per Mail, SMS oder Messenger ein. Zahlen Sie bei PayPal nicht über „Freunde und Familie“ an unbekannte Verkäufer. Prüfen Sie auch Rechnungen genau, vor allem unerwartete – eine Überweisung können Sie nicht mehr zurückrufen. Denken Sie daran, dass sich Schutzparameter wie Widerrufsrecht zu Ihren Ungunsten ändern, wenn Sie Waren persönlich abholen oder bar bezahlen (siehe Artikel “Onlinekauf-Checkliste Rückabwicklung“ auf S. 70). Mehr zu den Gefahren beim Online-Einkauf und wie Sie ihnen begegnen können, erfahren Sie in den Artikeln ab Seite 92.

Geld zurückholen

Kommt die Ware nicht oder weicht erheblich von der Produktbeschreibung ab, wenden Sie sich zunächst an den Händler. Bringt das trotz Sorgfalt kein Ergebnis, bieten die meisten Zahlungsarten Möglichkeiten, das Geld zurückzuholen – auch dann, wenn Sie einem Fake Shop aufgesessen sind.

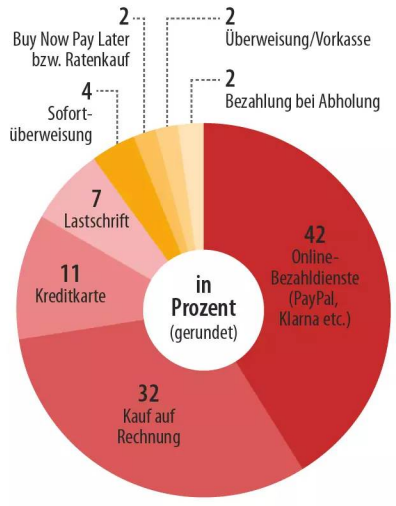
Am bequemsten und sichersten sind dabei der klassische Rechnungskauf, aber auch die 30-Tage-Angebote von Klarna und PayPal: Sie zahlen, nachdem Sie die Ware erhalten und geprüft haben. Erst wenn das Geld geflossen ist, wird es schwierig, denn eine Rückbuchung ist dann nicht mehr so einfach möglich. Achtung: Bei der Vorkasse haben Sie dieses Problem bereits, bevor Sie die Ware erhalten – Sie müssen dem Händler also vertrauen. Die Nachnahme liegt dazwischen: Sie zahlen zwar bei Paketübergabe, sehen den Inhalt aber erst danach.

Am leichtesten erhalten Sie tatsächlich bezahltes Geld bei einer Lastschrift zurück. Die dürfen Sie bis zu acht Wochen lang ohne Angabe von Gründen stornieren, ohne Lastschriftmandat sogar 13 Monate lang. Oft geht das direkt im Onlinebanking. Bei Kreditkarten – einschließlich Apple Pay und Google Pay – wenden Sie sich für ein sogenanntes Chargeback an die Bank oder Sparkasse, die Ihnen die Kreditkarte ausgestellt hat. PayPal, Giropay, Amazon Pay und Klarna haben Käuferschutzprogramme. Achtung: Bei der Sofortüberweisung muss der Händler dazu auch die Klarna-Plattform integriert haben.

In allen Fällen sollten oder müssen Sie zuerst den Händler kontaktieren. Bei Chargeback und Käuferschutz müssen Sie Regeln und Fristen einhalten

Bezahldienste sind beliebt

Bei Wahlfreiheit setzen Onlineshopper in Deutschland beim Checkout am liebsten auf Angebote wie PayPal & Co., noch vor dem Klassiker Rechnungskauf. Gleichwohl müssen Kunden auch bei den Bezahldiensten ein Lastschriftmandat erteilen oder eine Kreditkarte hinterlegen, damit diese die Zahlung abwickeln können.



Quelle: Bitkom Research 2021

und Nachweise liefern (siehe die entsprechenden Artikel in der Rubrik ab S. 62). Veranlassen Sie nicht auf eigene Faust eine Lastschriftrückgabe oder ein Chargeback von einem der Dienste wie PayPal oder Klarna oder aus einer Ratenzahlung! Ansonsten fliegen Sie dort aus dem Käuferschutz und riskieren ein Mahn- und Inkassoverfahren. Buchen Sie eine Lastschrift direkt von einem Händler zurück, müssen Sie ebenfalls mit einem Verfahren rechnen.

Internationale Bestellungen

Wollen Sie im Ausland bestellen, sind die Kredit- und Debitkarten von Mastercard und Visa klar von Vorteil, da weltweit nahezu alle international ausgerichteten Händler diese akzeptieren. Darauf folgen PayPal, das Sie zumindest in der westlichen Welt häufig antreffen werden, sowie Amazon Pay und Klarna – einschließlich der Sofortüberweisung. Auch Apple Pay und Google Pay sind weltweit vertreten, allerdings nicht so häufig anzutreffen wie die direkte Kredit- und Debitkartenzahlung mit Mastercard und Visa.

Ein Girokonto hilft außerhalb Deutschlands, Österreichs und der Schweiz selbst im SEPA-Raum nur begrenzt – die Bezahlarten Lastschrift, Vorkasse und Rechnungskauf sowie Giropay werden Sie dort in Onlineshops nur gelegentlich antreffen; außerhalb des SEPA-Raums nahezu nie.

Die eigenen Daten schützen

Abgesehen von der Nachnahme brauchen die Akteure bei einer Onlinezahlung immer bestimmte Informationen über Sie und Ihre Zahlungsmittel. Damit führen sie die Zahlung aus und prüfen sie auf möglichen Datendiebstahl durch Betrüger sowie auf Geldwäsche und Terrorismusfinanzierung. Die meisten Händler nutzen auf ihrer Seite die Dienste eines Zahlungsabwicklers (Payment Service Provider, PSP). In der Regel geben diese Zahlungsdaten nur zweckgebunden an Dritte weiter; Ihren Warenkorb kennen sie nicht. Auch Zahlungsdienste wie PayPal, Apple Pay, Google Pay, Amazon Pay und Klarna reichen Händlern keine Zahlungsdaten weiter, dafür nutzen alle bis auf Apple Daten für personalisierte Werbung.

Bei einer reinen Kreditkartenzahlung können auch Server außerhalb Europas beteiligt sein. Ohne Ihre explizite Zustimmung speichern Visa und Mastercard aber nur die Kartennummern und geben nichts weiter. Das Gros der Daten fließt zwischen der Kunden- und der Händlerbank.

Auch PayPal nutzt teilweise Infrastruktur und Dienste außerhalb der EU, um Daten zu sammeln, zu speichern und zu verarbeiten. PayPal kann die Daten mit Einverständnis des Kunden (Opt-out!) aber auch zu Marketingzwecken einsetzen. Beim ähnlich zu bedienenden, aber viel seltener angebotenen Dienst Giropay bleiben die Daten hingegen

in Deutschland – er speichert bei bestimmten Händlern allerdings Ihren Einkaufskorb.

Bei einer Klarna-Sofortüberweisung loggen Sie sich beim Checkout in Ihr Bankkonto ein und führen die Überweisung samt Zwei-Faktor-Authentifizierung durch. Diese Daten werden laut Klarna nicht gespeichert, dafür fragt die Firma mit Sitz in Schweden zwecks Risikoprüfung die Girokontodaten der letzten 30 Tage ab. Giropay per Banküberweisung hat optische Ähnlichkeiten, ist aber ein Dienst deutscher Banken. Auch bei diesen beiden Bezahlarten erhält der Händler keine Zahlungsdaten.

Nutzen Sie Ihr Bankkonto für Lastschriften oder um Rechnungsbeträge zu überweisen, entfallen zwar Datenflüsse nach Übersee. Doch dafür erhält der Händler oft Ihre Kontodaten. Kaufen Sie auf Rechnung, Lastschrift, Raten oder schieben Sie die Zahlung auf, fragt der beteiligte Zahlungsdienst – beispielsweise Klarna oder Ratepay – mitunter Ihre Kreditwürdigkeit bei einer Auskunftei wie der Schufa ab. Einfluss auf den „Score“ hat das erst bei häufigen Anfragen, wenn Sie einen Kredit aufnehmen oder fällige, ausreichend gemahnte und von Ihrer Seite unbestrittene oder gerichtlich zugunsten des Händlers entschiedene Forderungen nicht bedient haben.

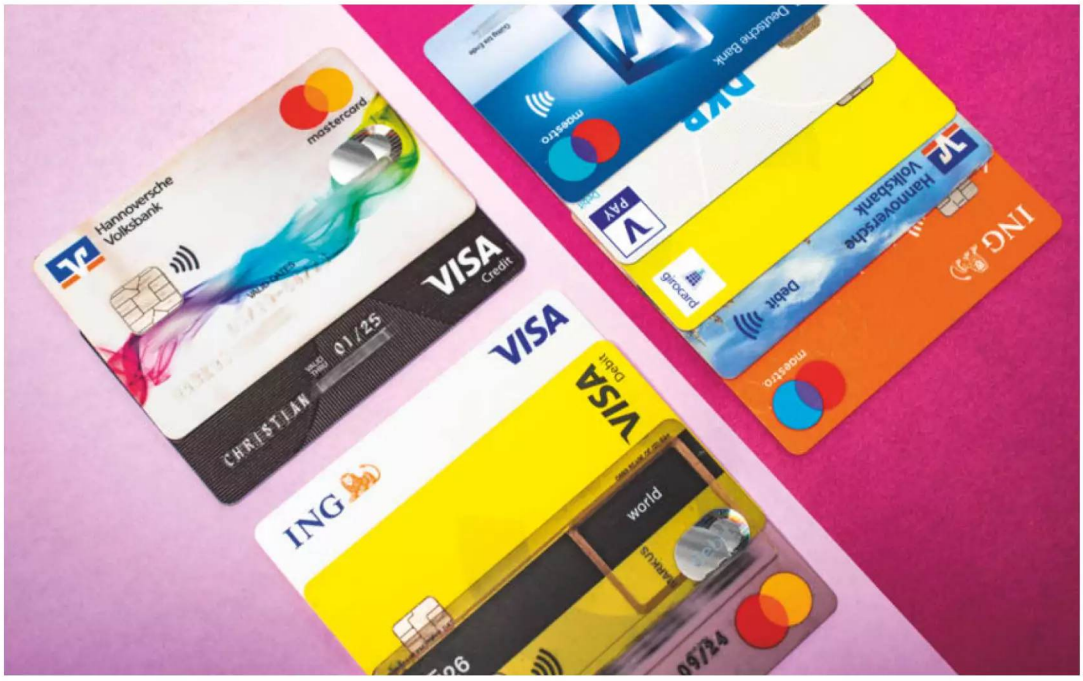
Verdeckte Kosten

Auch wenn es beim Bezahlvorgang im Shop so aussieht, als würden Sie dort keine Gebühren entrichten: Die Kosten für eine Transaktion tragen Sie zumindest teilweise mit. Die Händler und Ihre Bank beziehen diese in ihre Preiskalkulation ein. Auch die meisten Zahlungsarten kosten Sie etwas.

Bei Kredit- und Debitkarten verlangt die ausgebende Bank häufig ein jährliches Entgelt. Wird der Kredit nicht monatlich vollständig ausgeglichen (einige Vertragsmodelle erlauben dies), zahlen Sie hohe Kreditzinsen. Außerdem benötigen Sie ein Girokonto, das Sie mit der Kreditkarte verknüpfen. Für dieses Girokonto, das für Rechnungskauf, Lastschrift und Vorkasse sowie die Klarna-Sofortüberweisung und Giropay ebenfalls Voraussetzung ist, verlangen die meisten Banken ebenfalls Entgelte.

Tatsächlich kostenlos ist ein PayPal-Konto, jedenfalls für Käufe. Doch auch bei diesem benötigen Sie in der Praxis eine Kreditkarte oder ein Girokonto, um es zu nutzen. Für die Dienste von Apple Pay, Google Pay, Amazon Pay und Klarna brauchen Sie mindestens eins von beidem. Lediglich die Nachnahme, bei der Sie den Kaufpreis bar beim Paketzusteller zahlen können, kommt ohne Konto aus. Sie kostet dafür aber ein gesondertes Entgelt.

Kostenfallen entstehen insbesondere beim Ratenkauf und bei aufgeschobenen Zahlungen, auch „Buy now, pay later“ (BNPL) genannt. Vergessen Sie die Zahlung, drohen saftige Mahnkosten, von hohen Zinsen für Kredite ganz zu schweigen. Nutzen Sie solche Angebote häufiger und verlieren den Überblick, geraten Sie leicht in eine Schuldenfalle. (mon) c't



Girocard versus Debitkarten

Seit Jahrzehnten ist die Girocard („EC-Karte“) die wichtigste Bezahlkarte in Deutschland. Doch Visa und Mastercard machen ihr mit ihren Debitkarten zunehmend Konkurrenz. Die verursachen aber an mancher Kasse noch Probleme – und sorgen für steigende Preise, wie unsere Analyse erklärt.

Von **Markus Montz**

Karte abgelehnt: Den Einsatz ihrer neuen Karte hatte sich unsere Leserin und Kundin einer großen Direktbank anders vorgestellt. Als kostenlose Bezahlkarte zu ihrem Girokonto hatte ihr das Institut eine Debitkarte von Visa zugesandt. Mit der könne sie wie bisher mit der Girocard im stationären Handel und zusätzlich auch online und im Ausland einkaufen, hieß es. Während es mit der Girocard jedoch nie Probleme an der Ladenkasse gegeben hatte, war unsere Leserin nun schon auf die dritte Stelle gestoßen, die keine Karten von Visa und Mastercard annahm – zwei inhabergeführte kleine Geschäfte und eine Ärztin.

Mit ihrem Problem ist die Leserin nicht allein. Wir hörten auch von Schwierigkeiten in Hotels und Autovermietungen, besonders im Ausland. Davon

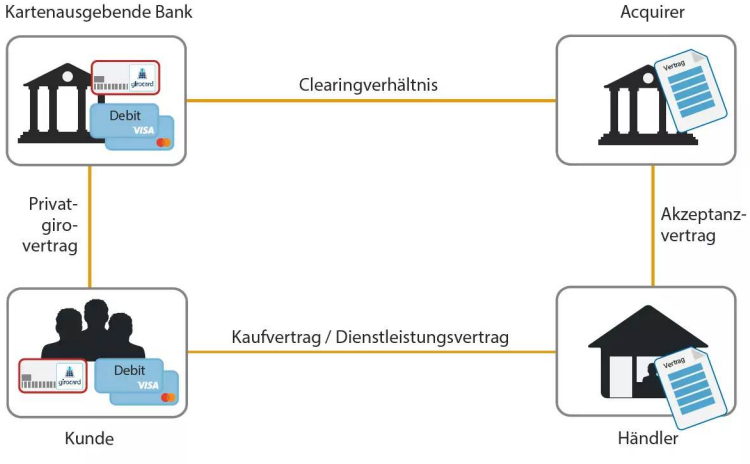
wurden viele Kartennutzer kalt erwischt: Hatten die Terminals oder Banken ein Problem? Lag es an den Karten selbst? Hatte die Abkündigung des Maestro-Systems durch Mastercard etwas damit zu tun? Ist Plastikgeld etwa nicht Plastikgeld? Was ist überhaupt der Unterschied zwischen Girocard, Debitkarte und Kreditkarte? Darüber hinaus fragen wir, welche Banken heute und in Zukunft welche Karten ausgeben und was das für Händler bedeutet.

Alles Debitkarten

Eine Debitkarte ist eine Bezahlkarte. In der Regel händigt eine Bank oder Sparkasse sie ihren Kunden aus und verknüpft sie direkt mit deren Girokonten. Nutzt ein Kunde eine Debitkarte, um damit irgendwo an einem Kartenterminal zu bezahlen, belastet („debitiert“) ihm sein Kreditinstitut den Zahlungsbetrag sofort auf dem Girokonto. Dabei kann „sofort“ ein bis zwei Werktage bedeuten, in jedem Fall aber ohne längeren Aufschub.

Parteien einer Debitkartenzahlung

Debitkartenzahlungen in Deutschland liegt rechtlich ein Vier-Parteien-Verhältnis zugrunde: Auf der einen Seite stehen der Kunde mit seiner kartenausgebenden Bank („Issuer“), auf der anderen der Händler mit seinem Akzeptanzpartner („Acquirer“). Er leitet das Geld abzüglich eines Entgelts an die Bank des Händlers weiter; mitunter sind Bank und Acquirer auch identisch. Acquirer und kartenausgebende Bank verrechnen die Zahlungen untereinander („Clearing“).
Die US-Unternehmen Visa und Mastercard agieren für die Karten in ihren Netzwerken als Lizenzgeber für Issuer und Acquirer und vermitteln Zahlungen zwischen ihnen. Für die Girocard übernehmen diese Rollen der Spitzenverband Deutsche Kreditwirtschaft und seine Mitglieder.



Das ist bereits der wichtigste Unterschied zu einer Kreditkarte: Bei ihr sammelt die Bank die Zahlungsbeträge als Kredit. In Deutschland rechnet sie diesen meist zu einem monatlichen Stichtag zinslos ab und zieht den Betrag vom verknüpften Girokonto ein. Auf den Karten von Mastercard und Visa ist dieser Unterschied an dem Aufdruck „Credit“ oder „Debit“ auf der Vorder- oder Rückseite zu erkennen. Ansonsten gleichen sich die Karten: Sie tragen die Logos des Kreditkartennetzwerks und der ausgebenden Bank sowie die 16-stellige Kartennummer (Personal Account Number, PAN), den Namen des Inhabers, den Gültigkeitszeitraum sowie einen dreistelligen Sicherheitscode für Onlinezahlungen.

Auch Zahlungen mit der deutschen Girocard („EC-Karte“) belasten das Konto sofort. Die Girocard ist ein System des Spitzenverbands Deutsche Kreditwirtschaft, also der deutschen Banken und Sparkassen. Wie bei den Karten der beiden US-Netzwerke geben Geldinstitute die Karten aus, die man am „Girocard“-Logo erkennt. Die Girocard ist technisch und rechtlich ebenfalls eine Debitkarte. Das stiftet oft Verwirrung. Wir bleiben dennoch beim Begriff „Girocard“, um diese von ihren Visa- und Mastercard-Pendants abzusetzen.

Noch größer machen die Verwirrung die Systeme Maestro und V Pay, deren Logos sich zusätzlich auf vielen Girocards finden. Auch bei ihnen handelt es sich um Debitkartensysteme, hinter denen wiederum Mastercard (Maestro) und Visa (V Pay) stecken. Viele Girocards enthalten dieses sogenannte „Co-Badge“ als Zweitsystem für den Auslandseinsatz, weil das Girocard-System auf Deutschland begrenzt ist. Neuerdings sind außerdem Girocards im Umlauf, die das Co-Badge einer „echten“ Debitkarte von Visa oder Mastercard tragen. In allen Fällen gilt, dass solch eine Karte grundsätzlich das Girocard-System nutzt, wenn das Kassenterminal des Händlers daran angebunden ist. Das Co-Badge-System springt erst ein, wenn das nicht der Fall ist.

Die Girocard

Nahezu alle Bezahlterminals bei Händlern und Dienstleistern in Deutschland akzeptieren die Girocard. Ausnahmen gibt es an den mobilen Bezahlterminals der Anbieter SumUp und Zettle, die man in manchen Restaurants und Läden findet, und bei der Modekette Primark. Dort benötigt die Girocard ein Co-Badge von Maestro, V Pay, Mastercard oder Visa. Grundsätzlich lohnt sich daher immer ein Blick auf die Symbole an der Kasse oder Ladentür oder

eine vorherige Nachfrage. Zahlungen im Ausland sind mit der Girocard ebenfalls nur möglich, wenn sie eines der Co-Badges aufweist – und der Händler es akzeptiert. Bargeld erhält man mit der reinen Girocard an nahezu jedem Geldautomaten in Deutschland. Im Ausland ist man auch dafür auf ein Co-Badge angewiesen.

Innerhalb Deutschlands ist die Nutzung der Girocard in den Kosten für das Girokonto enthalten (die Kartenausgabe kostet gelegentlich einen Obolus). Das gilt auch an Geldautomaten, solange man Geräte der eigenen Bank oder eines passenden Verbundes nutzt. An verbundfremden Automaten werden Zusatzkosten fällig. Deren Höhe hängt vom Kontomodell der eigenen Bank sowie der Entgeltordnung der Fremdbank ab. Alternativ zahlen auch manche Einzelhandelsketten in Deutschland kostenlos Bargeld aus; Voraussetzung ist ein Einkauf im Geschäft.

Im Euroraum ist der Einsatz der Girocard mit einem Co-Badge normalerweise entgeltfrei möglich. Außerhalb der Eurozone nimmt die eigene Bank für den Einsatz bei stationären Händlern meistens einen Aufschlag. Geldabheben am Automaten ist überall im Ausland an ein Co-Badge gebunden und kostenpflichtig; es sei denn, man findet einen Automaten des eigenen Instituts. Die Höhe der Aufschläge hängt vom eigenen Geldinstitut, der Fremdbank, deren Abrechnungswährung (Euro ist meist teurer als die Landeswährung), dem bereisten Land und vom Kartentyp ab. Mal sind Maestro und V Pay günstiger, mal eine „reine“ Mastercard- oder Visa-Debit- oder Kreditkarte. Das sollte man vorab klären.

In Sachen Onlinefähigkeit ist die Girocard im Hintertreffen. Insbesondere ist sie bislang für den E-Commerce quasi ungeeignet. Auch für das Bezahlen mit dem Smartphone im Laden eignet sie sich nur

Debitkarten von Visa oder Mastercard kann man auf den ersten Blick nur am entsprechenden Aufdruck auf der Vorder- oder Rückseite unterscheiden.

Das Ende von Maestro

Seit dem 1. Juli 2023 können Banken mit wenigen Ausnahmen (unter anderem in der Schweiz sowie Deutsche Bank und Commerzbank) keine neuen Karten mehr für das Maestro-Debitkartensystem ausgeben. Mastercard will das System ausmustern. Das gilt sowohl für reine Maestro-Karten als auch solche mit Maestro als Co-Badge. Kunden mit einer noch gültigen, Maestro-fähigen Karte können damit aber weiterhin bezahlen, bis ihre Bank die Karte austauscht. In vielen Fällen wird das erst 2027 der Fall sein. Offiziell hat Mastercard die Abkündigung mit der fehlenden Onlinefähigkeit von Maestro begründet. Experten werten den Schritt aber vor allem als Angriff auf nationale Kartensysteme wie die Girocard sowie auf die geplante European Payments Initiative. Gerade letztere soll ökonomisch und geopolitisch ein Gegengewicht zu Visa und Mastercard aufbauen.

Da mit Maestro dessen weltweit anzutreffendes Co-Badge-System wegfällt, sind die kartenausgebenden Banken wegen der Beschränkung des Girocard-Systems auf Deutschland in Zugzwang. Viele setzen bereits auf reine oder Co-Badge-Debitkarten von Visa und Mastercard. Zwar hat Visa sein Co-Badge-System V Pay bisher nicht offiziell abgekündigt, langfristig dürfte der Konzern aber seine Standard-Debitkarte favorisieren. Hinzu kommt, dass man V Pay weder außerhalb Europas noch online nutzen kann.

Die Girocard kann man überall in Deutschland nutzen, wo man das „Girocard"- oder das alte „EC"-Symbol an der Kasse findet. Für den Auslandseinsatz tragen viele Karten ein Co-Badge der Systeme Maestro oder V Pay.

bedingt. Immerhin bieten Sparkassen und Volksbanken Android-Apps an, in denen man seine Girocard hinterlegen und mit NFC-fähigen Geräten nutzen kann. Mit Apple Pay funktioniert bislang nur die Girocard der Sparkassen sowie der privaten Essener National-Bank. Apple Pay ist bislang auch der einzige Weg, mit einer Girocard in Onlineshops zu bezahlen – wenn der Shop denn sowohl Apple Pay als auch Girocard unterstützt. Derzeit verknüpft die deutsche Kreditwirtschaft die Girocard außerdem mit dem runderneuerten Onlinebezahlverfahren Giropay (siehe Artikel „Zahlen mit dem neuen Giropay" auf S. 46). Den Anfang sollen Karten der Sparkassen und VR-Banken in Kombination mit deren Android-Bezahl-Apps (siehe Artikel „Sicher mit dem Smartphone bezahlen" auf S. 40) machen.

Visa und Mastercard Debit

Mit den Debitkarten von Visa und Mastercard kann man an vielen, aber nicht allen Kassenterminals in Deutschland bezahlen. Große Handels- und Supermarktketten sowie Geschäfte mit internationaler Kundschaft nehmen Zahlungen mit Visa- und Mastercard-Debitkarten nahezu durchgängig an. Wie bei der Girocard zahlt man dafür keinen Extraaufschlag. Bares bekommt man an allen deutschen Geldautomaten. Die Kosten variieren allerdings stark: Bei den meisten Banken ist es kostenfrei, ohne dass man auf Automaten eines bestimmten Verbundes festgelegt ist. Viele Banken nehmen nach zwei bis fünf Abhebungen allerdings einige Euro Entgelt. Alternativ kann man wie bei der Girocard in manchen Handelsketten beim Einkaufen ohne Aufschlag Bargeld bekommen.

Auch beim Auslandseinsatz in vielen gängigen Reiseländern punkten die Karten von Visa und Mastercard, weil viele Händler sie anstandslos akzeptieren. Es empfiehlt sich wie bei der Girocard, vorab zu klären, welche Karten ein Laden annimmt. Zahlt man in der Eurozone, ist das ohne Extrakosten möglich. Hat das besuchte Land eine andere Währung, fallen meist Fremdwährungsaufschläge wie bei der Girocard an. Es gibt jedoch auch Ausnahmen, abhängig von Bank und Kontomodell.

Ein weiterer Vorteil der Debitkarten von Mastercard und Visa ist, dass sie anders als die Girocard voll onlinefähig sind. Im E-Commerce kann man sie überall dort verwenden, wo ein Shop Kreditkarten der beiden Netzwerke akzeptiert. Das gilt auch für ausländische Shops, solange der Händler deutsche Karten nicht ausschließt. Zahlt man in Deutschland und im Euroraum, ist das aufschlagfrei. Für andere Währungen kann die eigene Bank ein Entgelt verlangen.

Will man mit dem Smartphone im In- und Ausland bezahlen und dafür eine Visa- oder Mastercard-Debitkarte in Google Pay (Android) oder Apple Pay (iOS) hinterlegen, kommt es auf das kartenausgebende Institut an. Apple Pay unterstützen bis auf die Postbank mittlerweile fast alle größeren Geldhäuser. Bei Google Pay gibt es hingegen Lücken; neben Sparkassen und Volksbanken fehlen dort zum Beispiel auch die Deutsche Bank und ebenfalls die Postbank. Debitkarten der großen Direkt- sowie der Neobanken kann man dagegen anstandslos mit Google Pay nutzen. Die Kosten dafür sind bei Apple wie Google die gleichen wie beim Einsatz der Plastikkarte.

Ungewohnte Alltagsprobleme

Während Zahlungen mit der Girocard in Deutschland eingespielt sind, akzeptieren viele inhabergeführte Geschäfte in Deutschland Visa und Mastercard ebenso wie V Pay und Maestro bislang nicht. Die Verbraucherzentralen bestätigten auf Nachfrage diese Erfahrungen unserer Leser. Den Händlern sind oftmals die Kosten dafür zu hoch (siehe Kasten „Extrakosten für Händler" auf S. 33). Auch Behörden und Arztpraxen lehnen Debitkarten der US-Netzwerke häufig ab. Achten Sie also stets auf die Bezahllogos an der Ladentür oder neben dem Terminal. Falls möglich, sollten Sie mit einer Girocard bezahlen, weil deren Abzüge für die Händler niedriger sind als bei

Mastercard und Visa. Als Kunde tragen Sie die Mehrkosten indirekt mit, weil die Händler sie irgendwann in ihre Preise einkalkulieren dürften.

Probleme kann es mit den Debitkarten von Visa und Mastercard zudem geben, wenn man ein Hotelzimmer bucht und die Betreiber eine verspätete Abreise nachbelasten können wollen. Ähnliches hörten wir von Lesern, die bei Mietwagenfirmen eine Kaution hinterlegen mussten. Zwar versichern sowohl Visa und Mastercard als auch die kartenausgebenden Banken, dass ihre Debitkarten auch für diese Zwecke geeignet sind. In der Praxis kann man aber immer noch gegenteilige Erfahrungen machen. Daher sollte man im Ausland am besten mehrgleisig fahren und zusätzlich zur Debitkarte Bargeld und eine vollwertige Kreditkarte dabeihaben. Je nach Institut kann man diese sogar monatsweise zum Konto hinzubuchen und nach dem Urlaub wieder kündigen. So reduziert man die häufig fälligen Zusatzkosten.

Banken stellen um

Welche Karte eine deutsche Bank oder Sparkasse ihren Kunden als Standard zum Girokonto aushändigt, hängt vom Kontomodell ab. Lange Zeit war dies ausschließlich die Girocard mit V-Pay- oder Maestro-Co-Badge. Mit den Neobanken wie Fidor oder N26 kamen erstmals die Debitkarten heutigen Typs von Mastercard oder Visa hinzu. Neu waren diese nicht: In den USA sind sie schon seit Jahrzehnten im Umlauf.

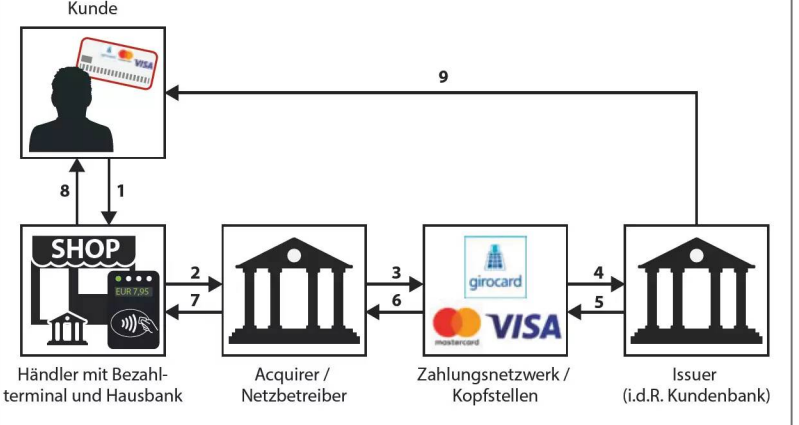
Mittlerweile stellen auch die drei großen Direktbanken Comdirect, DKB und ING ihren Kunden standardmäßig Debitkarten von Visa zum Girokonto aus. Die deutsche Girocard können Kunden bei allen drei Geldinstituten optional hinzubestellen. Sie kostet, ausgenommen ältere Karten der Comdirect, einen Euro im Monat – das werden viele Kunden nicht zahlen wollen. Da die drei Banken zusammengenommen eine achtstellige Zahl von Girokonten verwalten, werden die Debitkarten von Visa und Mastercard in den kommenden Jahren an Bedeutung gewinnen. Die Banken kalkulieren dabei knallhart: Ihnen geht es um Marktdurchdringung und die Einnahmen aus den Interchange-Abflüssen (siehe Kasten „Extrakosten für Händler“ auf S. 33). Bei den Debitkarten sprudeln diese auch im E-Commerce, wo man mit der Girocard so gut wie nicht zahlen kann. Hinzu kommen finanzielle Anreize der großen US-Kartennetzwerke, etwa bei den Lizenzkosten.

Doch auch bei den deutschen Filialbanken und Sparkassen stehen Änderungen im Raum, vor allem durch die Abkündigung von Maestro (siehe Kasten „Das Ende von Maestro“ auf S. 30). Auf Nachfrage von c’t beteuerten fast alle kundenstarken Banken und Sparkassen, die Girocard als Hauptkarte zu behalten. Viele Sparkassen setzen daher mittlerweile anstelle von Maestro auf ein Co-Badge mit Visa- oder Mastercard-Debitkarte, das die Girocard zugleich onlinefähig macht. Derzeit bieten das etwa 270 der 370 Sparkassen in Deutschland an, andere haben auf V Pay umgestellt. Auch etwa 30 Volks- und Raiffeisenbanken bieten bereits diese Option, die Entscheidung liegt aber bei den Filialen vor Ort. Bei vielen VR-Banken erhält man die Girocard ohnehin schon lange mit V Pay; dort ändert sich für Kunden vorerst nichts.

Die Sparda-Banken sowie viele Privatbanken haben kurzfristig die Maestro-Karten noch gegen neue getauscht oder eine längere Frist erhalten. Bereits jetzt bieten Deutsche Bank, Commerzbank und Sparda Baden-Württemberg sowie Hypovereinsbank optional eine Debitkarte von Mastercard res-

Ablauf einer Debitkartenzahlung

Der Kunde zahlt durch Stecken der Karte oder kontaktlos (1). Das Terminal prüft, ob der Kartentyp in Frage kommt und reicht die Autorisierungsanfrage sowie die Zahlungsdaten an den Acquirer oder bei der Girocard den Netzbetreiber weiter (2, 3). Der schickt beides an das Zahlungsnetzwerk von Visa und Mastercard respektive die Kopfstellen im Girocard-System; diese routen die Anfrage an den Kartenherausgeber des Kunden (Issuer, 4). Nach einer Deckungs- und Betrugsrisikoprüfung gibt der Issuer die Zahlung frei oder lehnt sie ab. Je nach Kartentyp liefern die Zwischenstationen eigene Risikoeinschätzungen. Anschließend laufen Freigabe oder Ablehnung zurück (5-8). Die Kundenbank belastet danach ohne Verzug das Konto des Kunden um den Zahlungsbetrag (9).



Extrakosten für Händler

Anders als für Kunden kostet eine Kartenzahlung den Händler grundsätzlich etwas. Die Basis bildet die Interchange Fee, die vom Acquirer (und damit de facto vom Händler) an die kartenausgebende Bank geht. Bei Debitkarten ist dieser Abzug in der EU auf 0,2 Prozent des Rechnungsbetrages gedeckelt.

Bei der Girocard kommen Händler nach Auskunft von Zahlungsexperten zusammen mit weiteren Rechnungsposten auf etwa 0,2 bis 0,25 Prozent. Diese umfassen zum Beispiel monatliche Grundkosten, Gerätemiete für das Kartenterminal, Kontoführungsentgelte sowie teilweise fixe Centbeträge pro Transaktion. Das kann Händlern bereits die gesamte Marge auffressen.

Debitkartenzahlungen mit den Systemen von Visa und Mastercard sind noch teurer. Zusammen mit der Interchange liegt der Gesamtabschlag oft bei 0,7 bis 0,9 Prozent, plus etwaige Fixkosten. Große Ketten zahlen oft deutlich weniger. Im E-Commerce liegt die Händlerbelastung aufgrund des höheren Zahlungsausfallrisikos für die Acquirer meist noch etwas höher.

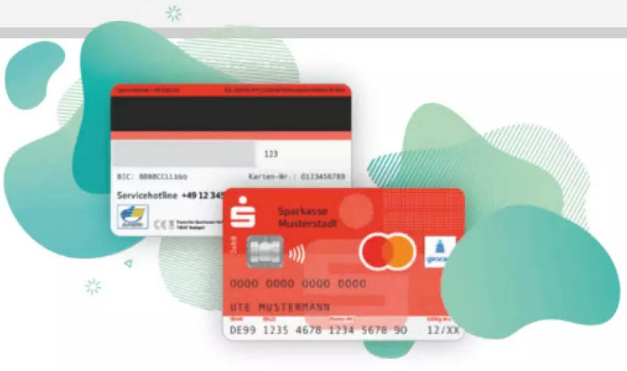


Bild: Finanz Informatik

Viele Sparkassen sowie einige Volks- und Raiffeisenbanken haben ihre Girocards um eine Debitkarte von Mastercard oder Visa als Co-Badge erweitert.

pektive Visa an. Die Santander Bank gibt seit Oktober 2022 standardmäßig eine Visa-Debitkarte aus, neue Girocards ohne Co-Badge kosten 12 Euro im Jahr. Die Targobank setzt auf Visa-Debitkarten und bewirbt die Girocard nicht mehr, hat sie aber weiterhin als Alternative im Angebot. Die Postbank macht zunächst mit dem bisherigen Angebot aus Girocard mit V Pay und optionaler kostenpflichtiger Kreditkarte weiter und dürften sich zukünftig an den Mutterkonzern Deutsche Bank anpassen.

Ausblick

Bankkunden können sich spätestens seit der Abkündigung von Maestro nicht mehr darauf verlassen, eine Girocard zum Konto zu bekommen. Direktbanken, Neobanken und zukünftig vielleicht auch einige klassische Institute geben stattdessen Debitkarten von Visa und Mastercard aus. Diese Debitkarten sind voll onlinefähig und ohne zusätzliche Technik auslandstauglich. Wer die Regeln kennt, kann sogar in Übersee gebührenfrei Geld ziehen und an der Ladenkasse zahlen. Auch die gelegentlichen Probleme in Hotels und bei Autovermietungen dürften sich bald geben.

Doch an deutschen Kassen und damit im Alltag bleibt die Girocard auch in den kommenden Jahren zuverlässiger. Wer gerne mit Karte bezahlt und sich nicht gerade auf große Handelsketten, das Ausland oder den Onlinehandel beschränkt, wird damit rechnen müssen, dass manche Händler und Institutionen die Debitkarten der US-Konzerne nicht annehmen – weil es ihnen zu teuer ist. Eine (zusätzliche) Girocard stellt sicher, überhaupt mit Karte zahlen zu können. In Zeiten steigender Preise reduziert sie zudem Gebühren für den Händler, sodass er den höheren Aufschlag der Finanzindustrie nicht an seine Kunden weitergeben muss. (mon) c't

Debitkarten

Immer öfter geben Banken Debitkarten von Visa und Mastercard aus anstelle der deutschen Girocard („EC-Karte"), zudem hat Mastercard sein „Maestro"-System abgekündigt. Wir beantworten die wichtigsten Fragen zu den alten und neueren Karten.

Von **Markus Montz**

Ende der Girocard?

? Ich habe gehört, dass die Girocard alias „EC-Karte" in nächster Zeit abgeschafft wird. Stimmt das?

! Nein, solche Meldungen in Fernsehen, Online- und Printmedien sind falsch. Die Girocard bleibt erhalten. Viele Kreditinstitute, darunter auch Sparkassen sowie Volks- und Raiffeisenbanken, wollen sie weiterhin als Standardkarte zu ihren Girokonten ausgeben. Abgeschafft wird ein Zweitsystem („Co-Badge") namens „Maestro", das sich auf vielen Karten befindet. Darüber konnte man bisher mit der Girocard auch außerhalb von Deutschland weltweit an Ladenkassen bezahlen und an Bankautomaten Bargeld ziehen. Maestro ist aber nicht sofort weg: Es werden zunächst bloß keine Karten mit Maestro-Zweitsystem mehr ausgestellt. Bereits vorhandene Karten können Sie weiterhin im Ausland benutzen, bis Ihre Bank diese austauscht.

Girocard nicht auslandstauglich?

? Das heißt, ich kann mit einer Girocard nicht mehr im Ausland bezahlen?

! Wenn es eine „reine" Girocard ist, geht das nicht. Die Girocard als solche funktioniert nur in Deutschland und in wenigen ausländischen Geschäften, meist in Grenznähe. Anderenfalls braucht sie ein Zweitsystem. Neben Maestro, das Mastercard betreibt, gibt es noch „V Pay" von Visa. V Pay ist auf Europa beschränkt.

Mittlerweile geben einige Banken und Sparkassen ihren Kunden Karten aus, die als Zweitsystem eine Debitkarte von Mastercard oder Visa bekommen haben. Diese erkennen Sie am jeweiligen Symbol und der zusätzlichen 16-stelligen Kartennummer. Diese Karten funktionieren nicht nur weltweit in Läden und an Automaten, sondern auch wie eine Kreditkarte im Internet.

Was bedeutet „Debitkarte"?

? Was ist überhaupt eine „Debitkarte" und was der Unterschied zur Kreditkarte?

! „Debit" bedeutet „Belastung". Wenn Sie mit einer Debitkarte bezahlen, belastet das kartenausgebende Kreditinstitut den Betrag direkt Ihrem Girokonto und rechnet ihn spätestens nach ein paar

Nur mithilfe von Zweitsystemen auf Ihrer Girocard, die Sie an den Logos von „Maestro" oder „V Pay" erkennen, können Sie mit der Karte bisher im Ausland zahlen. Man spricht von „Co-Badge".

In Deutschland ist die Girocard, früher „EC-Karte“, am gebräuchlichsten (links). Weitere Debitkarten laufen über Visa (Mitte) und Mastercard (rechts).

Tagen ab. Nach diesem Prinzip funktioniert auch die Girocard, die technisch und rechtlich deshalb ebenfalls zu den Debitkarten zählt. Bei einer Kreditkarte gewährt die Bank Ihnen hingegen einen Kredit für den Zahlungsbetrag. Jede Zahlung sammelt sie dazu auf einem Kreditkartenkonto. Diesen Kredit bucht sie meistens einmal im Monat komplett oder ratenweise von Ihrem Girokonto ab.

Unterschiede zwischen Debitkarten

? Was ist dann der Unterschied zwischen einer Girocard und einer Debitkarte von Mastercard oder Visa?

! Es handelt sich um drei verschiedene Zahlungsnetzwerke mit unterschiedlichen Betreibern. Hinter dem Girocard-System stehen die meisten deutschen Banken und Sparkassen. An das Netzwerk angebunden haben sich fast nur Ladengeschäfte und Banken (samt Geldautomaten) in Deutschland. Lediglich mit den Girocards der Sparkassen kann man mithilfe von Apple Pay auch manchmal im Onlinehandel zahlen (siehe außerdem den Artikel „Zahlen mit dem neuen Giropay“ auf S. 46).

Die Zahlungsnetzwerke von Visa und Mastercard umfassen Banken sowie Händler auf der ganzen Welt. Die Debitkarten für diese Netzwerke funktionieren genau wie deren Kreditkarten nicht nur in Läden und an Geldautomaten, sondern darüber hinaus auch uneingeschränkt im Onlinehandel: Genau wie bei der Kreditkarte geben Sie beim Online-Bezahlen mit einer Debitkarte von Mastercard und Visa Ihren Namen, die 16-stellige Kartennummer, das Ablaufdatum und eventuell den dreistelligen Code auf der Kartenrückseite ein. Anschließend authentifizieren Sie sich bei Bedarf mit „3-D Secure“ über Ihre Bank.

Hilfe bei Problemen

? Wo bekomme ich Hilfe, wenn ich Fragen oder Reklamationen habe?

! Ihr Ansprechpartner ist stets die „kartenausgebende“ Bank („Issuer“), von der Sie die Karte erhalten haben. Sie wickelt auch alle Zahlungen mit der Karte ab und kümmert sich um Anträge auf Rückerstattung (Chargeback), wenn etwas schief gelaufen ist (siehe Artikel „Kartenabbuchungen rückabwickeln“ auf S. 72). Deshalb finden Sie auf den Karten stets das Logo Ihrer Bank und das des Zahlungsnetzwerks aufgedruckt.

Möglichkeiten ohne Maestro

? Was machen die Banken ohne Maestro?

! Wenn Maestro nicht mehr verfügbar ist, gibt es mehrere Möglichkeiten. Option eins: Ihre Bank nutzt als Co-Badge V Pay, das Visa zumindest bisher nicht abgekündigt hat. Option zwei: Ihre Bank gibt reine Girocards zum Girokonto aus. Wenn Sie ins Ausland reisen, müssen Sie eine zusätzliche (meist kostenpflichtige) Debit- oder Kreditkarte bei Ihrer Bank oder einem Fremdanbieter beantragen.

Option drei: Sie bekommen von Ihrer Bank standardmäßig eine Debitkarte von Visa oder Mastercard. Damit können Sie in Deutschland und im Ausland bezahlen, im Laden und online – allerdings könnten Sie hierzulande immer mal auf Händler und in sehr seltenen Fällen auch auf Geldautomaten stoßen, die nur die Girocard akzeptieren. Gelegentlich gibt es auch bei Reservierungen Probleme, dazu gleich mehr. Variante vier: Ihre Bank gibt eine Girocard heraus, die mit dem Co-Badge einer Visa- oder Mastercard-Debitkarte versehen ist. Sie vereint die jeweiligen Vorteile auf einer Karte und Sie können damit auch im Onlinehandel bezahlen.

Warum machen Banken das?

? Warum gibt meine Bank Girocards respektive Visa- oder Mastercard-Debitkarten aus?

! Darüber entscheidet das liebe Geld. Die Karten herzustellen kostet die Banken etwas. Zahlen Sie damit an der Kasse, fließen unterschiedlich hohe Gebühren vom Händler an die Bank. Mit Visa und Mastercard nehmen die Banken außerdem Entgelte aus dem wachsenden Onlinehandel ein, wo die Girocard bisher nur selten funktioniert. Zudem locken Visa und Mastercard die Kreditinstitute mit finanziellen Anreizen.

Smartphone und Smartwatch

? Kann ich meine Debitkarte in einem Wallet hinterlegen und kontaktlos an der Ladenkasse zahlen?

! Ja, jedenfalls technisch. Jede Bank oder Sparkasse entscheidet aber selbst, ob sie ihren Kunden diese Möglichkeit anbietet (eine Liste finden Sie unter ct.de/whh2). Grob gesagt funktionieren Visa- und Mastercard-Debitkarten der meisten Banken und Sparkassen in Deutschland mit dem Apple Wallet. Als Sparkassenkunde können Sie dort außerdem die hauseigene Girocard hinterlegen, mit den Girocards anderer Banken klappt das aber bislang nicht.

Das Wallet von Google unterstützen weniger Häuser. Insbesondere fehlen Sparkassen sowie Volks- und Raiffeisenbanken, da sie für Android-Handys eigene Wallets entwickelt haben. Außerdem können Sie im Google Wallet nur Debitkarten von Visa und Mastercard unterbringen, bisher aber keine Girocards.

Als PayPal-Kunde können Sie aber auch dann per Google Pay bezahlen, wenn Ihre Bank es nicht unterstützt: In der PayPal-App auf dem Handy legen Sie dazu eigens für Google Pay eine virtuelle Mastercard-Debitkarte an. Zahlungen zieht PayPal von Ihrem PayPal-Konto ein. Alternativ hilft (auch bei Apple Pay) eine virtuelle Prepaid-Karte von „VIMpay“.

Läden verweigern Visa und Mastercard

? Warum akzeptieren manche Geschäfte Visa und Mastercard nicht?

! Grundsätzlich darf jeder Händler – von der Pommesbude bis zur Supermarktkette – selbst bestimmen, welche Bezahlarten er seinen Kunden anbietet. Die Entscheidung hängt vor allem von den Gebühren ab, die der Händler für jede Kartenzahlung entrichten muss. Den Kuchen teilen sich seine Bank, sein Zahlungsabwickler und die Kundenbank; bei Visa und Mastercard will auch das Kartennetzwerk etwas abhaben.

Debitkarten von Visa und Mastercard sind durchweg teurer als die Girocard und kosten Händler etwa 0,7 bis 0,9 Prozent des Umsatzes, online etwa das Doppelte. Enthalten ist oft ein Sockelbetrag von einigen Cent. Für eine Girocard-Zahlung im Laden müssen Händler mit bis zu 0,25 Prozent mit Sockelbetrag kalkulieren, im allmählich zunehmenden Onlinegeschäft etwas mehr. Kleine inhabergeführte Geschäfte nehmen oft nur die Girocard, da sie ihre Gewinnmarge weniger stark anknabbert. Kunden sollten dabei bedenken, dass die Händler die Entgelte in einer Mischkalkulation auf ihre Produktpreise aufschlagen.

Geldautomaten

? Meine Debitkarte von Visa respektive Mastercard funktioniert nicht am Geldautomaten. Was ist da los?

! In den meisten Fällen dürfte es sich um einen vorübergehenden Fehler handeln. Auf Anfrage versicherten uns die deutschen Banken und Sparkassen, dass es an ihren Automaten keine generellen Beschränkungen für bestimmte Kartentypen gibt. Das ist plausibel, da sie Entgelte kassieren, wenn jemand mit einer institutsfremden Karte Geld abhebt. Grundsätzlich kann aber jedes Institut selbst bestimmen, ob es auch Inhabern von Visa- und Mastercard-Debitkarten Bargeld am Automaten auszahlt. Insbesondere bei den regional organisierten

Sparkassen und Genossenschaftsbanken bleibt daher ein Rest Unsicherheit, ob wirklich jeder Automat uneingeschränkt Zugriff gewährt.

Girocard online nutzen

? Warum kann ich mit meiner Girocard nicht online bezahlen?

! Die polemische Antwort: Weil die deutschen Banken und Sparkassen es lange verschlafen haben, die Girocard für den E-Commerce zu ertüchtigen. Es gibt aber seit Kurzem eine Ausnahme. Wenn Sie eine Girocard einer Sparkasse sowie ein iPhone, iPad oder einen neueren Mac besitzen, können Sie die Karte im Apple Wallet hinterlegen. Damit können Sie bei allen Onlinehändlern zahlen, die Apple Pay als Bezahlart anbieten (siehe Artikel „Zahlen mit dem neuen Giropay“ auf S. 46).

Die Sparkassen sowie Volks- und Raiffeisenbanken wollen ihren Kunden außerdem in Kürze eine digitale Girocard für Android-Smartphones anbieten. Um damit zu zahlen, müssen Sie sich im Onlinebanking für Giropay registrieren und die Giropay-App auf dem Handy installieren. Zusätzlich benötigen Sie die App „Mobiles Bezahlen“ der Sparkassen oder „VR Pay“ der Volks- und Raiffeisenbanken und müssen darin eine Girocard hinterlegen.

Kautionen

? Wieso will ein Hotel mit meiner Debitkarte von Visa oder Mastercard kein Zimmer reservieren?

! Für Reservierungen und Kautionen wollen Hotels oder Autovermietungen sich die Option offenhalten, die Karte nachzubelasten, wenn Kunden das Zimmer nicht rechtzeitig räumen oder das Fahrzeug zu spät zurückgeben. Lange Zeit sahen die Regeln der Kartennetzwerke für solche Fälle aber nur bei Kreditkartenzahlungen eine Zahlungsgarantie vor.

Zwar garantieren die Regeln beider Netzwerke, die für Händler- und Kundenbanken bindend sind, den Hoteliers und Vermietungen ihr Geld längst auch bei Debitkarten. Einige haben aber noch das früher für sie nachteilige System im Kopf. Daher lehnen sie Debitkarten ab. Die pragmatische Lösung ist in diesem Fall, mit einer Kreditkarte zu reservieren und zu zahlen – und sicherheitshalber solch eine Karte dabei zu haben, wenn Sie ein Auto oder Hotelzimmer mieten.

Keine kontaktlose Zahlung mit Kombikarten

Warum kann ich mit meiner Sparkassen-Kombikarte (Girocard und Mastercard Debit) an manchen Kassen nicht kontaktlos zahlen?

Höchstwahrscheinlich ist das Kassenterminal noch nicht darauf vorbereitet. Wie uns die Sparkassen mitteilten, stellt der Händler respektive dessen Zahlungsdienstleister in der Regel eine Präferenz für Karten mit Co-Badge ein. In Deutschland ist das stets die für ihn kostengünstigere Girocard. Ohne Vorkonfiguration weiß das Terminal aber nicht, was es tun soll. Eventuell kann die Kassenkraft nachhelfen. Wenn nicht, müssen Sie die Karte ins Terminal stecken. Dann können Sie auswählen, ob Sie per Girocard oder Mastercard bezahlen möchten, und geben anschließend die PIN ein. Die meisten Terminals sind aber bereits auf die Kombination aus Girocard und Debitkarte von Mastercard oder Visa vorbereitet, der Rest dürfte mit den nächsten Softwareupdates folgen.

Übrigens: Bei einer Girocard mit Co-Badge können Sie der Kassenkraft vor (!) der Zahlung immer mitteilen, ob Sie lieber die Girocard oder das Co-Badge-Netzwerk nutzen möchten. Für Sie macht das preislich keinen Unterschied.

TAN-Generator

Funktionieren im TAN-Generator anstelle der Girocard auch Debitkarten von Visa und Mastercard?

Nein, grundsätzlich nicht. Stellt Ihre Bank um, haben Sie ein Problem, zum Beispiel als Kunde der DKB: Sie bietet das chipTAN-Verfahren mit ihren Girocards für das Onlinebanking noch an, gibt aber als Standard eine Visa-Debitkarte aus. Die Girocard bekommen Sie nur noch auf Anfrage und kostenpflichtig (siehe Artikel „Girocard versus Debitkarten“ auf S. 28).

Sicherheit

Was ist sicherer, Girocard oder Visa und Mastercard?

Technisch gibt es keinen Unterschied: Alle drei nutzen für ihre Karten die bisher nicht geknackten Kryptochips nach dem EMV-Standard. Größere Zahlungen müssen Kunden zudem durch eine Zwei-Faktor-Authentifizierung absichern. Besonders sicher sind Zahlungen mit einem gut geschützten Smartphone (siehe Artikel „Sicher mit dem Smartphone bezahlen“ auf S. 40). Auch im E-Commerce, der vor allem Visa und Mastercard betrifft, ist das Sicherheitsniveau hoch. Deshalb versuchen Betrüger dort vor allem, die Nutzer selbst zu Fehlern zu verleiten. Da man die Girocard im Onlinehandel bisher kaum antrifft, wird sie auch selten zum Ziel. Speziell für Apple Pay gibt aber auch Maschen, die auf Girocard-Nutzer abzielen (siehe Artikel „Neue Masche beim Kartenbetrug“ auf S. 95).

Bild: Finanz Informatik

Die neuen Girocards mit Visa oder Mastercard Debit als Co-Badge (erkennbar an der 16-stelligen Kartennummer) bereiten gelegentlich noch Probleme beim kontaktlosen Bezahlen.

Datenflüsse

Wohin fließen meine Daten?

Das kommt darauf an. Bei der Girocard bleiben die Daten auf deutschen Bankservern, bei Zahlungen mit Visa und Mastercard können Daten auf Servern in den USA landen. Weitere Akteure wie Apple und Google kommen bei Smartphone-Zahlungen ins Spiel, wobei Apple Daten allein für die Zahlung nutzt, Google auch für personalisierte Werbung (siehe Artikel „Sicher mit dem Smartphone bezahlen“ auf S. 40). Händler bekommen aber auf legalem Weg keine persönlichen Daten, sofern Sie das nicht ausdrücklich erlauben. (mon) *ct*

Banken, die Google Pay und Apple Pay anbieten
ct.de/whh2

Glossar

Einige Begriffe tauchen im Zusammenhang mit Bezahlkarten und Giropay immer wieder auf. Wir erklären sie.

Von **Markus Montz**

Bild: www.freepik.com

Acquirer/Akzeptanzpartner: Stellt dem Händler den Anschluss an die Systeme zum Beispiel von Girocard, Mastercard oder Visa her und wickelt Zahlungen für ihn ab.

Chargekarte: Bei dieser Art von Kreditkarte sammelt der Issuer die Zahlungen, rechnet sie in der Regel einmal im Monat ab und bucht den Gesamtsaldo vom Konto ab.

Co-Badge: Ein sekundäres Bezahlsystem auf einer Bezahlkarte, das zum Einsatz kommt, wenn das Kartenlesegerät das primäre System nicht unterstützt – erkennbar am zweiten (Co-) Symbol (Badge). Beispiele sind Maestro und V Pay und neuerdings auch vollwertige Debitkarten von Mastercard und Visa.

Debitkarte: Bezahlkarte, bei der die Bank das Geld innerhalb weniger Tage vom Konto abbucht (also ohne Aufschub oder Kreditrahmen wie bei Kreditkarten). Zu den Beispielen zählen die Debitkarten von Visa und Mastercard einschließlich Maestro und V Pay, aber auch die deutsche Girocard.

Digitale Karte: Das Abbild einer Plastikkarte, das im Wallet eines Smartphones oder einer Smartwatch landet. Digitale Karten erhalten eine eigene Pseudo-Kartennummer (Token) und sind an das genutzte Gerät gebunden.

Deutsche Kreditwirtschaft (DK): Spitzenverband der deutschen Banken und Sparkassen, unter anderem für Standards und Spezifikationen im Zahlungsverkehr zuständig.

Echtzeitüberweisung: Vom Europäischen Zahlungsverkehrsausschuss spezifiziertes Überweisungsverfahren, bei dem die Banken dem Empfänger im einheitlichen europäischen Zahlungsraum (SEPA) eine Überweisung nach spätestens zehn Sekunden gutschreiben müssen.

European Payments Initiative (EPI): Projektname für ein geplantes paneuropäisches Bezahlverfahren mittels Wallet. Ein Bankenkonsortium will es im gesamten Euroraum zur Verfügung stellen.

Giropay: Internet-Bezahlverfahren der Deutschen Kreditwirtschaft, bei dem der Nutzer Geld an den Händler überweist und seine Bank den Händler darüber in Echtzeit informiert. Wurde mit Paydirekt und Kwitt zum „neuen" Giropay zusammengeführt.

Issuer/Kartenherausgeber: Finanzinstitut, das eine Bezahlkarte (z.B. in den Systemen von Girocard, Mastercard, Visa) an den Kunden herausgibt.

Kreditkarte: Im Unterschied zu Debit-Bezahlkarten zahlen Inhaber einer Kreditkarte ihre Käufe nicht sofort, sondern erhalten dafür vom Kartenherausgeber einen Kredit. Man unterscheidet Chargekarten und revolvierende Karten.

Kwitt: P2P-Zahlungsverfahren in Banking-Apps auf dem Smartphone. Nutzer können anderen Nutzern, deren Handynummer sich im Adressbuch befindet, direkt Geld schicken.

Maestro: Weltweites Debitkartensystem von Mastercard; primär für den stationären Handel und Geldautomaten konzipiert. Läuft ab Juli 2023 bis Juni 2027 zugunsten der „Mastercard Debit" aus.

Open Banking: Vom Kunden genehmigter Zugriff von Drittdiensten auf dessen Girokonto. Anbieter – sogenannte Kontoinformations- und Zahlungsauslösedienste – benötigen eine Erlaubnis der Finanzdienstleistungsaufsicht. Beispiele: „Sofortüberweisung", seit 2014 Teil von Klarna, und das ursprüngliche Giropay.

Paydirekt: Internet-Bezahlverfahren der Deutschen Kreditwirtschaft, mit dem Kunden mittels Nutzername und Passwort in Onlineshops bezahlen können; firmiert mittlerweile unter „Giropay".

P2P-Zahlung: Elektronische „Person-to-Person"-(P2P-)Geldtransaktion zwischen zwei Wallets, bei der an die Stelle der Kontonummer des Empfängers in der Regel dessen Mailadresse oder Handynummer tritt.

Prepaid-Karte: Um solch eine Karte einzusetzen, muss der Nutzer sie vorher per Überweisung oder Abbuchung aufladen und kann dann damit zahlen, bis das Guthaben bei null ist. Da man diese Karten nicht überziehen kann, bekommt man sie auch ohne Schufa-Prüfung.

Revolvierende Kreditkarte: Bei dieser Art von Karte bestimmt der Inhaber je nach Vertrag selbst, wie viel vom Gesamtsaldo er zum monatlichen Stichtag abbuchen lässt oder zu einem selbst gewählten Zeitpunkt per Überweisung ausgleicht. Für den verbleibenden Restbetrag kassiert der Issuer teils hohe Kreditzinsen. Kreditkarten ohne Grundgebühr sind oft revolvierend. Um Kostenfallen zu umgehen, sollten Nutzer daher in den Voreinstellungen prüfen, ob der Issuer monatlich den vollen oder nur einen Teilbetrag abbucht.

V Pay: Debitkartensystem von Visa für Europa, für den stationären Handel und Geldautomaten konzipiert; konkurriert intern mit der „Visa Debit".

Virtuelle Karte: Eine Bezahlkarte, die nur digital existiert, also kein Plastik-Gegenstück bekommt.

Wallet: Digitale Brieftasche für elektronische Zahlungen, in der man Bezahlkarten oder andere Zahlverfahren hinterlegt – Beispiele sind PayPal, Apple Pay und Google Pay.

(mon) c't

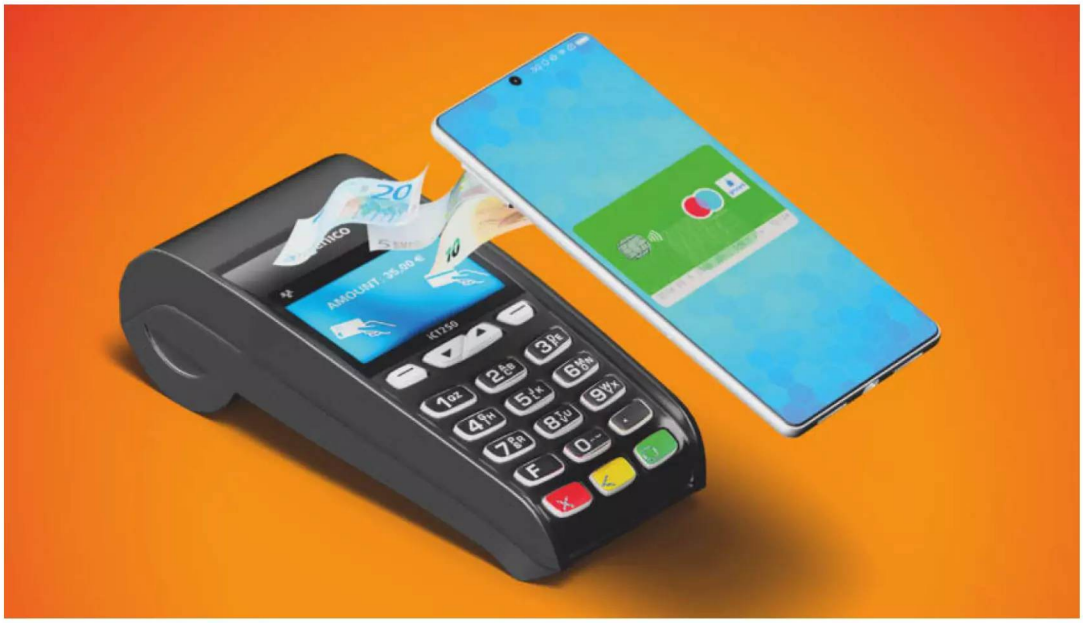


Bild: Andreas Martini

Sicher mit dem Smartphone bezahlen

Digitale Kopien Ihrer Bank- und Kreditkarten machen das Bezahlen mit dem Smartphone nicht nur einfacher, sondern auch sicherer als mit Plastik. Je nach Wallet-Anbieter geht das sogar sehr datensparsam, wie unser Überblick zeigt.

Von **Markus Montz**

Achtzehnfünfzig, bitte! Nur kurz das Smartphone entsperren, vor das Kartenterminal an der Ladenkasse halten, ein „Pling“ und fertig ist die Laube: Mit dem Handy statt mit Plastikkarten kontakt- und bargeldlos zu bezahlen, gehört für manche längst zum Alltag. Wer eine Smartwatch mit Bezahlfunktion hat, muss nicht einmal das Handy zücken: Auch die schlauen Uhren ersetzen zuverlässig die Girocard oder Kreditkarte im Portemonnaie – oder genauer: nehmen ein digitales Pendant der Karten auf.

Doch was passiert, wenn ein Dieb das Smartphone oder die Smartwatch stiehlt oder ein Hacker das Wallet mit den virtuellen Karten knackt? Können die Diebe dann auch Ihr Konto leerräumen? Und wer hat eigentlich alles Zugriff auf Ihre Einkaufsdaten? Schließlich dürften die wenigsten Menschen ein Interesse daran haben, dass der Anbieter der Wallet App erfährt, wo sie für wie viel Geld einkaufen und wofür sie es ausgegeben haben.

Wir erklären, weshalb Wallets für Bezahlkarten auf dem Smartphone so komfortabel sind und digitale

Karten ihre Plastikzwillinge bei der Sicherheit sogar ausstechen. Doch für die Sicherheit und Bequemlichkeit bezahlen Sie unter Umständen mit Daten. Insbesondere Google wertet Ihre Bezahlvorgänge auf Android-Smartphones detailliert aus. Wie detailliert, können Sie immerhin ein Stück weit beeinflussen.

Wallet-Apps in Deutschland

iPhone-Nutzer können nur über Apple Pay mit den digitalen Zwillingen ihrer Karten im Apple Wallet bezahlen. Android-Nutzern steht das bordeigene Wallet von Google zur Verfügung, außerdem bieten die Sparkassen sowie die Volks- und Raiffeisenbanken spezielle hauseigene Wallet-Apps an. Bei den Sparkassen heißt diese „Mobiles Bezahlen“, bei den Genossenschaftsbanken schlicht „Pay“.

Apple hat sein Wallet fest in iOS und WatchOS integriert, das Google Wallet ist Bestandteil von Android und Wear OS. Beide speichern beliebig viele Kredit- und Debitkarten verschiedener Kreditinstitute in digitaler Form. Damit können Sie dann per Apple Pay beziehungsweise Google Pay kontaktlos per NFC (Near Field Communication) an dazu fähigen Ladenkassen zahlen. Das sind mittlerweile so gut wie alle, die auch Kreditkarten akzeptieren. Mit beiden Wallets können Sie außerdem in Onlineshops einkaufen, beide nehmen zusätzlich Portemonnaie-Inhalte wie Tickets oder Kundenkarten auf. Wie das zum Beispiel mit Kundenkarten funktioniert, lesen Sie im Artikel „Kundenkarten via App digitalisieren“ ab Seite 18.

Im Laden begleicht sich die Rechnung dann wie von selbst: Sie bitten die Kassenkraft um Kartenzahlung, entsperren das Gerät und halten es wenige Zentimeter vor das Kartenterminal. Die Karten-PIN brauchen Sie gar nicht mehr einzugeben – ein klarer Vorteil gegenüber der Plastikkarte. Im Onlinehandel geben Sie nach der Bestellung die Zahlung via Smartphone oder Tablet frei. Bei Apple ist das auch auf MacBooks mit Touch ID möglich.

Apple Wallet und Google Wallet

Apple unterstützt die Bezahlfunktion per Wallet ab iOS 10. Sie steht somit allen iPhones ab der 6er-Reihe

In den Wallets von Apple und Google kann man außer Bezahlkarten auch Konzertkarten, Kundenkarten und allerlei anderen Portemonnaie-Inhalt unterbringen.

Möchte man per Google Pay bezahlen, obwohl die eigene Bank den Dienst nicht unterstützt, kann man eine virtuelle Debitkarte von PayPal hinterlegen und mit seinem Bankkonto verknüpfen.

zur Verfügung, ebenso Apple Watches ab Series 1. Damit man eine Bezahlkarte für Apple Pay hinterlegen kann, muss die eigene Bank oder Sparkasse mit Apple kooperieren. In Deutschland tun das nahezu alle großen Kreditinstitute außer der Postbank und einem Teil der Sparda-Banken. Die Girocard, vormals EC-Karte, können Sie derzeit nur als Kunde einer Sparkasse sowie der Essener National-Bank hinterlegen. Die Liste der Apple-Pay-fähigen Banken haben wir unter ct.de/wgnh verlinkt.

Googles Wallet setzt zum Bezahlen ein NFC-fähiges Smartphone mit Android ab 7.0 oder eine Smartwatch mit Wear OS ab 2.0 voraus. Aus Sicherheitsgründen können Sie kein Smartphone verwenden, dessen Schutzmechanismen zur Ausführung von unsignierten Programmen deaktiviert sind (gerootete Geräte). Zwar ist Googles Systemvoraussetzung für das Wallet hinreichend sicher, dennoch empfehlen wir wie übrigens auch bei Apple ein möglichst aktuelles Betriebssystem. Im Idealfall bedenkt der Smartphone-Hersteller es noch mit Sicherheitsupdates.

Von den großen Banken unterstützen Google Pay in Deutschland außer der Commerzbank vor allem die Direktbanken ING, DKB und Comdirect sowie N26. Dafür fehlen viele große Filialbanken, darunter die Sparkassen, die Volks- und Raiffeisenbanken, die Deutsche Bank, die Postbank und die meisten Sparda-Banken. Die Liste der Kreditinstitute, deren Karten für Google Pay geeignet sind, finden Sie ebenfalls unter ct.de/wgnh.

Falls Ihre Bank auf der Liste fehlt, müssen Sie nicht gleich ein neues Kreditkartenkonto mit Google-Unterstützung eröffnen. Mit einem PayPal-Konto können Sie dieses Problem recht einfach lösen: PayPal bietet seinen Kunden eine virtuelle (also rein digitale, siehe auch das Glossar auf S. 39) Mastercard speziell für Google Pay an; sie funktioniert allerdings nicht mit Wear OS. Alternativ legen Sie sich eine virtuelle Prepaid-Karte zu, zum Beispiel von VIMPay.

Der Kontaktlos-Standard

Der beherrschende internationale Standard hinter dem mobilen Bezahlen ist in Europa und Nordamerika die Near Field Communication (NFC). Über elektromagnetische Induktion lassen sich mit NFC auf wenige Zentimeter Entfernung Daten zwischen einem Chip (etwa in einer Kredit- oder Bankkarte oder einem Smartphone) und einem Lesegerät drahtlos übertragen.

Der NFC-Standard ließ sich gut mit dem etablierten EMV-Standard für Zahlverfahren zu „EMV Kontaktlos“ verheiraten. EMV steht für „Europay International, Mastercard, Visa“. Diese drei Dienstleister hatten bereits in den Neunzigerjahren gemeinsame Spezifikationen für Zahlungskarten-Chips und Lesegeräte festgelegt. Dem EMV-Standard folgen beispielsweise auch die deutsche Girocard oder American Express.

Da Banken und Kreditkartennetzwerke an jeder Transaktion verdienen, hatten sie ein Interesse daran, Bezahlen per Karte attraktiv und schnell zu gestalten. Dabei halfen ihnen nicht nur die Standardisierung und Massenfertigung von NFC-Chips für Bezahlkarten, sondern auch die immer schnelleren Lesegeräte und Datenverbindungen. Das lockt immer mehr Einzelhändler und Dienstleister, Kontaktloszahlungen zu akzeptieren, offensiv flankiert von Kampagnen der Finanzindustrie. Die legt außerdem seit Jahren Wert darauf, dass nahezu alle neu ausgelieferten Kartenlesegeräte den Kontaktlos-Standard unterstützen.

Daneben trug die EU mit dem gedeckelten Interbankenentgelt zur Attraktivität für Händler bei (siehe Text). Zwar fallen für diese noch weitere Entgelte an, sodass sie pro Zahlung zwischen 0,2 und 0,3 Prozent für Girocard-Zahlungen und 0,7 bis 0,9 Prozent für Kreditkartenzahlungen abdrücken, häufig inklusive eines fixen Sockelbetrags von beispielsweise 9 Cent pro Zahlung. Hinzu kommen Kontoführungsgebühren, Monatsgrundgebühren und eventuell eine Gerätemiete. Das wiegen das Tempo der Zahlungen und die vereinfachte Abrechnung gegenüber Bargeld jedoch meistens auf.

Denn die EU hat dem kontaktlosen Bezahlen mit Karte oder Smartphone auch an einer anderen Stelle Vorschub geleistet: Die Zweite Europäische Zahlungsdiensterichtlinie (PSD2, Payment Services Directive 2) enthält für „Kleinbeträge bis 50 Euro“ eine Ausnahme von der obligatorischen PIN-Eingabe. Das vereinfacht und beschleunigt den elektronischen Bezahlvorgang zusätzlich.

Sparkassen und VR-Banken

Außer mit dem Google Wallet können Sie unter Android auch mit den Apps der Sparkassen („Mobiles Bezahlen“) sowie Volks- und Raiffeisenbanken („Pay“) zur Kasse gehen. Beide nehmen jeweils ihre hauseigenen Girocards, Debit- und Kreditkarten auf. Damit können Sie im Laden per Smartphone bezahlen, aber weder online noch mit der Smartwatch. Immerhin läuft der Bezahlprozess ähnlich komfortabel ab wie mit den Wallets von Apple und Google.

Für „Mobiles Bezahlen“ benötigen Sie mindestens Android 6, für „Pay“ Android 8. Generell empfehlen wir aber auch für diese Wallets ein möglichst aktuelles Android, das optimalerweise noch Sicherheitsupdates bekommt. Karten fügen Sie in den Apps einfach hinzu, indem Sie einmalig Ihre Zugangsdaten für das Onlinebanking eingeben.

Die Sparkassen wie auch die Volks- und Raiffeisenbanken rüsten ihre Apps momentan auf. Sie sollen sich zukünftig mit der „Giropay“-App des gleichnamigen Bezahldienstes der deutschen Kreditwirtschaft koppeln lassen. Über Giropay könnten Sie dann auch in Onlineshops mit der Girocard zahlen. Zunächst beschränkt sich das Angebot aber auf In-App-Käufe auf dem Smartphone, außerdem muss der Händler Giropay als Bezahlmethode akzeptieren (siehe Artikel „Zahlen mit dem neuen Giropay“ ab S. 46).

Mehr eingebaute Sicherheit

Bei allen vier vorgestellten Apps erhöht das Wallet die Sicherheit gegenüber der Plastikkarte deutlich. Die hat nämlich einen grundsätzlichen Nachteil: Sobald ein Dieb sie in der Hand hält, kann er damit bereits kleine Beträge bezahlen. Nutzt er die Karte kontaktlos, kann er im Laden ohne PIN 50 Euro pro Zahlung und insgesamt bis zu 150 Euro ausgeben. Auch im Internet könnte er insgesamt 100 Euro verprassen, ohne sich über das 3D-Secure-Verfahren mit einem zweiten Faktor zu legitimieren.

Die Kontaktlos-Funktion einer Karte ist noch in weiterer Hinsicht ein Unsicherheitsfaktor. Kommt ein Angreifer beispielsweise mit einem mobilen Bezahlterminal dicht genug an die Karte, kann er damit heimlich Beträge bis zu 50 Euro abbuchen. Nun fällt so ein Angriff aber meistens auf, weil der Täter nach der Position der Karte suchen und mit dem Gerät wie mit einer Metallsonde am Opfer entlangfahren muss. Überdies würde er mit der Abbuchung auch eine Datenspur hinterlassen. Bislang ist das Szenario daher zum Glück Labortheorie geblieben.

Smartphones sind gegen Angriffe mit mobilen Kartenlesegeräten geschützt, die Plastikkarte kann dagegen Beträge bis 50 Euro herausrücken – nach unserer Kenntnis ist das aber nur eine theoretische Gefahr.

Auch die Kartendaten sind ein Problem: Auf der Karte sind fast immer die Kartennummer (PAN, Personal Account Number), der Name des Inhabers, der Ablaufmonat und der Sicherheitscode aufgedruckt. Die Kartennummer und das Ablaufdatum einer Karte könnte man zudem wie eben beschrieben drahtlos mit einem NFC-fähigen Smartphone im Klartext auslesen. Mit diesen Daten können Betrüger Kartenkopien herstellen, die manchmal noch in Übersee oder im Internet funktionieren, ohne dass die automatische Betrugswarnung anschlägt. Zwar bekommen Sie das Geld normalerweise zurück, den Ärger haben Sie dann trotzdem.

Das digitale Wallet ist hingegen immun gegen Angreifer, die sich die Kontaktlos-Funktion zunutze machen wollen. Das ist selbst dann der Fall, wenn der Täter das Smartphone oder die Smartwatch gestohlen hat. Um überhaupt auf das Wallet zuzugreifen, muss er das Gerät nämlich vorher entsperren. Das ist durch Sie hoffentlich biometrisch und per Geräte-PIN gesichert. Er hat also nur dann eine Chance, wenn er die PIN kennt.

Das Konzept dahinter nennt sich CDCVM („Consumer Device Cardholder Verification Method“). Dabei prüft das Gerät des Kunden, ob es der rechtmäßige Karteninhaber in der Hand hält. Dazu schickt das Handy bei jeder Zahlung im Hintergrund eine individuelle Gerätekontonummer (Device Account Number, DAN) mit, die der Wallet-Dienst bei der Einrichtung zuteilt. Das Gerät gibt diese Nummer unabhän-

gig vom Betrag erst frei, wenn Sie es entsperrt haben. Da nahezu alle Smartphones der letzten Modelljahre Fingerabdruck oder Face ID unterstützen, bringt das keinen Komfortverlust.

Solange der Bildschirm abgeschaltet ist, deaktivieren die meisten Handys außerdem die NFC-Schnittstelle. Es gibt allerdings Ausnahmen: Haben Sie beispielsweise auf einem Samsung-Gerät Smart Lock aktiviert und das Handy über Bluetooth mit einem vertrauenswürdigen Gadget wie Ihren Kopfhörern gekoppelt, bleibt NFC in Bereitschaft. So können theoretisch kleine Beträge doch unbemerkt den Besitzer wechseln. Auch eine Kartennummer kann der Täter auslesen. In diesem Fall ist sie jedoch wertlos.

Token statt Nummer

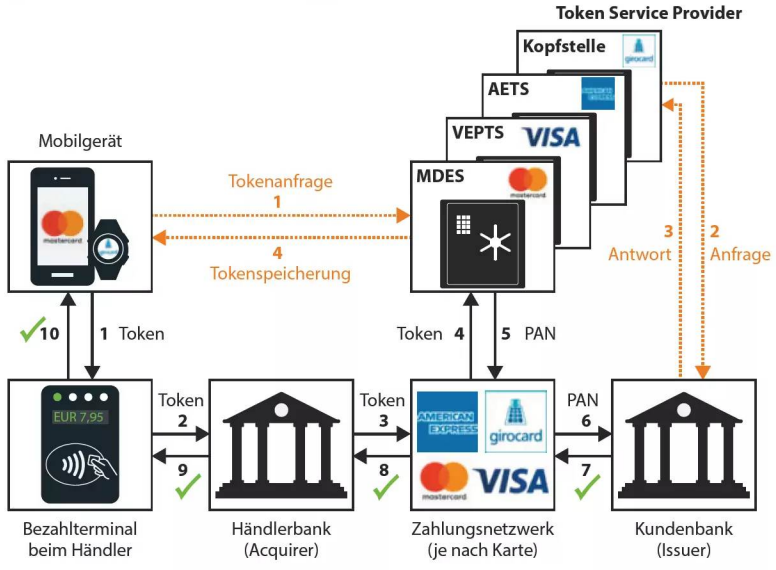
Denn selbst wenn ein Angreifer über NFC an die hinterlegte Kartennummer auf dem Smartphone kommt, kann er damit nichts anfangen. Die kartenherausgebende Bank teilt Ihrem Smartphone nämlich nicht die echte Nummer einer Karte zu, wenn Sie diese im Wallet hinterlegen. Stattdessen erzeugt sie ein gleich langes, statisches Token. Nur diese Pseudo-Kartennummer kommt auf Ihr Gerät und nur das Kartennetzwerk kann sie bei einer Zahlung der tatsächlichen Nummer zuordnen. Genau wie die erwähnte Gerätekennnummer ist dieses Token einzigartig und individuell an Ihr Gerät gebunden.

Zahlen Sie mit dem Gerät, geht außer dem Token aber auch noch die Gerätekennnummer auf die Reise. Um die Sicherheit weiter zu erhöhen, sind beide jedes Mal mit einem Kryptogramm verschlüsselt. Fehlen diese Komponenten oder das Netzwerk erkennt sie als falsch, routet es die Zahlung gar nicht erst an Ihre Bank. Ein Angreifer kann mit der Pseudo-Kartennummer also nicht online shoppen und auch nicht über den Magnetstreifen einer gefälschten Plastikkarte zahlen.

Kennnummer und Kryptogramme liegen in einem besonders geschützten Bereich des Smartphones, an den Angreifer nicht einmal auf einem gekaperten Gerät kommen. Auf iPhones und immer mehr Android-Handys enthält ein kryptografischer Chip – das Secure Element – die Kryptogramme. Android-Handys ohne solche Hardware nutzen die „Host Card Emulation“ (HCE) des Betriebssystems. Ihr Handy speichert nur einen kleinen Vorrat an Kryptogrammen und ergänzt diesen regelmäßig beim Token Service Provider (siehe Infografik rechts). Weder die eine noch die andere Variante ist nach unserer Kenntnis bisher geknackt worden.

Kontaktloses Zahlen per Token

Hält der Kunde das Smartphone oder die Smartwatch an das Bezahlterminal, wird lediglich eine Pseudo-Kartennummer (Token) plus Gerätekennnummer verschlüsselt an die Händlerbank übertragen. Deren Server schickt das Token an das jeweilige Zahlungsnetzwerk, das es schließlich beim eigenen Token Service Provider in die echte Kartennummer (PAN, Primary Account Number) übersetzen lässt und an die Kundenbank übergibt. Sie autorisiert die Zahlung, Zahlterminal und Händlerbank sehen die PAN dabei nicht.



Kulanz bei Schäden

Unabhängig vom technischen Schutz müssen Sie auch selbst etwas für die Sicherheit tun, indem Sie mit den digitalen Karten genauso sorgfältig umgehen wie mit Ihren Plastikkarten. Schützen Sie Ihre (sorgfältig gewählte) Geräte-PIN also ebenso gut wie Ihre Karten-PIN und lassen Sie sich beim Eingeben nicht beobachten. Genau wie bei der Karte müssen Sie zudem sicherstellen, dass Ihr Gerät nicht abhanden kommt. Solange Sie sich an die Nutzungsbedingungen Ihres Kreditinstituts halten, schützt Sie der Gesetzgeber vor allzu hohen Schäden, die Dritte anrichten. Das gilt auch dann, wenn Sie das Gerät tatsächlich verlieren oder jemand es stiehlt.

In solch einem Fall kontaktieren Sie unverzüglich Ihre Bank oder Sparkasse und lassen die Karte

sperren. Bei fast allen Geldhäusern können Sie das auch über die zentrale Notfallnummer 116 116 erledigen. Solange Ihre Plastikkarte noch da ist, reicht es oft praktischerweise, das digitale Äquivalent zu sperren. Zusätzlich können Sie mithilfe der Fernlöschfunktion das Gerät außer Gefecht setzen, sofern dessen Hersteller dies unterstützt.

Wenn Sie Ihren Sorgfaltspflichten nachkommen und nicht grob fahrlässig gehandelt haben, haften Sie genau wie bei der Plastikkarte mit maximal 50 Euro. Was darüber hinausgeht, muss Ihre Bank tragen. Viele Kreditinstitute verfahren sehr kulant; oft müssen Sie nicht einmal die 50 Euro Eigenanteil abschreiben.

Datenschutz von hui bis pfui

Ihr Einkaufsverhalten ist eine Goldgrube für Dienste, die ihr Geld mit personalisierter Werbung verdienen. Je präziser die Daten ausfallen, desto wertvoller sind sie. Egal ob Sie Apple Pay, Google Pay oder die Apps von Volks- und Raiffeisenbanken und Sparkassen nutzen: Über Ihr Wallet oder zumindest über Ihr Betriebssystem klinkt sich ein dritter Akteur in den Bezahlvorgang ein. Wie tief dieser in Ihre persönlichen Vorlieben schauen kann und was er mit diesem Wissen anfängt, hängt vom Geschäftsmodell ab.

Apple erklärt in seiner Datenschutzerklärung und in den Nutzungsbedingungen von Apple Pay und Apple Wallet ausdrücklich, keine Daten auszuwerten. Demnach beschränkt sich der Konzern auf jene Daten, die die Beteiligten brauchen, um die Zahlung abzuwickeln. Diese Aussage ist plausibel: Apple sichert sich einen großen Anteil am Interbankenentgelt, das das Kreditinstitut des Kunden bei einer Kartenzahlung vom Händler verlangt. Angesichts der Einnahmen aus dieser Quelle braucht das Unternehmen die Daten nicht und wirbt stattdessen mit der Datensparsamkeit.

Google ist nicht an den Entgelten beteiligt, die die Händler an die Banken zahlen, sondern verdient sein Geld mit personalisierter Werbung. Das spiegeln auch die Datenschutzbestimmungen von Google Pay wider: Sie führen die Daten auf, die Google für die Zahlung an sich braucht, verweisen aber darüber hinaus auf die Datenschutzerklärung von Google selbst. Die wiederum sichert dem Konzern weitreichende Möglichkeiten, Nutzerdaten zu erheben und auszuwerten. So weiß Google stets, bei welchem Händler Sie wann für welchen Gesamtbetrag eingekauft haben.

Eins weiß Google jedoch nicht: Was genau in Ihrem Warenkorb lag. Dafür bräuchte das Unternehmen einen Vertrag mit dem Händler und dieser eine geeignete Kasse. Dagegen sträubt sich der Einzelhandel aber bisher. Der Nutzer müsste all dem außerdem DSGVO-konform zustimmen – so, wie es Bonusprogramme wie Payback handhaben. Bis zu einem gewissen Grad können Sie auch in Ihrem Google-Konto einschränken, inwieweit Google Ihre Daten erhebt und verwendet. Vollständig unterbinden lässt sich das aber nicht.

Bezahlen Sie auf einem Android-Telefon über die Apps von Volksbank oder Sparkasse, sind Sie deutlich besser vor Googles Datensammelei geschützt. Ihr Kreditinstitut gibt keine Daten weiter; Absturzberichte können Sie in den Apps abschalten. Machen Sie sich aber klar, dass Google abhängig von Ihren Datenschutzeinstellungen trotzdem einen gewissen Einblick erhält. Schließlich kann der Dienst prinzipiell Ihren Standort ermitteln und sieht, wann Sie die Apps bei einem Händler aufrufen. Google sieht jedoch nicht, ob Sie bezahlt haben, geschweige denn, wie hoch der Rechnungsbetrag ausfiel oder was in Ihrem Einkaufskorb lag.

Fazit

Jeder der vier vorgestellten Dienste bewahrt Ihre Kredit- und Debitkarten sicherer auf als Ihr Portemonnaie. Selbst wenn Sie Ihr Handy verlieren, erleiden Sie normalerweise bei keinem der vier Wallets einen Verlust – vorausgesetzt, Sie haben das Gerät mit einer guten PIN gesichert und melden sich unverzüglich bei Ihrer Bank. Beim Bezahlkomfort ist das Smartphone der Plastikkarte ebenfalls überlegen. Anstatt die Karte (oder Bargeld) aus dem Portemonnaie zu nesteln, zücken Sie das Gerät, legitimieren sich und halten es an das Kartenterminal. Die Verfahren sind ausgereift und Probleme an der Kasse die Ausnahme.

Aufpassen sollten Sie beim Datenschutz, zumindest mit einem Android-Handy. Wenn Sie Google Wallet nutzen, sammelt Google zwecks personalisierter Werbeangebote alles, was es kriegen kann. Deutlich besser geschützt sind Ihre Daten hingegen mit den Apps von Sparkassen sowie Volks- und Raiffeisenbanken, vor allem dann, wenn Sie Google in Ihrem Google-Konto die Datensammelei so weit wie möglich einschränken. Dass sich Komfort und Sicherheit auch mit hohem Datenschutzniveau vertragen, zeigt hingegen Apple, bei dessen Wallet wir als Portemonnaie-Ersatz keinen Haken fanden. (mon) c't

Apple- und Google-Pay-fähige Banken
ct.de/wgnh

Zahlen mit dem neuen Giropay

Giropay, das Bezahlsystem deutscher Banken und Sparkassen, hat sich neu erfunden. Es ist schneller, günstiger und vor allem datensparsamer als PayPal und Kreditkarten. Wir erklären die Vorzüge des Systems und warum wir einen Umstieg empfehlen.

Von **Tobias Weidemann**

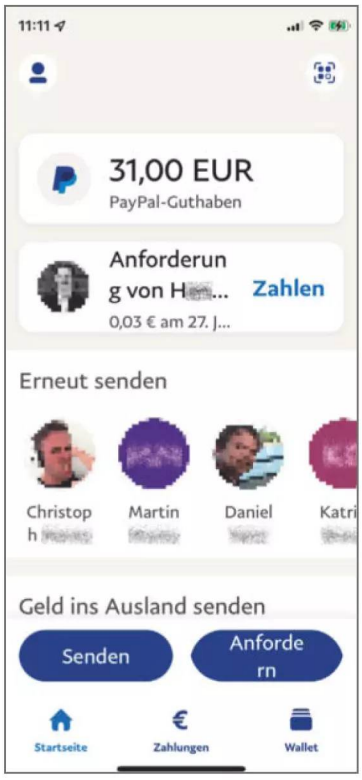
Klick-klick. Ihre neuen Klamotten liegen im Warenkorb, nun geht es an die virtuelle Kasse. Aber welche Bezahlart soll es sein? Neben bekannten und komfortablen Vertretern wie PayPal und Kreditkarte oder auch Rechnung und Lastschrift steht in einigen Shops „Giropay“ zur Auswahl. Sie haben bisher einen Bogen um dieses Feld gemacht? Damit sind Sie nicht allein: Vielen Kunden war das Bezahlverfahren entweder zu umständlich oder sie kannten es nicht einmal. Denn nur vergleichsweise wenige Händler und Marktplätze bieten es bisher überhaupt an – während PayPal, Visa und Mastercard der Standard sind.

Das wollen viele deutsche Banken und Sparkassen nun ändern. Deshalb haben sie Giropay mit dem ebenfalls verschmähten hauseigenen Bezahldienst

Paydirekt zusammengelegt und gründlich renoviert: Das Ganze firmiert jetzt nur noch unter dem Namen „Giropay“. Insbesondere den Bezahlprozess haben die Kreditinstitute stark vereinfacht und eine neue Smartphone-App dafür entwickelt. Damit können Kunden zukünftig sogar online per Girocard shoppen; bisher konnten sie mit der Karte nur an der Ladenkasse zahlen. Wir haben uns das neue Giropay angesehen und nach Hintergründen und weiteren Plänen gefragt.

Bisher nur Nischenprodukte

Paydirekt und Giropay sind im Onlinehandel keine neuen Akteure. Die deutschen Banken und Sparkassen hatten deren Einführung jedoch so lange hinausgezögert, bis die Konkurrenz sich bereits etabliert hatte, und verwirrten ihre Kunden dann mit zwei unterschiedlichen Systemen nebst umständlicher Bedienung. Da half es auch nicht, dass die Daten bei beiden Verfahren auf deutschen Bankservern bleiben.



PayPal ist für den Onlinehandel bislang die Referenz in Sachen Bedienkomfort und Funktionsumfang und den deutschen Bezahlarten weit überlegen. Beim Datenschutz macht der US-Konzern allerdings keine gute Figur.

All das schlug sich in den Marktanteilen nieder. Trotz millionenschwerer Werbezuschüsse für Onlinehändler, die ihren Kunden das Bezahlen per Paydirekt schmackhaft machen sollten, kam der Dienst 2020 gerade einmal auf 3,3 Millionen Zahlungen mit einem Volumen von rund 290 Millionen Euro. Zum Vergleich: Der Gesamtumsatz im deutschen Onlinehandel lag 2022 laut Handelsverband Deutschland (HDE) bei rund 100 Milliarden Euro, und diese Summe enthält noch nicht mal die Umsätze mit Konzerttickets oder Fahrkarten. Den Großteil des Umsatzes wickelten PayPal und Rechnungskauf ab (laut EHI Retail Institute jeweils rund knapp 30 respektive 25 Prozent), gefolgt von Lastschrift und Kreditkarten.

Mittlerweile haben die deutschen Banken die beiden Systeme nun unter dem (passend zur Girocard eingängigeren) Namen „Giropay“ zusammengeführt, wobei die Bezeichnung „Paydirekt“ bald komplett verschwindet. Giropay soll dabei zum einen „der Brückenkopf für die digitalen Zahlungslösungen“ sein, wie es Henning vorm Walde als Geschäftsführer der für das neue Giropay verantwortlichen Paydirekt GmbH formuliert. Zum anderen soll das neue Giropay zum Wallet mit drei Autorisierungsmethoden werden: Zu den beiden alten aus Giropay und Paydirekt gesellt sich die digitale Girocard als neues Verfahren.

Damit verfolgen die Banken laut vorm Walde das Ziel, den Zukunftsmarkt der digitalen Zahlungslösungen nicht den US-Playern zu überlassen. Man wolle das Giropay-Ökosystem „zu einem Omnichannel-Zahlungssystem ausbauen“, heißt es in schönstem Marketingdeutsch – sprich: einem einheitlichen Verfahren für Online- und Offline-Einkäufe.

Frischzellenkur

Auch die deutschen Banken sehen Onlinezahlungen einem Bankenvertreter zufolge mittlerweile als wichtigsten Zukunftsmarkt. Dabei wollen sie es den Kunden beim bargeldlosen Zahlen möglichst einfach machen. Und tatsächlich: Mit dem neuen Giropay zahlt es sich deutlich komfortabler als früher.

Die wichtigste Voraussetzung für den Kunden ist dabei, dass sein Kreditinstitut Giropay unterstützt. Dazu zählen insbesondere die Sparkassen, fast alle Genossenschaftsbanken, außerdem Postbank, Deutsche Bank, Commerzbank und Comdirect sowie die HypoVereinsbank. Die ING hat Giropay ausgemustert (nicht aber Kwitt, siehe Kasten „Kwitt: Haste mal ’ne Mark?“ auf S. 52). Ebenso fehlen zum Beispiel DKB,

Santander und Targobank, außerdem alle Neobanken wie N26 oder Tomorrow.

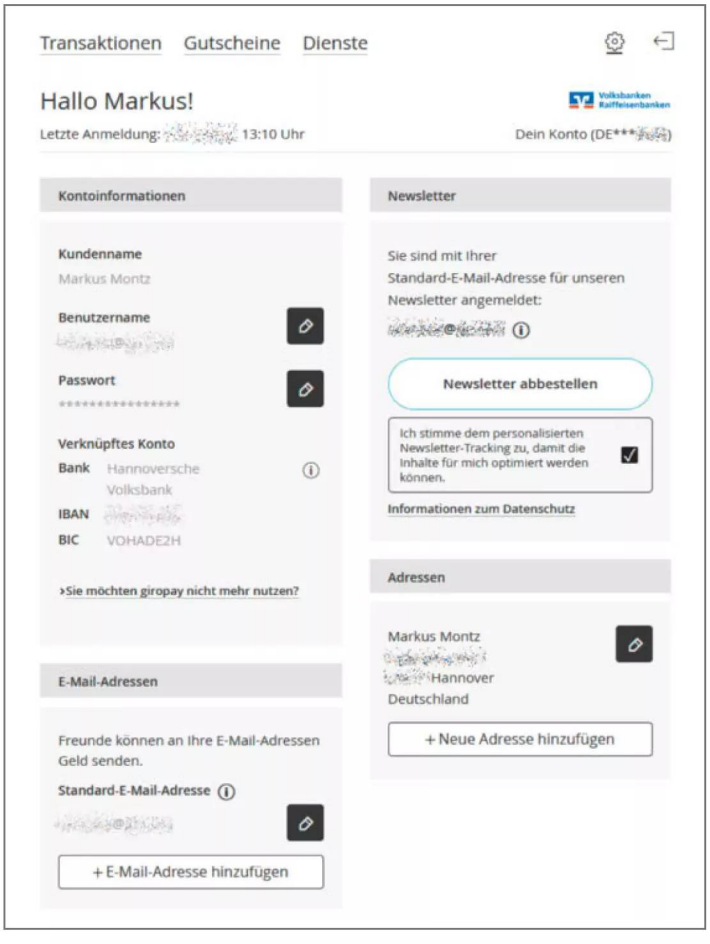
Zunächst muss man im Onlinebanking ein Giropay-Nutzerkonto anlegen. Einzig dieser Prozess ist noch etwas umständlich, die Mühe lohnt sich aber. Anschließend installiert man die Giropay-App für Android oder iOS und meldet sich an. Wählt man Giropay nun in einem Onlineshop am PC als Bezahlmethode, klickt man in der nachfolgenden Auswahl für den einfachsten Weg auf „Giropay-Login“ (die „Online-Überweisung“ als zweite Option kann man getrost ignorieren). Anschließend startet man die neue Giropay-App auf dem Handy und authentifiziert sich mit vierstelliger PIN, Fingerabdruck oder Gesichtserkennung.

Nun scannt man mit der App nur noch einen QR-Code auf dem PC-Bildschirm, fertig. Tempo und Komfort sind PayPal mehr als ebenbürtig. Kauft der Kunde via Handy ein, leitet der Onlineshop ihn zu Giropay, wo er im Modus „Giropay-Login“ mit einem Klick die Giropay-App erreicht. Dort gibt er die Zahlung nach der Authentifizierung per PIN, Fingerabdruck oder Gesichtserkennung ähnlich einfach frei.

Selbst ohne Smartphone ist das Verfahren komfortabler als früher. Je nach eigenen Einstellungen im Onlinebanking und in Giropay entfällt nun bei Beträgen unter 30 Euro oftmals die Authentifizierung über die Bank; es genügen Giropay-Nutzername und Passwort.

Besonders ins Auge sticht auf Android-Handys jedoch ein dritter Weg: die digitale Girocard. Die Idee dahinter: Kunden bezahlen an der Ladenkasse und online mit demselben statt mit unterschiedlichen Mitteln. Die digitale Girocard steht zunächst Kunden von Sparkassen sowie Volks- und Raiffeisenbanken zur Verfügung. Auch dafür muss man das Giropay-Nutzerkonto einrichten und dann zusätzlich die institutseigene Bezahl-App „Mobiles Bezahlen“ respektive „Pay“ installieren. Darin hinterlegt man eine Girocard (wie das technisch funktioniert und weshalb es sicher ist, erklären wir im Artikel „Sicher mit dem Smartphone bezahlen“ auf S. 40). Beim Bezahlen wählt man dann die „Digitale Girocard“. Anschließend leitet Giropay in die Bezahl-App weiter, in der man sich per PIN, Fingerabdruck oder Gesichtserkennung authentifiziert.

Ob, wann und wie die ersten Privatbanken wie die Deutsche Bank oder Direktbanken wie die Comdirect ihr Giropay-Angebot um die digitale Girocard erweitern, ist indes noch offen. Auch iOS-Nutzer müssen fürs Erste noch auf die digitale Girocard als dritte Option in ihrem Giropay verzichten. Grundsätzlich wären iPhone & Co. aber dazu fähig, schließlich kann man als Sparkassenkunde schon seit Mitte 2021 über Apple Pay in Onlineshops mit der Girocard zahlen.



Giropay schaltet man im Onlinebanking seines Kreditinstituts frei. Anschließend passt man seine Einstellungen im Nutzerportal von Giropay an.

Die Konkurrenz schläft nicht

Die digitale Girocard ist eine Antwort auf Mastercards Schritt, sein Zweitsystem Maestro ab Juli 2023 abzukündigen, über das viele Girocard-Nutzer bislang im Ausland bezahlten. Die reine Girocard funktioniert hingegen nur in Deutschland. Viele Beob-

achter sehen in Mastercards Entscheidung daher auch die Absicht, der Girocard langfristig Marktanteile zugunsten der eigenen Mastercard-Debitkarten abzunehmen. Dabei dürften Mastercard und quasi nebenbei auch Visa darauf hoffen, dass die Banken entweder nur noch deren reine Debitkarten ausgeben oder die Girocard zukünftig mit diesen Debitkarten anstelle von Maestro oder Visas V Pay kombinieren (mehr zu diesen Debitkarten und dem Unterschied zu Girocard und Kreditkarte im Artikel „Girocard versus Debitkarten“ auf S. 28).

Bei der Euro Kartensysteme, einem Dienstleister der Banken und Sparkassen für die Vermarktung und Technik der Girocard, gibt man sich nach außen jedoch entspannt. „Was Maestro angekündigt hat, macht uns jetzt keine Angst“, so Geschäftsführer Oliver Hommel. „Denn zum einen ist die Kooperation ja erst einmal nur bei ab Mitte 2023 ausgegebenen Karten nicht mehr dabei und läuft erst nach und nach über die nächsten vier Jahre aus. Zum anderen sehen wir, dass die meisten Institute ihre Girocards mit einer Debit-Mastercard oder mit Visa Debit kombinieren und die Girocard damit im Ausland weiterhin einsetzbar bleibt.“

Dennoch: Ohne die jetzt nachgerüstete Online-Bezahlfunktion dürfte die Girocard gegenüber den Debitkarten von Visa und Mastercard langfristig kaum konkurrenzfähig bleiben, denn mit diesen kann man bereits im Internet einkaufen. Dass die deutschen Banken nun nachziehen, hilft aber keineswegs nur den Kreditinstituten, sondern entlastet auch das Portemonnaie der Verbraucher. Denn für Zahlungen mit der digitalen Girocard müssen Händler geringere Gebühren an ihre Zahlungsdienstleister entrichten als beim Einsatz von Debit- und insbesondere Kreditkarten von Visa und Mastercard (siehe Artikel „Girocard versus Debitkarten“ auf S. 28).

Während Händler für den Einsatz der Girocard je nach Zahlungsdienstleister meist rund 0,2 bis 0,3 Prozent Provision inklusive Sockelbetrag von einigen Cent entrichten, können es bei einer der beiden großen Kreditkarten je nach Vertragsgestaltung zwischen 0,7 und 0,9 oder mehr Prozent sein.

Im Internet ist es meist noch mehr. Die reine Visa- und Mastercard-Debitcard ist für den Handel zwar etwas günstiger, liegt aber oftmals ebenfalls nur knapp unter einem Prozent. Verbraucher sehen diese Kosten zwar nicht auf dem Kassenbon, die Händler legen sie aber auf ihre Endpreise um.

Weiteres Ausbaupotenzial

Bei der Umgestaltung von Giropay haben die deutschen Banken mehr denn je mit den Onlinehändlern zusammengearbeitet, wie ein Vertreter eines großen Handelskonzerns berichtet. Für Handelsunternehmen (auch stationäre) bedeute dies eine bisher nicht gekannte Dynamik, wenn sie neue Funktionen in Giropay vorschlagen. Hinzu kommt, dass vor allem das Girocard-System dem stationären Handel schon lange weitgehende Sicherheit vor nicht gedeckten und zurückgewiesenen Zahlungen bietet. Das macht die Kombination aus Girocard und Giropay für den Handel attraktiver. Die deutsche Kreditwirtschaft setzt also einige Hebel in Bewegung, damit ihr neues, komfortableres Zahlungsverfahren auch in den (Online-)Shops ankommt: Kunden können sich berechtigte Hoffnungen machen, dass es sich etabliert und mehr und mehr Funktionen hinzukommen.

So wünscht sich die Wirtschaft beispielsweise eine Zusammenarbeit mit Bonusprogrammen, damit Kunden einfacher Treuepunkte sammeln können. Eine Altersverifikation für den Handel nimmt derzeit konkrete Formen an. Sie könnte etwa in kassenlosen Supermärkten helfen oder bei Lieferdiensten, die Spirituosen und Tabakwaren anbieten. Auf der Liste stehen außerdem In-App-Käufe und regelmäßig wiederkehrende Zahlungen; die Tourismusbranche wünscht sich, mit Giropay zusätzliche Nächte vor Ort buchen zu können. All das geht bislang eleganter über die Kreditkarte.

Das Ende der technisch möglichen Entwicklung wäre damit noch lange nicht erreicht: Die Banken könnten pro Girokonto beliebig viele digitale Girocards ausgeben, sodass nicht nur der Kunde, sondern auch einige Systeme in seinem vernetzten Gerätezoo eine eigene Karte bekommen. Beispielsweise könnte das E-Auto mit seiner eigenen Girocard automatisch an der Ladesäule oder im Parkhaus bezahlen – „Seamless Payment“ nennt sich dieses Bezahlen ohne explizite Kassenzone.

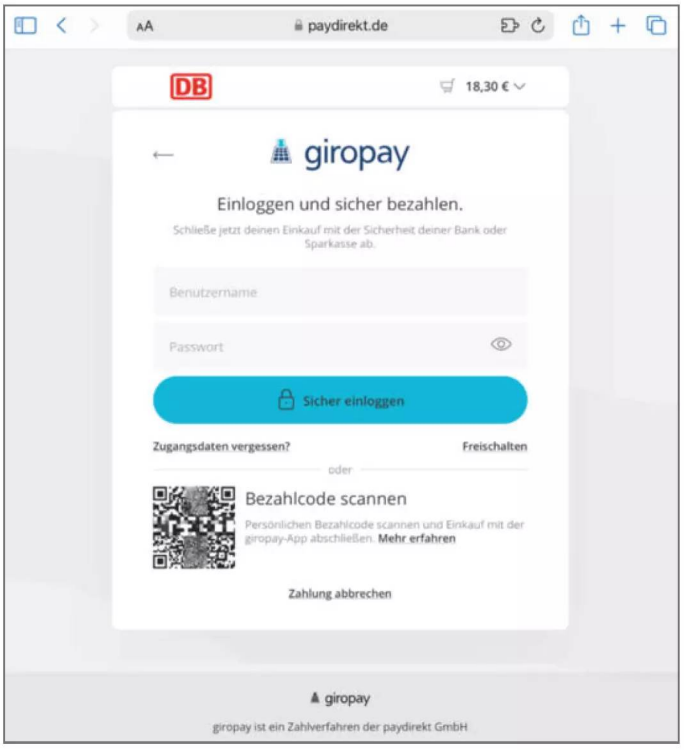
Lässt Giropay damit womöglich PayPal und Kreditkarten hinter sich? Ralf Gladis vom Zahlungsabwickler Computop ist der Meinung, dass sowohl die Kreditkarten als auch die Girocard, respektive Giropay, in Zukunft ihre Daseinsberechtigung haben. „Die Kreditkarte ist eindeutig teurer für den Handel, aber sie bietet zumindest bisher auch deutlich mehr Funktionen, die im Girocard-Lager erst nach und nach entwickelt werden müssen.“ Der Handel könne daher bestimmte Bezahllösungen wie Upgrades, regelmäßig wiederkehrende Transaktionen für Abonnements oder internationale Lösungen bislang einfacher über Visa- und Mastercard abwickeln. Kreditkarten lohnen sich für den Handel auch noch aus einem anderen Grund: „Kunden geben mit der Kreditkarte oftmals mehr Geld aus, da sie die Abbuchung erst im nächsten Monat haben“, so Gladis.

Computop und andere Zahlungsabwickler haben die Shop-Systeme zahlreicher Onlinehändler an die Giropay-Welt angebunden und mussten parallel auch ihre eigenen Schnittstellen an die neue API anpassen. Das ist zunächst mit Aufwand verbunden, lohnt sich aber aus Gladis‘ Sicht: „Die gute Nachricht aus Sicht der Händler ist, dass sich das in Zukunft sowohl technisch als auch vertraglich einfacher umsetzen lassen wird. Denn mit dem neuen Giropay haben auch die Zahlungsdienstleister nur noch einen Ansprechpartner. Der funktioniert wie ein Acquirer [Vertragspartner des Händlers, die Red.] und macht einen Preis und Vertrag.“

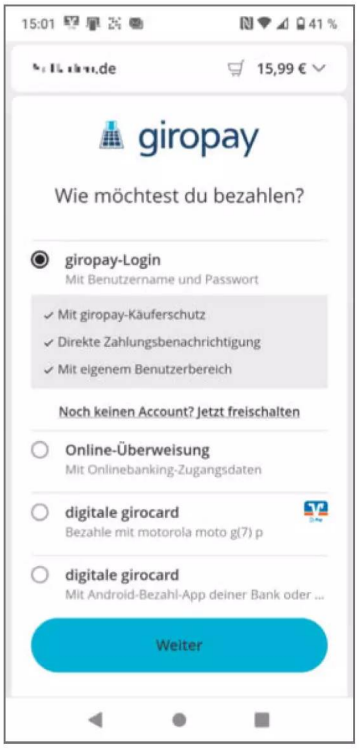
Vorteil Datenschutz

Die Themen Datenschutz und Privatsphäre waren und sind aus Kundensicht ein großer Vorteil gegenüber den US-Konzernen. Denn die Kundendaten bleiben ausnahmslos in Deutschland. Doch auch technisch verfolgt das Girosystem einen datensparsameren Ansatz als die US-Anbieter. Dieser stützt sich auf Unique User IDs (UUID). Diese tauschen der Zahlungsdienstleister oder die Bank des Händlers und die Kundenbank verschlüsselt als Platzhalter (Token) aus, wenn sie die Zahlung autorisieren und auslösen. Nur die Kundenbank kann sie dem Kunden zuordnen. Abgesehen vom Zahlungsvorgang prüfen die Beteiligten die Daten ansonsten lediglich auf Muster für Geldwäsche und Betrug.

Auch die Konzeption des Giropay-Systems selbst verhindert, dass jemand die Transaktionen analysieren und für weiterreichende Marktforschung oder Datenhandel zweckentfremden kann. „Im Gegensatz zu anderen Bezahldiensten ist so kein externer Dritter involviert, wir nutzen die Daten weder für Werbezwecke noch für Warenkorbanalysen“, erklärt Paydirekt-Geschäftsführer Henning vorm Walde. Eine Besonderheit ist nämlich der dezentrale Ansatz:



Bezahlen, wie man es sich 2023 im Netz vorstellt: Einfach Giropay-App öffnen, mit Fingerabdruck oder Face-ID authentifizieren, QR-Code scannen und fertig ist die Laube.



Die digitale Girocard kommt auf Android-Handys. Den Anfang machen die Sparkassen sowie die Volks- und Raiffeisenbanken.

Giropay verrechnet die Zahlung der Kunden nicht selbst, vielmehr wickeln Händler und Kundenbank sie direkt miteinander ab. „Kurzum: Wir autorisieren direkt gegen das Konto, die Daten liegen bei der einzelnen Bank“, so vorm Walde. Die Bank wiederum darf die Daten nur mit ausdrücklichem Einverständnis des Kunden für weitergehende Zwecke verwenden, ebenso der Händler.

Ausblick: Guter Start, offene Fragen

Das neue Giropay wirkt verheißungsvoll, auch aus Kundensicht. Zum Glück sind sich die beteiligten deutschen Privatbanken sowie Genossenschaftsbanken und Sparkassen inzwischen weitgehend einig, dass Girocard und Giropay über ihre zukünftige Rolle im Zahlungsverkehr mitentscheiden. Allerdings handelt auch weiterhin jedes Institut für sich, sprich: Jede Privatbank und jede der 370 Sparkassen und 770 Genossenschaftsbanken bestimmt selbst, ob, wie und zu welchen Konditionen sie ihren Kunden das digitale Zahlungsverfahren anbieten. Welche Möglichkeiten der Kunde abseits der Basisfunktionen erhält, liegt also in den Händen seiner jeweiligen Bank. Dabei ist Kwitt, der P2P-Zahlungsdienst im Giropay-System, noch gar nicht einbezogen (siehe Kasten „Kwitt: Haste mal ’ne Mark?“ auf S. 52).

Am Ende werden die Banken aber nur erfolgreich sein, wenn sie ihre Kunden und den Handel mit Komfort, Einheitlichkeit und einem kompletten Angebot für alle Lebenslagen überzeugen. Denn gerade die Kunden dürften ihre eingespielten Zahlungswege wie Rechnungskauf, PayPal oder Kredit-

Kwitt: Haste mal 'ne Mark?

Ebenfalls zur Dachmarke Giropay gehört das P2P-Bezahlsystem Kwitt, über das sich Privatpersonen mithilfe ihrer Handynummern Geld schicken können. Kwitt ist bisher Teil von Onlinebanking-Apps für Smartphones. Lange Zeit boten es vor allem die Sparkassen und Volks- und Raiffeisenbanken an, mittlerweile sind ING und Commerzbank hinzugestoßen. Auch Kwitt soll mit Giropay zusammenwachsen. Will man bargeldlos Geld für ein Geburtstagsgeschenk einsammeln, sich unterwegs gegenseitig Geld leihen und zurückzahlen oder auf dem Flohmarkt kleine Beträge an andere Privatleute schicken, regelt man das hierzulande vorrangig über PayPal – während dafür beispielsweise in der Schweiz Twint, in Spanien Bizum und in Dänemark MobilePay die Mittel der Wahl sind.

In der Giropay-App ist eine rudimentäre P2P-Zahlungsfunktion bereits implementiert. Doch genau wie bei Kwitt kann das System Geld nur an Kontakte aus dem eigenen Adressbuch im Smartphone übertragen – eine Einschränkung, die beispielsweise für Zahlungen auf dem Flohmarkt unpraktischer ist als die Abwicklung per PayPal. Hinzu kommt, dass Sparkassen-Kunden bisher mit der Giropay-App kein Geld senden können. Wann und in welchem Umfang weitere P2P-Funktionen in Giropay einfließen, beispielsweise Zahlungen an Personen ohne Adressbucheintrag, ist noch offen. Die Erfahrungen im Ausland zeigen aber, dass ein offenes P2P ein enorm nachgefragtes Anwendungsfeld ist.

Kwitt gehört nominell zu Giropay, es bleibt aber vorerst Teil der Onlinebanking-Apps der Banken, die es anbieten.

karte nur aufgeben, wenn es ihnen spürbare Vorteile bringt. Bei der Bedienung haben die Banken ein Zwischenziel erreicht: Das neue Giropay ist nicht mehr nur datenschutzfreundlich, sondern funktioniert für Kunden sogar so komfortabel wie PayPal & Co. Wir können es daher (endlich!) ausdrücklich empfehlen.

Die Branche ist aber noch lange nicht am Ziel, weder an der Ladenkasse noch im Onlinehandel. Insbesondere bei P2P-Zahlungen könnte sie sich mehr von den europäischen Nachbarn zum Beispiel in der Schweiz oder in Dänemark abgucken und dort Angebote schaffen, wo PayPal, Visa und Mastercard für Verkäufer – vor allem kleingewerbliche und private – zu teuer und zu aufwendig sind (siehe Kasten „Kwitt: Haste mal 'ne Mark?").

Auch den Datenschutztrumpf könnten Banken und Sparkassen stärker ausspielen und viel deutlicher mit dem hohen Maß an Privatsphäre werben. Anders ausgedrückt: Ein Zahlungsdienst wie Klarna analysiert Käufe und Warenpräferenzen, um Marktforschung zu betreiben; das ist Teil seines Geschäftsmodells. Bei PayPal kann man sich nie ganz sicher sein, welche Daten in den USA landen. Die deutschen Banken setzen dem mit Giropay ein System entgegen, das die sensiblen Daten ihrer Kunden schützt. Sie besinnen sich damit bewusst oder unbewusst auf einen alten Wert: Vertraulichkeit. (mon) **c't**

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Torsten Beeck (tbe)
(verantwortlich für den Textteil)

Konzeption: Markus Montz (mon)

Koordination: Jobst Kehrhahn (Leitung, keh), Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Jo Bager (jo), Mirko Dölle (mid), Wilhelm Drehling (wid), Tim Gerber (tig), Ulrike Kuhlmann (uk), Markus Montz (mon), Georg Schnurer (gs)

Mitarbeiter dieser Ausgabe: Nick Akinci, Tobias Weidemann

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Dörte Bluhm, Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Kapell, Steffi Martens, Marei Stade, Matthias Timm, Christiane Tümmler, Ninett Wagner

Digitale Produktion: Christine Kreye (Ltg.), Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Albert Hulm, Berlin; Andreas Martini, Wettin

Titel: Steffi Martens, www.freepik.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 22.08.2023

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Giropay

Die deutsche Kreditwirtschaft hat ihre Online-Bezahldienste Paydirekt und Giropay vereint und dem Ganzen ein großes Komfort-Upgrade spendiert. Wir beantworten die wichtigsten Fragen zur deutschen Antwort auf PayPal & Co.

Von **Markus Montz**

FAQ

Voraussetzungen

Was benötige ich, um Giropay nutzen zu können?

Wenn Sie mit Giropay zahlen wollen, brauchen Sie ein Girokonto bei einem deutschen Kreditinstitut, das Giropay unterstützt (siehe Artikel „Zahlen mit dem neuen Giropay“ auf S. 46). Zu den angeschlossenen Instituten zählen momentan die Sparkassen, die Volks- und Raiffeisenbanken, die Deutsche Bank, die Postbank, die Commerzbank, die Comdirect, die Sparda-Banken, die PSD-Banken, die HypoVereinsbank, die BW Bank, die GLS Bank, die BBBank, die Norisbank, die Degussa Bank und MLP. Aus dem Bezahldienst für Onlineshops ausgestiegen ist dagegen die ING.

Die zweite Voraussetzung ist ein Onlinebanking-Zugang. Darin aktivieren Sie Ihr Giropay-Nutzerkonto und bestätigen spätere Änderungen an Ihren Daten. Außerdem muss der Onlineshop, bei dem Sie einkaufen, Giropay anbieten. Meist handelt es sich dabei um deutsche Händler, prinzipiell können aber auch ausländische Shops Giropay einbinden.

Giropay aktivieren

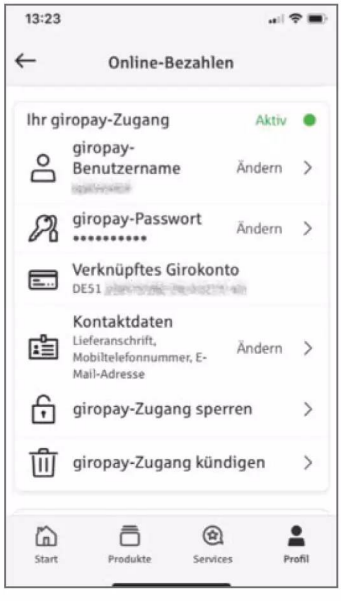
Okay, ich habe die Voraussetzungen erfüllt. Wie richte ich Giropay ein?

Im Onlinebanking Ihres Instituts navigieren Sie zunächst zum Punkt „Giropay“. Gelegentlich firmiert Giropay dort auch noch unter dem Vorgängernamen „Paydirekt“. Anschließend bestimmen Sie den Nutzernamen und das Passwort, mit denen Sie Giropay später verwenden. Außerdem hinterlegen Sie eine Telefonnummer und eine Mailadresse, über die zum Beispiel Sicherheitsabfragen kommen. Die Daten bestätigen Sie am Ende mit der Zwei-Faktor-Authentifizierung Ihrer Bank. Weitere Einstellungen nehmen Sie im Giropay-Nutzerkonto vor.

Einstellungen

Wo verwalte ich mein Giropay-Nutzerkonto?

Die Einstellungen für Giropay legen Sie im Kundenportal fest, das Sie im Browser über giropay.de erreichen. Beim Login leitet Giropay Sie auf die Präsenz des Vorgängerdienstes paydirekt.de um. Das ist irritierend, es ist aber technisch sicher. Dort



Ihre Kerndaten richten Sie im Onlinebanking Ihres Kreditinstituts ein und verwalten sie dort. Bei einigen (hier den Sparkassen) geht das auch in der Banking-App.

loggen Sie sich mit dem Nutzernamen und dem Passwort ein, die Sie im Onlinebanking Ihres Kreditinstituts für Giropay vergeben haben.

Im Kundenportal können Sie die Einstellungen für Ihr Giropay-Nutzerkonto ändern, zum Beispiel Nutzernamen oder Mailadresse. Giropay führt Sie dafür in manchen Fällen in Ihr Onlinebanking weiter und Sie bestätigen den Vorgang dort anschließend mit einer TAN oder einem anderen zweiten Faktor. Sie können in den Einstellungen außerdem eine Mobilnummer festlegen, wenn Sie über Giropay auch Geld an andere Giropay-Nutzer im Adressbuch Ihres Smartphones schicken und von diesen empfangen wollen.

Giropay-App

? Wozu dient die Giropay-App?

Vorweg: Die App ist ein Kann, kein Muss. Wenn Sie ein Smartphone besitzen, können Sie Zahlungen mithilfe der App aber sehr komfortabel freigeben – egal, ob Sie am PC oder auf dem Smartphone selbst shoppen. Es genügt eine vierstellige PIN, ein Fingerabdruck oder Face ID. In der App finden Sie außerdem eine (eher schlecht als recht gemachte) P2P-Zahlungsfunktion für die Kontakte in Ihrem Smartphone. Die Zahlungshistorie verschafft Ihnen einen Überblick und die Möglichkeit, Zahlungen zu reklamieren. Ihr Nutzerkonto können Sie über die App jedoch nicht verwalten – dazu müssen Sie sich im Browser einloggen.

Probleme mit Comdirect-Konten

? Ich bin Comdirect-Kunde. Wenn ich die Giropay-App auf dem Smartphone einrichten will, zeigt dieses mir für die Authentifizierung einen Farbmatrixcode an. Mit der photoTAN-App auf demselben Gerät kann ich den aber nicht scannen und bekomme die TAN nicht. Was soll ich tun?

! In der Tat, die Push-Freigabe der photoTAN-App funktioniert bei der Comdirect in Drittanbieter-Apps wie Giropay (immer noch) nicht. Das Workaround: Leiten Sie den Vorgang auf Ihrem Smartphone ein und brechen ihn zunächst ab, wenn der Farbmatrixcode erscheint. Danach loggen Sie sich auf einem anderen Gerät über den Browser in das Giropay-Kundenportal ein. Dort navigieren Sie in den Einstellungen nach unten zum Feld „App“ und schließen die Einrichtung ab. Das Bezahlen auf dem Smartphone funktionierte mit der Giropay-App anschließend problemlos – ohne die App bleibt das Problem.

Im Onlineshop

? Wie zahle ich mit Giropay?

! Grundsätzlich haben Sie derzeit zwei Möglichkeiten, wenn ein Shop Giropay als Bezahloption anbietet. Die einfachste ist das „Giropay-Login“: Am PC geben Sie Nutzernamen und Passwort ein und bestätigen die Zahlung bei Bedarf mit der Zwei-Faktor-Authentifizierung Ihres Onlinebankings. Haben Sie die Giropay-App auf dem Smartphone installiert, können Sie damit auch den Bezahlcode abscannen. Anschließend geben Sie die Transaktion mittels PIN, Face ID oder Fingerabdruck frei und sind fertig. Für Einkäufe auf dem Smartphone empfehlen wir ebenfalls die Giropay-App. Diese rufen Sie beim Check-out mit einem Klick auf und authentifizieren sich wie beim Scan des Codes. Alternativ tun Sie dies im Smartphone-Browser, der Ablauf ist wie am PC.

Mit der Option „Online-Überweisung“ leitet Giropay Sie zu einer speziellen Giropay-Seite Ihres Kreditinstituts weiter. Dort loggen Sie sich mit Ihren Onlinebanking-Zugangsdaten ein, finden eine vorausgefüllte Überweisung an den Händler vor und schicken diese nach der obligatorischen Zwei-Faktor-Authentifizierung ab. Für diese Variante brauchen Sie sich übrigens nicht einmal zu registrieren – aber Ihre Bank muss Giropay anbieten.

Käuferschutz

? Hat Giropay einen Käuferschutz?

! Ja. Bevor Sie ein Käuferschutzverfahren einleiten, sollten Sie wie bei PayPal zunächst versuchen, Probleme bilateral mit dem Händler zu lösen. Können Sie sich nicht einigen, loggen Sie sich in Ihr Giropay-Kundenportal oder die Smartphone-App ein. Dort rufen Sie die Zahlungshistorie („Transaktionen“) auf und können zu jeder einzelnen Zahlung ein „Problem melden“. Genau wie bei PayPal müssen Sie sich an die Regeln des Verfahrens halten und auf Rückfragen fristgerecht antworten.

Mehrere Girokonten

? Kann ich Giropay nutzen, wenn ich bei meiner Bank mehrere Girokonten führe, zum Beispiel ein Privat- und ein Geschäftskonto?

Das kommt darauf an, ob Sie für diese Girokonten eigene Onlinebanking-Zugänge haben oder nicht. Für jeden Onlinebanking-Zugang können Sie nur ein Giropay-Konto anlegen, egal, wie viele Girokonten Sie darunter führen. Sofern Sie mehrere Giropay-Konten bei derselben Bank brauchen, müssen Sie dort also mehrere Onlinezugänge einrichten lassen.

Verweigerte Zahlung

Meine Zahlung wurde abgewiesen – was ist da los?

Genau wie bei anderen Zahlungsarten kann ein Beteiligter eine Giropay-Zahlung durchaus im Prozess oder nachträglich stornieren. Infrage kommen der Händler, sein Zahlungsabwickler und seine Bank – oder Ihre (Kunden-)Bank. Die Gründe können ebenso vielfältig sein. Wir empfehlen, zunächst den Händler, dann die eigene Bank und erst zum Schluss den Giropay-Service anzusprechen. Giropay stellt letztlich nur das System bereit. Die eigentliche Zahlung wickeln die Banken untereinander direkt ab.

Was ist dieses „Paydirekt“?

Warum erscheinen immer mal wieder Hinweise auf „Paydirekt“?

Das aktuelle Giropay ist 2021/22 aus den Diensten Giropay und Paydirekt entstanden. Beide standen (und stehen) unter dem Dach der deutschen Kreditwirtschaft. Die Fusion ist aber noch nicht überall komplett abgeschlossen. Bei manchen Banken firmiert Giropay daher noch unter dem Namen „Paydirekt“, auch anderswo stoßen Sie auf den Begriff. Loggen Sie sich auf giropay.de in Ihr Nutzerkonto ein, leitet Giropay Sie zum Beispiel auf paydirekt.de um. Technisch ist das sicher, allerdings verwirrt es viele Nutzer – und Verwirrung nutzen auch Cyberkriminelle gerne. Daher sollten Giropay und die Banken das Durcheinander möglichst schnell beseitigen.

Giro, Giro, Giro

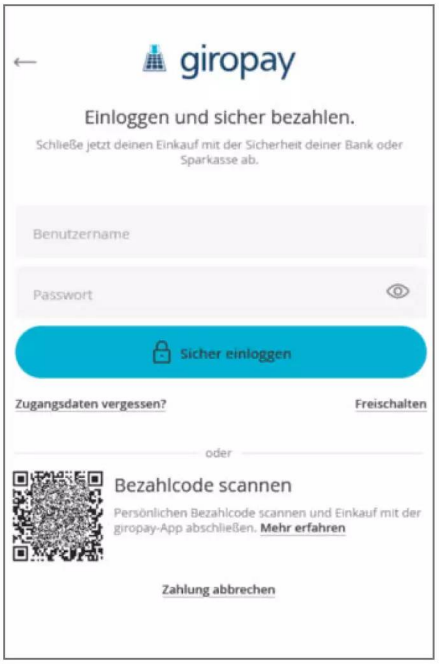
Girocard, Giropay, Girokonto – was ist da eigentlich der Unterschied?

Die Girocard, früher „EC-Karte“, ist die Debit-Bezahlkarte (siehe Artikel „Girocard versus Debitkarten“ auf S.28) der Deutschen Kreditwirtschaft (DK) für den stationären deutschen Einzelhandel. Online kann man sie nur als Sparkassen-Kunde mit Apple Pay einsetzen. Giropay ist das Bezahlsystem der DK für den Onlinehandel. In der Funktionsweise lehnt es sich an seinen Konkurrenten PayPal an. Ihr Girokonto ist das Zahlungskonto, das Sie bei Ihrer Bank führen. Zahlen Sie mit Girocard oder Giropay, belastet Ihre Bank den Betrag auf dem Girokonto.

Unterschiede zu „Twint“

Kann ich mit Giropay ähnlich wie mit dem schweizerischen Twint auch direkt an Hofläden oder Flohmarkthändler zahlen?

Nein. Die Giropay-App ist für Onlinezahlungen in Shops mit Giropay-Akzeptanzpartner gedacht. Sie hat zwar ein P2P-Bezahlsystem, es ist aber sehr unkomfortabel. Außerdem können Sie Geld nur an Kontakte im eigenen Smartphone schicken oder von diesen anfordern. Damit ist Giropay für die genannten Einsatzzwecke nicht geeignet. Etwas einfacher zu bedienen ist Giropay-Kwitt, das Sie in den Smartphone-Apps teilnehmender Banken finden – die Reichweite unterliegt aber denselben Einschränkungen.



Am PC scannen Sie beim Checkout mit der Giropay-App den QR-Code und bestätigen dort die Zahlung. Auf dem Smartphone gelangen Sie über einen Button in die App.

Sicherheit

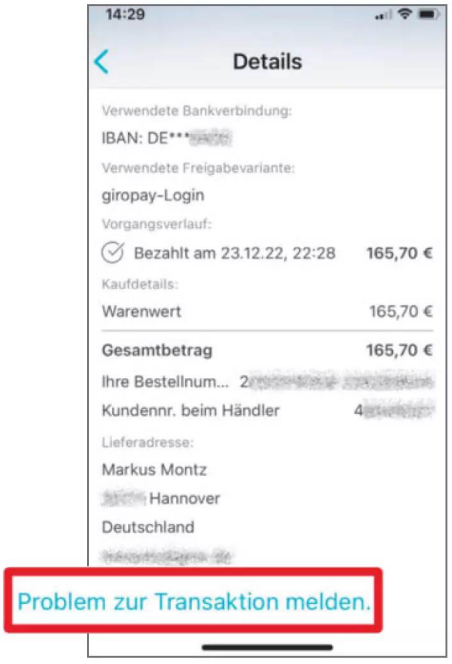
Wie sicher ist Giropay?

Sehr sicher. Zahlungen sind spätestens ab 30 Euro mit einer Zwei-Faktor-Authentifizierung abgesichert, Sie können diese im Giropay-Nutzerkonto aber auch für sämtliche Zahlungsbeträge unabhängig von der Höhe aktivieren. Bei Verschlüsselung und Transportsicherheit unterliegt Giropay denselben Standards wie das Onlinebanking Ihrer Bank. Für Angriffe, die das Opfer zu Fehlern verleiten sollen („Social Engineering"), ist es aber ebenso ein potenzielles Ziel wie andere Dienste auch.

Zahlung ohne Konto beim Händler

Hat Giropay eine Funktion wie „direkt zu PayPal", mit der Händler auch gleich meine Adresse bekommen und ich kein Kundenkonto einrichten muss?

Nein, bislang nicht. Wir empfehlen, bei dieser Funktion generell den Komfort und das nicht benötigte Kundenkonto gegen die fehlende Kontrolle über die Datenweitergabe an den Händler abzuwägen.



In den Details zu jeder Zahlung haben Sie die Möglichkeit, Probleme zu melden und ein Käuferschutzverfahren einzuleiten.

Cashback

Bietet Giropay ein Cashback?

Nein. Bislang gibt es nur Rabattaktionen, die einzelne Händler für begrenzte Zeit anbieten. Um davon zu erfahren, müssen Sie aber den Giropay-Newsletter abonnieren.

Vergleich zu PayPal

Klingt kompliziert. Ist PayPal dann nicht doch die bessere Wahl?

Das kommt auf Ihre persönlichen Präferenzen an. PayPal punktet auf der Habenseite vor allem mit Reichweite und Präsenz in vielen Onlineshops, auch international. Hinzu kommt das komfortable P2P-Bezahlsystem, mit dem Privatpersonen Zahlungen untereinander abwickeln können – das für Verkäufer allerdings vergleichsweise teuer ist, wenn die Zahlung mit einem Käufer- und Verkäuferschutz abgesichert sein soll. Dafür werden PayPal-Konten trotz eines technisch soliden Sicherheitsniveaus systembedingt häufiger von Betrügern gekapert. Die wiederum nutzen gerne die Grenzen des Käuferschutzes aus (siehe Artikel „PayPal-Betrug auf Kleinanzeigenportalen" auf S. 108). Problematisch ist außerdem der Datenschutz, weil Sie quasi ein Zwischenkonto führen, dessen Daten auch über Server in den USA fließen. PayPal nutzt Ihre Daten außerdem für persönliches Marketing, solange Sie diese Option nicht abschalten.

Beim Datenschutz wiederum liegt die Stärke von Giropay: Die Zahlungen fließen direkt von Girokonto zu Girokonto, die Daten bleiben in Deutschland und Werbung findet allenfalls über Newsletter statt. Da Händler einen Akzeptanzpartner benötigen und P2P-Zahlungen auf dem Smartphone nur an Kontakte in Ihrem Telefonbuch möglich sind, ist Giropay außerdem unattraktiv für Betrüger. Das reduziert allerdings auch die Reichweite; international werden Sie Giropay höchstens in Onlineshops finden, die einen Fokus auf deutsche Kunden legen.

In Sachen Bedienkomfort im Onlinehandel befinden sich beide auf Augenhöhe. Beide können Sie auf Wunsch außerdem mit zusätzlicher Zwei-Faktor-Authentifizierung absichern. (mon) c't

Sicher bezahlen im Ausland

Das Terminal weist Ihre Karte zurück, der Kassierer versteht Sie nicht, hinter Ihnen scharrt man bereits mit den Hufen – puh. Mit etwas Vorbereitung umschiffen Sie im Ausland solche und andere Kalamitäten wie Kartendiebstahl.

Von **Markus Montz**

Können Sie sich im Inland meistens noch einigermaßen aus der Affäre ziehen, wenn Ihre Karten nicht funktionieren und Sie kein Bargeld dabeihaben, verdirbt Ihnen das im Ausland schnell den Spaß und Sie stehen quasi mittellos da. Wenn Sie im Ausland stets flüssig sein wollen, gibt es daher vor allem zwei Grundsätze: Setzen Sie niemals alles auf eine Karte und auch nicht alles auf Plastik. Vielleicht nimmt ein Händler oder Geldautomat Ihre Karten nicht an oder Sie geraten umgekehrt an einen Verkaufsautomaten, der nur Karten akzeptiert. Manchmal hat auch das Kartenlesegerät einen Defekt oder ist inkompatibel mit Ihrer Karte, von deren Verlust ganz abgesehen. Gleichzeitig fallen Improvisationsmöglichkeiten wie eine Rechnung meist weg.

Mischen Sie daher Plastik- und Bargeld sowie das digitale Plastik im Smartphone. Ihr individuelles Mischungsverhältnis richten Sie danach, wohin Sie reisen, wie lange Sie bleiben wollen und ob Sie persönliche, aktuelle Erfahrungen mit der Zielregion haben. Kalkulieren Sie außerdem das Risiko mit ein, dass Ihnen etwas abhandenkommt. Informieren Sie sich vorab aus aktuellen Quellen darüber, welche Zahlungsmöglichkeiten vor Ort herrschen. Allgemeingültige Aussagen gibt es nicht.

Münzen und Scheine

Mit Bargeld kommen Sie nahezu überall auf der Welt zum Zuge. Selbst in kartenaffinen Ländern wie

Schweden lohnt sich eine kleine Bargeldreserve für den Notfall; andersherum ist es in einigen Ländern wie Japan selbst um die Akzeptanz von Visa und Mastercard mäßig bestellt, auch an Bankautomaten.

Sofern Sie nicht wissen, ob Sie zum Beispiel direkt am Flughafen einen mit Ihren Karten funktionierenden Geldautomaten finden, lohnt es sich daher, bereits vor der Reise etwas Bargeld für die ersten Tage zu tauschen; achten Sie aber auf mögliche Ein- und Ausfuhrbestimmungen. Teilen Sie die Summe am besten auf. Verwahren Sie einen Teil am Körper, einen Teil im Hotelsafe oder an einem anderen sicheren Ort. Wenn Sie Bargeld an einem Automaten außerhalb des Euroraums ziehen, achten Sie zudem auf die Wechselmodalitäten. Die jeweilige Fremdbank bietet Ihnen oft eine Abrechnung in Euro an. Allerdings fällt deren Wechselkurs meist signifikant schlechter aus als bei einer Abrechnung in der jeweiligen Landeswährung, die Ihre Bank vornimmt. Schauen Sie gut hin, was der Automat Ihnen anbietet; manche Geräte sollen Sie gezielt zum Schlechteren bewegen.

Girocard

Die Girocard Ihrer Bank oder Sparkasse, oft nach ihrer früheren Bezeichnung „EC-Karte“ genannt, können Sie als solche nur an sehr wenigen Punkten im Ausland einsetzen, oft nicht mal innerhalb der EU. Wenn Sie damit zahlen oder an Automaten Bargeld abheben möchten, benötigt die Karte ein zweites, international akzeptiertes Zahlungssystem. Das zeigt eine „Co-Badge“ an, sie sitzt als zusätzliches Symbol meist auf der Vorderseite rechts.

Auf das Logo kommt es an: Zeigt Ihre Karte nur das Girocard-Symbol (links) ohne Co-Badge von Maestro/Mastercard oder V Pay/Visa (rechts), können Sie damit im Ausland nichts anfangen.

Aus für Maestro

Mastercard hat Maestro abgekündigt. Gültige Girocards mit Co-Badge von Maestro funktionieren bis zu ihrem Ablaufdatum aber weiterhin im Ausland. Von wenigen befristeten Ausnahmen abgesehen stellen Banken und Sparkassen ab 1. Juli 2023 lediglich keine neuen Karten mit Maestro-Funktion mehr aus. Da Banken und Zahlungsdienstleister ihren Kunden in der Regel alle vier Jahre eine neue Karte ausstellen, können Sie damit im besten Fall noch bis weit ins Jahr 2027 zahlen und Geld abheben.

Traditionelle Co-Badges sind Maestro von Mastercard und V Pay von Visa. Für Maestro können Sie weltweit Akzeptanzstellen finden, V Pay ist auf Europa beschränkt. Für V Pay braucht der Händler außerdem ein Kartenterminal, das mit dem Chip in der Karte zurechtkommt. Maestro hingegen funktioniert auch mit Geräten, die den Magnetstreifen auslesen.

Einige Sparkassen und Banken haben außerdem begonnen, Girocards mit vollwertigen Debitkarten-Co-Badges von Mastercard und Visa auszugeben. Diese können Sie mit wenigen Ausnahmen überall dort einsetzen, wo Sie auch mit Visa- und Mastercard-Kreditkarten zahlen können. Welche Zahlart ein Händler annimmt, erkennen Sie meist an entsprechenden Symbolen an der Ladentür oder neben der Kasse.

Mastercard, Visa & Co.

Mit den Kreditkarten der beiden großen Netzwerke sind Sie an vielen Orten der Welt gut aufgestellt. Zumindest in touristischen Regionen sowie bei größeren Handels- und Hotelketten können Sie damit häufig Einkäufe, Mietwagen und die Unterkunft zahlen oder an Bargeld kommen.

Die meisten europäischen Länder haben ein dichtes Akzeptanznetz für Visa und Mastercard. Probleme kann es hingegen in Einzelfällen mit Visa- und Mastercard-Debitkarten geben, die Sie beispielsweise von Direktbanken wie ING, DKB und Comdirect erhalten. Das betrifft vor allem Hotels und Autoverleiher. Diese wollen die Karte nachbelasten können, wenn Sie die vereinbarte Mietdauer überschreiten. Zwar erhalten

Händler mittlerweile auch für Debitkarten eine Zahlungsgarantie, doch nicht alle vertrauen darauf.

Das gilt umso mehr für Prepaid-Karten von Mastercard und Visa. Diese haben den Vorteil, dass man Ihnen maximal das Geld stehlen kann, das Sie auf die Karte geladen haben. Allerdings kann ein Händler auch nur so viel abbuchen, wie sich noch auf der Karte befindet. Manche Händler akzeptieren diese Karten daher nicht. Außerdem kosten solche Karten je nach Maximalbetrag oder Auslandsfähigkeit teilweise Gebühren, auch am Geldautomaten. Noch dünner und meist auch teurer wird es bei der Akzeptanz von Kreditkarten wie American Express (Amex) oder Diner's Club, und zwar auf der ganzen Welt, inklusive der USA.

Smartphone & Co.

Noch misstrauischer als mit Karten sollten Sie mit Ihrem Smartphone verfahren. Damit das funktioniert, muss das Kassenterminal nicht nur die hinterlegte Karte akzeptieren. Es muss auch für kontaktlose Zahlungen mit NFC ausgerüstet sein.

Anders als in Deutschland und großen Teilen Europas ist das weltweit längst nicht überall der Fall. Selbst in den USA kommen Sie mit den Wallets von Apple und Google häufig nicht weiter. Viele Kartenterminals verarbeiten schlicht keine kontaktlosen Zahlungen oder die Händler wollen es nicht. Nehmen Sie daher stets auch Plastikkarten mit. Andersherum gilt: Wenn Sie kontaktlos zahlen können, funktionieren auch Smartphones, und dann zum Beispiel auch die Kreditkarten in den Apps von Sparkassen und VR-Banken oder die virtuelle PayPal-Mastercard für Googles Wallet.

Für Uhren mit Google Wear OS und Apple WatchOS gilt das Gleiche, ebenso für Garmin, Fitbit, Swatch und anderen mit eigenem Smartwatch-System. Probieren Sie das Zahlen am besten vorab im Inland aus.

Außerhalb Europas ist die Lage noch uneinheitlicher. Verlassen Sie sich nicht auf pauschale Aussagen, dass die USA ein „Kartenland" seien oder es in Japan und Südkorea mit ihrer Technikbegeisterung keine Probleme gebe. Auch dort stoßen Sie öfter auf „Cash only", als es die Stereotypen erwarten lassen. Als Faustregel gilt, übrigens auch in Europa: Wenn Sie die touristischen Hotspots verlassen, erhöht sich die Wahrscheinlichkeit, dass Bargeld Trumpf ist. In Japan wie auch zahlreichen anderen Ländern, zum Beispiel China, akzeptieren viele Händler ansonsten nur nationale Bezahlsysteme.

Achten Sie außerdem wie bei der Girocard immer auf die Gebühren und vergleichen Sie. Selbst wenn Ihre Bank mit „kostenlosem" Abheben und Bezahlen „weltweit" wirbt, kann sich das auch lediglich auf die eigenen Entgelte beziehen, exklusive Fremdbank oder Händler. Es kann sich preislich außerdem lohnen, wenn Sie Kreditkartenanbieter abseits Ihrer Hausbank nutzen oder beispielsweise bei einer Neobank ein kostenloses Zweitkonto mit Debitkarte eröffnen. Das kann Ihnen die Jahresgebühr ersparen, mitunter erhalten Sie auch bessere Konditionen für einzelne Auslandszahlungen.

Sicherheit

Generell empfehlen wir, immer mindestens zwei Plastikkarten – zahlfähige Uhren und Handys sowie Amex nicht eingerechnet – mitzunehmen und getrennt voneinander aufzubewahren. Eine haben Sie am Körper, eine verbleibt während der Reise im Handgepäck und am Ziel im Hotel- oder Zimmersafe. Sie haben dann ein Backup bei Diebstahl, Verlust oder wenn eine Karte mal nicht funktioniert. Das ist aus den schon genannten Gründen besonders bei Debitkarten ratsam, zu denen ja auch die Girocard mit Co-Badge zählt. Noch ein Quäntchen mehr Sicherheit bringt es, wenn Sie einmal Visa und einmal Mastercard dabeihaben.

Schützen Sie stets Ihre PIN; zusammen mit der Karte ist sie der Jackpot für Diebe. Kriminelle können außerdem Ihre Kartendaten ausspähen. Mit Ausnahme der Girocard sind die Kartendaten schließlich aufgedruckt. Lassen Sie die Karte nirgends – auch nicht im Hotelzimmer – frei zugänglich liegen. Mit den Kartendaten können Kriminelle Kopien der Karte erstellen. Zwar ist der Chip dagegen immun, der Magnetstreifen jedoch nicht. Anschließend nutzen die Täter die Karte in einem Kartenlesegerät, das Magnetstreifen akzeptiert. Alternativ versuchen sie, mithilfe der Ausnahmen von der Zwei-Faktor-Authen-

Debit- und Kreditkarten von Visa und Mastercard funktionieren an der Kasse gleich, aber manche Hotels und Autoverleiher akzeptieren Debitkarten nicht.

tifizierung an der Kasse oder im Internet so viel wie möglich damit zu kaufen. Überdies sind Kartendaten eine beliebte Handelsware unter Cyberkriminellen. Sie können schlicht nicht prüfen, welchen Weg Ihr Datenstrom nimmt.

Prüfen Sie daher regelmäßig Ihre Kartenumsätze. Um Betrug zu reklamieren, reichen die monatliche Kreditkartenabrechnung oder bei Debitkarten die Girokontoauszüge. Noch besser ist es aber, die Umsätze täglich über die Smartphone-App oder das Onlinebanking auf dem Laptop zu checken. Im Mobilfunknetz ist die Verbindung meistens sicher. Wenn Sie Zweifel daran hegen, bauen Sie die Verbindung über ein VPN auf [1], auch dann, wenn Sie aus anderen Gründen das Onlinebanking nutzen. In einem fremden WLAN empfiehlt sich das immer.

Stellen Sie Betrug fest oder geht Ihnen eine Karte verloren, melden Sie dies unverzüglich Ihrer Bank. Erst ab diesem Zeitpunkt haften Sie nicht mehr für weitere Schäden. Die meisten deutschen Banken und Sparkassen halten dafür eine gemeinsame Notrufnummer vor, die Sie weltweit unter +49 116 116 erreichen. Prüfen Sie das vor dem Urlaub für Ihre Bank und notieren Sie eine abweichende Nummer. In Österreich und der Schweiz gibt es je nach Karte und Kreditinstitut verschiedene Nummern.

Ihre Bank prüft Ihre Zahlungen ebenfalls automatisiert auf Betrug und kann eine Sperre veranlassen. Auch deshalb lohnt es sich, eine zweite Karte dabei zu haben. Mit Glück und je nach Kreditinstitut ruft Sie bei verdächtigen Zahlungen vorher ein Mitarbeiter der Bank an und fragt nach. Ist der Anruf seriös, fragt er sie aber niemals nach Kartendaten, Passwörtern oder PINs. Ebenso wenig verlangt er eine Zwei-Faktor-Authentifizierung von Ihnen. Noch sicherer ist es, wenn Sie Ihren Bankberater oder die Hotline unter der bekannten Nummer zurückrufen.

Reißen alle Stricke, gibt es noch einen letzten, teuren Notnagel: Verwandte oder Freunde können Ihnen Bargeld über Western Union oder vergleichbare Dienste schicken. Wenn Sie unsere Regeln beherzigen, dürfte so etwas aber normalerweise gar nicht notwendig werden und Sie können Ihre Reise entspannt genießen. (mon) c't

Literatur

[1] Urs Mansmann, Online unterwegs, Mit dem Smartphone im Ausland: Roaming ohne Kostenfallen, c't 15/2023, S. 64

Womit Kunden immer wieder Ärger haben

Die Geschichten der c't-Rubrik „Vorsicht, Kunde“ schreibt das Leben. Manche Themen ziehen sich wie ein roter Faden durch unser Magazin, werden aber jedes Mal um eine neue Facette bereichert. Andere wiederum sind komplett neu, beispielsweise weil neue Regularien die Position der Verbraucher stärken sollen. In der Praxis kommt das oft nicht oder nur mit Verspätung an. Trotzdem konnten wir im Lauf der Jahre vielen Lesern zu ihrem Recht verhelfen.

Von **Tim Gerber**

Für viele Nutzer ist es ein Supergau, wenn ihr Internetanschluss nicht mehr funktioniert. So geschehen beim Provider-Wechsel im Fall von Jürgen W. Ein Anbieterwechsel zur Deutschen Glasfaser führte dazu, dass sein Internetanschluss kurz vor Weihnachten plötzlich tot war. In der Nacht hatte der bisherige Provider die Verbindung abgeschaltet. Sein neuer, die Deutsche Glasfaser (DG), hatte ihn offenbar nicht wieder aktiviert. Am späten Nachmittag des 20. Dezember erhielt Jürgen W. zwar eine Willkommensmail der Deutschen Glasfaser, aber der Anschluss funktionierte immer noch nicht.

Am folgenden Morgen rief Jürgen W. bereits ein zweites Mal bei der DG an, aber auch da konnte man ihm nichts Neues sagen. Wenige Minuten nach seinem Anruf erhielt er aber immerhin eine Bestätigung, dass seine Störungsmeldung aufgenommen wurde, auch wenn der Text nichts Konkretes enthielt: „Unser Techniker-Team arbeitet bereits intensiv und mit höchster Priorität an der Störungsbehebung“, hieß es in der Mail. „Wir können Ihnen aktuell leider noch kein Enddatum nennen. Sobald wir über ausreichende Informationen verfügen, nennen wir Ihnen gern umgehend ein Enddatum. Wir halten Sie auf dem Laufenden“, versprach die DG.

Trotz täglicher Anrufe und E-Mails des Kunden tat sich bis zu den Feiertagen nichts. Bei seinen täglichen Anrufen hörte Jürgen W. sogar immer wieder, dass sein Anschluss in Ordnung sei, nur die Verbindung zwischen Netzabschlussgerät (NT) und seinem Router funktioniere wohl nicht.

Anfang des folgenden Jahres stand Jürgen W. noch immer ohne Internet da. Wir kontaktierten Anfang Januar die Pressestelle der DG und baten um Auskunft zu dem Vorgang. Nun erschien bald ein Techniker vor Ort, der innerhalb weniger Minuten feststellte, dass er den Verteilerkasten einige hundert Meter vom Haus der W.s entfernt aufsuchen müsse. Es stellte sich heraus, dass in der Verteilung der Steckplatz für den Anschluss von Jürgen W. ausgefallen war. Der Techniker musste nur das Modul tauschen. Der Provider hätte die Störung also ohne Weiteres auch gleich am 20. Dezember beheben können, statt den Kunden über Weihnachten und Neujahr ohne Internet und Festnetztelefon zu lassen.

Wirksames Gesetz

Da so ein Ausfall den Alltag auch in privaten Haushalten erheblich beeinträchtigt, steht auch ihnen gemäß § 58 TKG pauschal ein Schadensersatz von mindestens 5 Euro pro Tag des Ausfalls zu. Das gilt allerdings erst ab dem dritten Tag. Ab dem fünften Tag gibt es dann aber auch schon mindestens 10 Euro. Bei Anschlüssen, die im Monat mehr als 100 Euro kosten, kann es auch mehr sein, nämlich 5 Prozent davon ab dem dritten und 10 Prozent ab dem fünften Tag. Die für die Zeit der Störung wegfallenden Entgelte können die Provider allerdings gegenrechnen.

Die genannten Mindestbeträge stehen dem Kunden selbst dann zu, wenn er aktuell gar keine monatlichen Kosten für den Anschluss hat. Das ist gerade bei Providerwechseln häufig der Fall, weil in den ersten Monaten nach Vertragsbeginn für Neukunden oft erst mal Sonderrabatte oder Nulltarife gelten. Auch dann gelten aber die Entschädigungsansprüche, denn einen konkreten Schaden durch den Ausfall müssen die Kunden nach dem Gesetz nicht nachweisen.

Voraussetzung ist lediglich, dass man die Störung dem Provider nachweislich gemeldet hat. Damit die Provider den drohenden Schadensersatz nicht vereiteln, hat ihnen der Gesetzgeber die Pflicht auferlegt, solche Meldungen unverzüglich für den Kunden nachweisbar zu dokumentieren. Wird die Störung nicht binnen zweier Tage behoben, muss eine Mitteilung über die geplanten Maßnahmen und das voraussichtliche Ende an den Kunden folgen.

Betroffene sollten vor allem auf eine sofortige saubere Dokumentation ihrer Störungsmeldung achten und im Zweifel sofort die Bundesnetzagentur als zuständige Aufsichtsbehörde informieren, wenn ihr Provider dieser Pflicht nicht wie im Gesetz gefordert unverzüglich nachkommt. Nicht zuletzt dank unserer Berichte scheint das Gesetz rasch Wirkung entfaltet zu haben. Jedenfalls sind uns in der Folge keine weiteren solchen Fälle geschildert worden.

Garantie

Ein Dauerbrenner sind hingegen scheiternde oder schlecht ausgeführte Garantiereparaturen. Für Verkäufer und Hersteller sind sie immer ein Ärgernis. Ganz gleich, auf welcher Rechtsgrundlage sie beruhen – dem gesetzlichen Gewährleistungsrecht gegenüber dem Verkäufer oder einer eingeräumten Garantie, meist durch den Hersteller –, für alles muss der Handel Vertragswerkstätten vorhalten, die eingesandten Geräte untersuchen und meist gegen Fallpauschalen reparieren.

Die Pauschalen sind oft höher als die Gewinnmargen. Folglich versuchen häufig auch namhafte Produzenten und Handelsketten, die Kunden mög-

lichst davon abzuhalten, ihre Rechte geltend zu machen. Deshalb spiegelt die Häufigkeit, mit der ein bestimmter Händler oder Hersteller Anlass zu Beschwerden an die c't-Redaktion gibt, eher seine Marktanteile als seine Servicequalität wider.

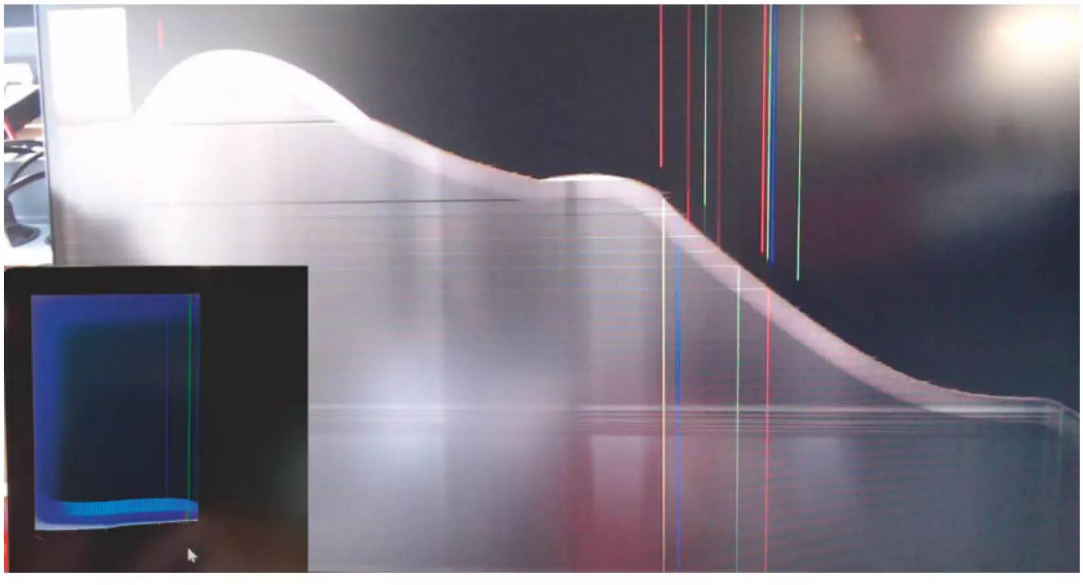
Unser Leser Tilo M. hatte beim Onlinehändler Galaxus einen 4K-Monitor mit 27 Zoll Bilddiagonale vom Typ Dell S2721QS erworben. Der knapp 280 Euro teure Monitor zeigte bereits nach ein paar Wochen einen deutlichen Bildausfall in der linken oberen Ecke. Nachdem Tilo M. das Gerät zurück an den Händler gesandt hatte, ließ der sich über einen Monat Zeit und teilte anschließend dem verblüfften Kunden mit, dass er den Monitor nicht kostenlos innerhalb der Garantie reparieren könne, da es sich um einen mechanischen Schaden handle, welcher nicht unter die Garantie falle. Die Servicestelle habe die Garantie abgelehnt. Ausschlussgründe im Rahmen einer Garantie seien unter anderem Abnutzung, Schäden durch Fehlmanipulationen, Eingriffe sowie äußere Umstände wie Elementar-, Feuchtigkeits-, Sturz- und Schlagschäden.

Auch wir hielten die dem Kunden erteilte Auskunft nicht für nachvollziehbar, insbesondere angesichts der zahlreichen Bilder, die Tilo M. uns zu der Bildstörung übermittelt hatte und auf denen keinerlei äußere Beschädigung erkennbar war.

Ansprüche gegen den Verkäufer aus der gesetzlichen Gewährleistung beziehen sich auf Mängel, die schon beim Kauf vorhanden waren. Folglich sind Beschädigungen durch unsachgemäße Behandlung durch den Kunden ausgeschlossen. Aber dafür gab es hier keine Anzeichen. Der Bildausfall konnte ebenso gut auf einem bereits vorhandenen Bruch an einer Leiterbahn beruhen, der sich eben erst nach einigen Wochen bemerkbar macht. Bis zu einem Jahr nach dem Kauf muss im Zweifel der Verkäufer beweisen, dass der Ausfall nicht auf einem solchen versteckten Sachmangel beruht, welcher bei Übergabe der Ware bereits vorhanden war. Tilo M. musste allerdings einen Anwalt bemühen, um seine Rechte durchzusetzen.

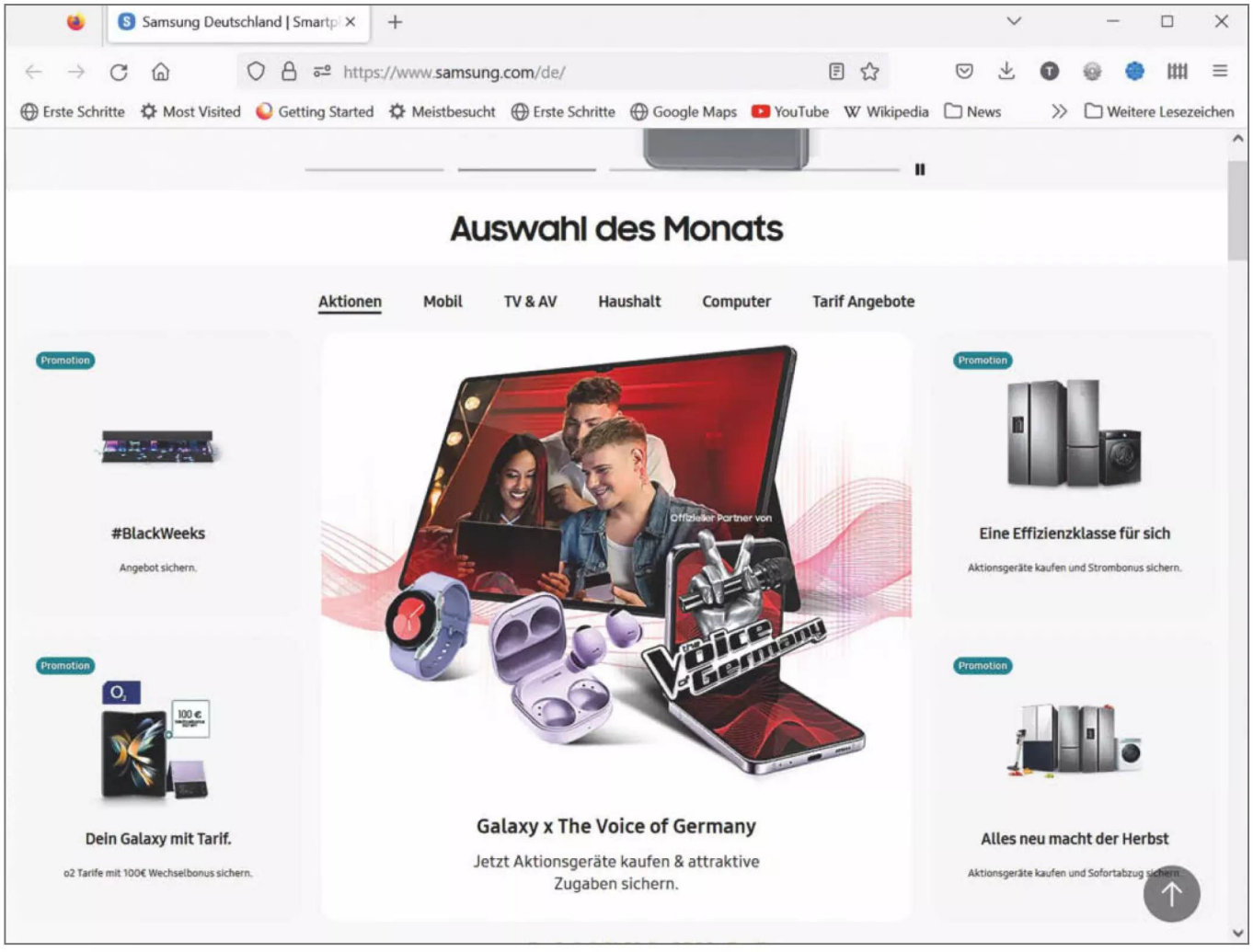
Warten auf Godot

Immer wieder sind Kunden mit dem Phänomen konfrontiert, dass bestellte und bezahlte Ware partout nicht geliefert wird – besonders beliebt nach den alljährlich wiederkehrenden Rabattaktionen wie „Cyberweek“ oder „Black Friday“. An einem solchen hatte Mathias K. im Onlineshop von Samsung spontan ein Smartphone Galaxy Note 20 Ultra 5G mit 256 GByte Speicher bestellt. Der Aktionspreis von 665 Euro versprach ein echtes



Bilder: Tilo M. und Galaxus

Auf den Fotos von Kunden und Händler sind zwar eindeutige Bildausfälle zu erkennen. Die behaupteten Spuren äußerer Einwirkung zeigen sie aber nicht. Trotzdem machte der Händler solche geltend und verweigerte die Garantie.



Wie viele andere Firmen bietet auch Samsung in der Vorweihnachtszeit zahlreiche Rabattaktionen an. Ob es dann auch mit der Lieferung des Schnäppchens klappt, ist nicht immer so ganz sicher.

Schnäppchen. Als Liefertermin war der 3. Dezember angegeben. Doch die Sache zog sich bis ins Frühjahr und erst nach Anfragen der c't-Redaktion lieferte Samsung dann Ende April ein adäquates Nachfolgemodell.

Dabei sind zugesagte Liefertermine im Onlinehandel verbindlich. Das gilt auch bei Rabattaktionen. Kommt der Händler in Verzug, kann sich der Kunde nach erfolgloser Mahnung das Gerät woanders beschaffen und sich den Mehrpreis vom Verkäufer ersetzen lassen. Allerdings ist es für Kunden schwer, solche Ansprüche auch durchzusetzen. Bevor man tatsächlich eine Ersatzbeschaffung vornimmt, sollte man sich also unbedingt von einer Verbraucherzentrale oder einem Anwalt beraten lassen, um keine formalen Fehler zu begehen. (tig) c't

§ 58 TKG

ct.de/wbnj

Bild: Andreas Martini

Onlinekauf-Checkliste Reklamation

Nachdem die Bestellung auf den Weg gebracht und die Ware bezahlt wurde, kommt in der Regel ein paar Tage später eine Lieferung ins Haus. Aber was, wenn bei der Lieferung etwas schiefgeht, das Paket nicht das Gewünschte enthält oder später ein Mangel auftritt?

Von **Tim Gerber**

Paket kommt zu spät

Online-Händler sind verpflichtet, bereits bei der Bestellung verbindliche Lieferfristen anzugeben. Die Lieferfrist sollte auch auf der Bestellbestätigung oder Rechnung zu finden sein, sonst sollten Sie sie von der Webseite des Händlers kopieren, am besten per Screenshot, um sie am Ende nachweisen zu können.

Kommt es bei der Lieferung zum Verzug, dann können Sie den Kauf in jedem Fall widerrufen (siehe Artikel „Onlinekauf-Checkliste Rückabwicklung“ auf S. 70). War es ein besonders günstiges Angebot, können Sie theoretisch die Mehrkosten für eine Ersatzbestellung verlangen, in der Praxis ist es aber recht schwierig, das auch durchzusetzen. Sie sollten sich gut überlegen, ob der zu erwartende Streit finanziell überhaupt lohnt. Be-

sonders billige Angebote kommen nicht selten von Händlern, von denen keinerlei Entgegenkommen zu erwarten ist.

Ware ist verschollen

Wurde die Ware versendet, kommt aber nicht bei Ihnen an, ist der Kaufvertrag im Online-Handel ebenfalls nicht erfüllt. Nachweispflichtig ist der Versender. Hier können Sie also auf Ersatzlieferung innerhalb einer angemessenen Frist bestehen. Welche Frist angemessen ist, hängt von der ursprünglichen Lieferfrist und der Art der Ware ab, also wie schnell sie der Händler nachbeschaffen kann. Bei einem Möbelstück dauert das sicher länger als bei einem USB-Stick.

Die Mühe, selbst nach dem Verbleib zu forschen, müssen Sie sich nicht machen. Heikel wird es dann, wenn die Sendungsverfolgung eine Zustellung meldet, die Sendung aber nicht angekommen ist. Dann sollten Sie schnell handeln und den Verbleib klären. Oft verlangen die Händler dann eine eidesstattliche Versicherung, vor deren Abgabe Sie gründlich prüfen sollten, ob die Sendung nicht doch beim Nachbarn gelandet ist. Für eine versehentlich falsche Versicherung kann man zwar strafrechtlich nicht belangt werden, muss aber eventuellen Schaden ersetzen, wenn man fahrlässig gehandelt hat.

Paket ist beschädigt

Weist die Verpackung bereits bei Anlieferung deutliche äußere Schäden auf, sollten Sie die Annahme verweigern. Den Verkäufer müssen Sie dann möglichst rasch entsprechend informieren und um Ersatzlieferung bitten. Dies sollte erfolgen, bevor die Sendung wieder bei ihm ankommt, weil er die Rücksendung sonst als Rücktritt vom Kauf auffassen könnte.

Liegt das Päckchen schon vor der Haustüre, beim Nachbarn oder in einer Packstation, zücken Sie am besten sofort das Smartphone und fotografieren den Schaden noch vor dem Auspacken. Am besten tun Sie das im Beisein eines Zeugen, zum Beispiel desjenigen, der das Päckchen angenommen hat. Nachbarn oder Freunde sind grundsätzlich bessere Zeugen als Familienangehörige. Selbst nicht volljährige Kinder können als Zeugen dienen; je älter, desto besser.

Ist nur die äußere Verpackung defekt, sollten Sie die Ware vorsichtig auspacken und feststellen, ob sie unbeschädigt ist – auch das möglichst unter Zeugen. Bei einer schweren Beschädigung sollten Sie das Päckchen gar nicht erst auspacken, sondern zuerst den Händler kontaktieren und das Paket erst öffnen, wenn der Versender dies wünscht.

Mit dem Paketdienst müssen Sie sich als Verbraucher übrigens nicht auseinandersetzen. Es ist Sache des Händlers, Schadensersatzansprüche gegenüber dem Transportunternehmen geltend zu machen.

Lieferung ist unvollständig

Fehlt ein Teil der Lieferung, sollten Sie ebenfalls so schnell wie möglich einen oder mehrere Zeugen herbeirufen und den Zeitpunkt der Feststellung notieren. Das ist insbesondere angeraten, wenn Sie noch keine Erfahrung mit dem Händler haben und deshalb nicht wissen, wie er reagiert. Alle Online-Käufe sollten immer möglichst schnell ausgepackt und auf Vollständigkeit geprüft werden – je näher am Zeitpunkt der Zustellung, umso glaubwürdiger ist Ihre Reklamation.

Der Verkäufer ist verpflichtet, fehlende Artikel auf seine Kosten nachzuliefern. Weitere Versandkosten darf er dabei nicht erheben. Für die Fristen gilt dasselbe wie bei verschollenen Sendungen.

Ware aus Übersee

Bei Bestellungen aus Ländern außerhalb der EU müssen Sie mit Extrakosten durch Importzölle rechnen, die in etwa der Mehrwertsteuer entsprechen, die im Preis ja nicht enthalten ist.

Theoretisch gelten auch hier die europäischen Verbraucherrechte, doch die lassen sich nur äußerst schwer durchsetzen. Geld einzutreiben oder Lieferungen zu erzwingen ist schon gegenüber einer Firma in Deutschland nicht so einfach. Die muss aber immerhin fürchten, tatsächlich verurteilt zu werden und dann auch noch Gerichtskosten zahlen zu müssen. Nach China fährt der Gerichtsvollzieher bestimmt nicht.

Die Gefahr, dass Sie den tatsächlichen Firmensitz nicht erkennen, besteht vor allem auf Marktplätzen wie eBay und Amazon. Generell empfiehlt es sich, direkt in Fernost Bestellungen nur in einem finanziellen Umfang zu tätigen, dessen Verlust Sie im Zweifel verschmerzen können. Elektronische Bauteile für ein paar Euro beispielsweise können Sie gut und günstig bei Aliexpress bestellen, so Sie denn einige Wochen auf die Lieferung warten wollen, hochwertige Gebrauchsgüter eher nicht.

Späteren Defekt reklamieren

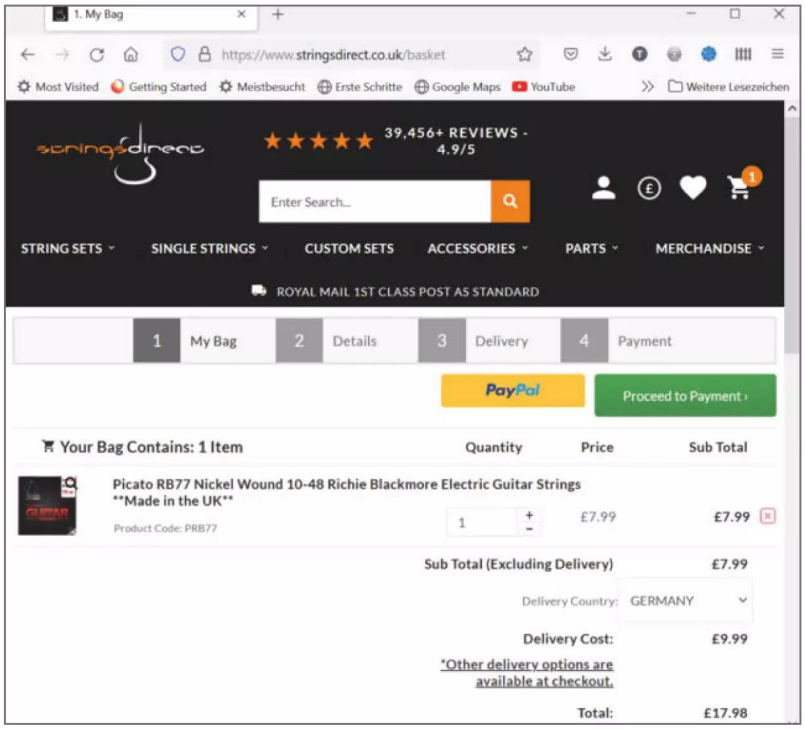
Ist die gelieferte Ware mangelhaft, haben Sie gegenüber dem Verkäufer bestimmte Rechte aus der gesetzlichen Sachmangelgewährleistung. Im Grunde fallen darunter auch die bereits behandelten Transportschäden. Oft sind Mängel an einer Ware aber nicht sofort erkennbar, sondern treten erst nach Wochen oder Monaten des Gebrauchs zutage. Eine kalte Lötstelle etwa muss nicht dazu führen, dass ein Notebook von Anfang an gar nicht funktioniert. Man spricht dann von versteckten Sachmängeln.

Die gesetzliche Gewährleistung bezieht sich auf genau diese Mängel, die schon bei Übergabe der Ware vorhanden waren, aber noch keine Wirkung entfaltet haben. In der Regel sind das Material- oder Herstellungsfehler. Fällt das Gerät später aus, müssen Sie das beim Verkäufer reklamieren. Zwei Jahre nach dem Kauf sind die Gewährleistungsrechte in der Regel aber verjährt.

Als Käufer haben Sie die Wahl, ob Sie eine Nachbesserung, also Reparatur verlangen oder auf die Lieferung eines intakten Geräts bestehen. Auch die Minderung des Kaufpreises ist denkbar. Der Verkäufer kann dem nur in Ausnahmefällen entgegenhalten, dass eine bestimmte Art der Nacherfüllung unverhältnismäßig wäre. Vom Kauf zurücktreten, also den Kaufpreis zurückerhalten, können Sie erst nach zwei erfolglosen Nachbesserungsversuchen.

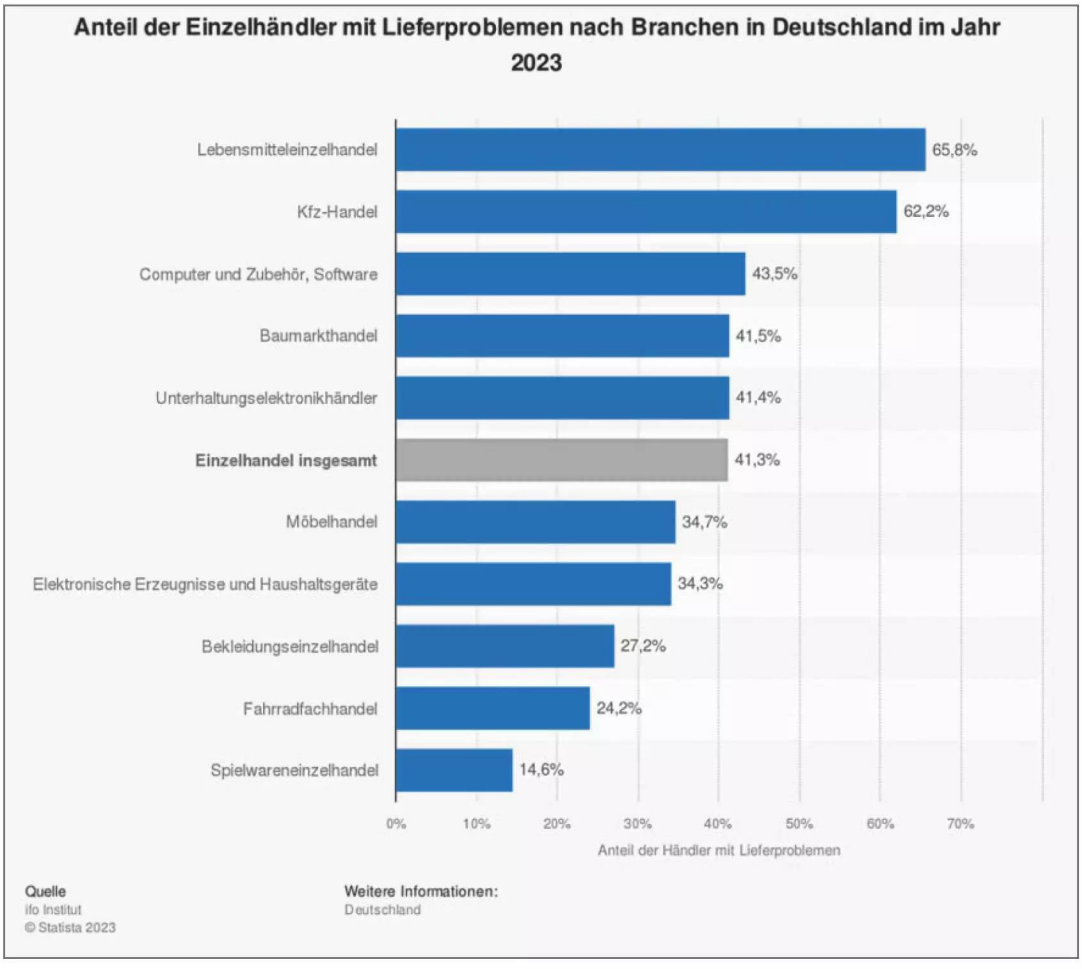
Oft besteht neben der gesetzlichen Gewährleistung noch eine Garantie des Herstellers. Auf diese muss der Verkäufer im Online-Handel hinweisen. Doch auch wenn eine Herstellergarantie besteht, sollten Sie stets zuerst den Verkäufer kontaktieren. Er darf für die Abwicklung an den Hersteller verweisen, wenn dadurch keine Nachteile für den Kunden entstehen. In der Praxis landen mangelhafte Geräte ohnehin meist in einer Vertragswerkstatt des Herstellers und werden zunächst dort geprüft. Die Rücksendekosten trägt in jedem Fall der Verkäufer.

Wird der Mangel anerkannt, können Sie die eingangs erwähnten Rechte auf Nachbesserung oder Nachlieferung geltend machen. Auf ein gebrauch-



Bei Bestellungen von außerhalb der EU, etwa in Deutschland schwer zu bekommende Gitarrensaiten von Ritchie Blackmore, müssen Sie neben dem Kaufpreis und den Lieferkosten noch etwa 20 Prozent Einfuhrzoll einkalkulieren.

Computer und Zubehör liegen bei Lieferengpässen auf dem dritten Platz.



tes Ersatzgerät oder eine Reparatur des mangelhaften Geräts müssen Sie sich nicht einlassen. Ihre Rechte als Käufer sollten Sie allerdings so ausüben, wie Sie es vom Gegenüber auch erwarten: mit Augenmaß.

Kaputt oder kaputt gemacht?

Je mehr Zeit seit dem Kauf vergangen ist, um so häufiger kommt es zum Streit darüber, ob es sich tatsächlich um einen Gewährleistungsfall handelt, also ob der Mangel bereits vor dem Kauf bestand, oder ob er erst nachträglich entstanden ist, etwa durch unsachgemäße Behandlung. Nachweisen muss das seit 2022 im ersten Jahr nach dem Kauf der Verkäufer. Danach ist der Käufer beweispflichtig.

Tritt ein Mangel auf, sollten Sie also nicht zögern, ihn zu reklamieren. Bevor Sie das Gerät einschicken, sollten Sie es möglichst von allen Seiten fotografieren, um Beweise für die äußerliche Unversehrtheit in der Hand zu haben. Auch hier sind Zeugen hilfreich. Es kommt immer wieder vor, dass beim Rückversand oder in der Vertragswerkstatt äußerliche Schäden entstehen, die dann genutzt werden, um die Gewährleistung auszuschließen. Bei einem äußerlich unversehrten elektronischen Gerät kann auch nach Ablauf der Beweislastumkehr der Beweis des ersten Anscheins für den Käufer sprechen. (tig) c't

Gewährleistungsrecht und Reklamation
ct.de/w3ad

Bild: Andreas Martini

Onlinekauf-Checkliste Rückabwicklung

Im Internet bestellte Ware können Sie innerhalb einer kurzen Frist ohne jede Begründung zurückgeben. Damit die Rückabwicklung reibungslos funktioniert, gibt es einiges zu beachten.

Von **Tim Gerber**

Richtig widerrufen

Das Recht zum Widerruf im Onlinehandel soll den Nachteil ausgleichen, den der Käufer dadurch hat, dass er die Ware nicht vorher begutachten konnte. Dafür hat man zwei Wochen ab Erhalt der Ware Zeit, um den Kauf gegebenenfalls zu widerrufen. Wie alle Rechte sollten Sie auch dieses Recht fair und mit Augenmaß gegenüber dem Verkäufer ausüben, also die Ware sorgfältig auspacken und vor dem Zurücksenden wieder sorgsam verpacken.

Das Recht selbst wird durch eine Erklärung an den Verkäufer ausgeübt. Sie müssen dabei keine bestimmte Form wahren, sich aber eindeutig dahingehend äußern, dass Sie den Kauf widerrufen. Und Sie sollten es so dokumentieren, dass Sie hinterher den Zeitpunkt des Widerrufs nachweisen können.

Viele Onlinehändler stellen eine Widerrufsfunktion in ihrem Webshop bereit. Das ist die beste Variante, denn dann muss der Händler per Gesetz auch rasch eine Bestätigung liefern. Kommt die nicht oder fehlt eine solche Funktion ganz, ist eine E-Mail das Mittel der Wahl. Dabei setzen Sie sich selbst oder noch besser einen Bekannten in CC, der den Empfang gegebenenfalls bestätigen kann. Auch ein Fax ist denkbar. Wollen Sie auf Nummer sicher gehen, versenden Sie den Widerruf auf verschiedenen Wegen – doppelt hält besser.

Fristen einhalten

Das Widerrufsrecht gilt 14 Tage lang. Die Frist beginnt mit Erhalt der Ware, bei Teillieferungen erst, wenn der letzte Artikel eintrifft. Für digitale Inhalte wie Musikdownloads oder eBooks erlischt das Widerrufsrecht allerdings mit der Lieferung, sofern der Anbieter darauf hingewiesen hat und Sie sich mit der Lieferung vor Ablauf der Widerrufsfrist einverstanden erklärt haben. Den Widerruf können Sie in jedem Fall schon erklären, wenn die Ware noch gar nicht angekommen, ja noch nicht einmal unterwegs ist: je eher, desto besser.

Damit die Frist überhaupt startet, muss der Verkäufer mit der Vertragsbestätigung einen Hinweis auf das Widerrufsrecht geben. Andernfalls haben Sie ein Jahr lang Zeit, das Widerrufsrecht auszuüben. Es darauf ankommen lassen lohnt sich aber nicht. Die Wahrscheinlichkeit, dass der Händler anfängt zu streiten, ist nach Ablauf der 14-Tage-Frist deutlich höher und es kommen dann regelmäßig Beweisfragen auf, ob auf das Widerrufsrecht hingewiesen wurde oder nicht.

Infos zum Widerrufsrecht
ct.de/wkys

Selbstabholer

Während der Corona-Pandemie hat sich das Verkaufsmodell „Click & Collect“ etabliert: Viele Märkte bieten Bestellungen und Bezahlungen über ihre Webshops an, die Ware holt sich der Kunde dann in der nächsten Filiale ab. Meist liegt das Gewünschte bereits nach wenigen Stunden bereit.

Viele Handelsketten bieten freiwillig Rückgaberechte unabhängig vom jeweiligen Kaufvorgang an und oft auch über das gesetzliche Mindestmaß von 14 Tagen hinaus. Das geschieht zwar freiwillig, ist aber verbindlich, weil diese Rahmenbedingungen Teil des abgeschlossenen Kaufvertrags geworden sind. Sie können sich im Zweifel also darauf berufen.

Viele Einzelhändler können oder wollen sich solche Kulanz nicht leisten. Das generelle Rückgaberecht gilt gesetzlich aber nur bei reinen Fernabsatzgeschäften, also beim Onlinekauf, bei dem die gesamte Abwicklung außerhalb von Geschäftsräumen stattfindet. Allein die Bestellung per E-Mail oder Webshop genügt dafür nicht. Erfolgt zum Beispiel die Bezahlung erst vor Ort bei der Abholung, handelt es sich rechtlich nicht mehr um ein Fernabsatzgeschäft.

Besonders bei kleineren Einzelhändlern mit Filiale um die Ecke sollten Sie sich deshalb vorher vergewissern, wie es mit Umtausch- und Rückgaberechten aussieht. Sie können solche auch individuell vereinbaren. Bestätigt der Verkäufer auf Nachfrage bei einer Bestellung, dass er ein Rückgaberecht einräumt, ist er ebenfalls daran gebunden. Sie sollten die Bestätigung aber nachweisbar, also in Textform vorliegen haben, um sie im Zweifel nachweisen zu können.

Retourkutsche

Liegt der Sendung ein Retourenschein nebst Paketaufkleber bei, können Sie sich die gesonderte Erklärung ersparen, indem Sie die Retoure rechtzeitig auf den Weg bringen.

Ansonsten müssen Sie die Ware spätestens innerhalb von 14 Tagen zurücksenden. Dasselbe gilt für die Rückzahlung des Kaufpreises, die innerhalb von zwei Wochen erfolgen muss. Allerdings darf der Verkäufer den Eingang der Rücksendung abwarten. Für eventuelle Transportschäden haftet der Verkäufer. Mit ein paar Fotos von der ordentlich verpackten Ware sind Sie auf der sicheren Seite. Die Rückzahlung muss grundsätzlich über dasselbe Zahlungsmittel erfolgen, mit dem Sie bezahlt haben. (tig) c't

Bild: www.freepik.com

Kartenabbuchungen rückabwickeln

Nachträglich entdeckte Fehler bei Zahlungen im Internet oder an Ladenkassen sind selten, aber oft teuer. Haben Sie eine Debit- oder Kreditkarte genutzt, können Sie ein Rückerstattungsverfahren einleiten. Wir erklären, wie das geht.

Von **Markus Montz**

Doppelte Abbuchung, weiße Socken statt schwarze, der Geldautomat verrechnet sich: Nicht jeder Einsatz Ihrer Kredit- oder Debitkarte läuft wie gewünscht; von Betrug oder Missbrauch Ihrer Kartendaten durch Dritte ganz zu schweigen. Prüfen Sie Ihre Kontoumsätze oder Kartenabrechnungen und stellen einen Fehler fest, können Sie die fehlerhafte Buchung zum Glück zurückfordern – auch dann, wenn die Gegenseite eine Rückerstattung verweigert oder gar pleite ist. Die Kartenunternehmen Visa und Mastercard bieten dafür genau wie American Express als Sicherheitsmechanismus ein standardisiertes Reklamationsverfahren, oft auch „Chargeback“ genannt. Wir be-

leuchten, wann Sie eine Zahlung zurückfordern können, welche Bedingungen dafür gelten, wer Ihre Ansprechpartner sind und wie Sie vorgehen.

Mögliche Gründe

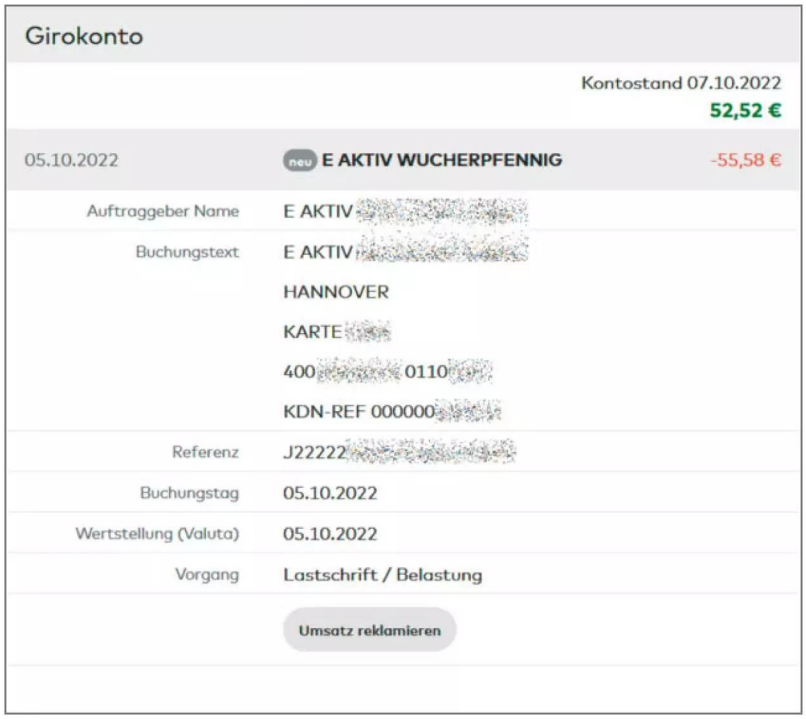
In vielen Fällen können Sie mit guten Erfolgsaussichten versuchen, eine Kredit- oder Debitkartenzahlung rückabzuwickeln. Nahe liegt das vor allem bei Betrugs- oder Missbrauchsverdacht, sprich: bei Zahlungen, die Sie nicht mit PIN oder online mit 3-D Secure autorisiert haben oder bei kontaktlosen Zahlungen mit einer gestohlenen Karte. Sie gehören zusammen mit Produktmängeln, Produktfälschungen oder falschem Paketinhalt zu den häufigsten Reklamationsgründen.

In selteneren Fällen kann es vorkommen, dass Händler oder Dienstleister (die wir in der Folge unter „Händler“ subsumieren) einen Betrag trotz technischer Absicherungen doppelt buchen oder die Karte mit einer zu hohen Summe belasten. Manchmal berechnet Ihnen ein Händler auch einen bereits stornierten Kauf oder ein gekündigtes Abonnement. Ebenso mag eine zugesagte Gutschrift nicht ankommen, nachdem Sie einen Artikel zurückgesandt haben. Vielleicht passt auch der Name des Händlers auf der Kartenabrechnung nicht zu der Quittung, die Sie erhalten haben.

Hotels und Autovermietungen können für eine Reservierung geblockte Beträge oder Kautionen nachbelasten, anstatt sie wieder freizugeben. Mitunter schließen sie auch den Check-out oder die Fahrzeugrückgabe nicht korrekt ab. Selbst bei der Insolvenz eines Unternehmens haben Sie meist Anspruch auf eine Rückerstattung, wenn Sie eine Leistung im Voraus bezahlt und nicht erhalten haben. So konnten zum Beispiel etliche Kunden nach der Pleite des Reiseveranstalters Thomas Cook ihr Geld retten.

Geldautomaten sind ebenfalls nicht frei von Fehlern. So kann ein Gerät in Ausnahmefällen weniger Geld auszahlen als auf der späteren Abrechnung ausgewiesen oder es verweigert die Auszahlung komplett.

Um für diese Eventualitäten gewappnet zu sein, sollten Sie sich stets Rechnungen mitschicken oder Kassenbons drucken lassen. Bei Fremdbanken lohnt es sich auch, am Automaten eine Quittung anzufordern. Diese bewahren Sie mindestens so lange auf, bis Sie Ihre Kontoumsätze (bei Debitkarten) oder die Kartenabrechnung (bei Kreditkarten) kontrolliert haben. Falls Sie einen Artikel zurückschicken, warten Sie mindestens so lange, bis die Gutschrift auf der Abrechnung steht.



Bei vielen Banken können Sie eine Rückerstattung („Chargeback“) für Zahlungen mit Visa oder Mastercard im Onlinebanking anstoßen, bei der Comdirect beispielsweise über „Umsatz reklamieren“.

Erst den Händler fragen

Wenn Sie einen Fehler entdecken, versuchen Sie zunächst, sich mit dem Händler direkt zu einigen. Schließlich kann jeder einen Fehler machen. Abgesehen davon, dass viele Banken diesen Schritt für ein späteres Rückforderungsverfahren abfragen, erspart Ihnen eine gütliche Einigung viel Zeit und Aufwand. Nach der Abbuchung des Betrages oder Ihrer Kreditkartenrechnung vom Girokonto haben Sie ohnehin mindestens acht Wochen Zeit für einen möglichen formalen Widerspruch. Bei Visa und Mastercard sind es je nach Vertrag oft sogar 120 Tage.

Nehmen Sie per Mail oder schriftlich Kontakt zum Händler auf. In der Regel haben seriöse Händler eine Mail- oder Postadresse für diesen Zweck; im stationären Handel hilft oft der Kassenbon weiter. Setzen

Girocard-Zahlungen

Für die Girocard („EC-Karte“) gibt es kein übergreifendes Regelwerk wie bei Mastercard und Visa. Stattdessen gelten die Bedingungen Ihrer Bank oder Sparkasse. Zwar können Sie dort auch Girocard-Buchungen anfechten, die bei einem Händler oder am Geldautomaten erfolgt sind. Ebenso bekommen Sie dann vorläufig eine Gutschrift auf Ihr Girokonto. Grundsätzlich gilt aber: Es muss sich um einen technischen Fehler oder eine nicht ordnungsgemäß autorisierte Zahlung handeln. Das bedeutet, dass Ihnen die Bank keine Verletzung der Sorgfaltspflichten oder gar betrügerische Absicht nachweisen kann. Da die Girocard fast ausnahmslos auf den stationären Handel beschränkt ist, ist dies deutlich seltener der Fall: Hat beispielsweise jemand die korrekte PIN eingegeben, gilt oft der Anscheinsbeweis mangelnder Sorgfalt und Sie haben schlechte Chancen. Dann zieht die Bank eine vorläufig geleistete Gutschrift wieder ab. Alle anderen Fälle wie Mängel an der Ware müssen Sie mit dem Händler direkt klären. Die Sparkassen bieten für Apple-Pay-Onlinezahlungen mit der Girocard einen eigenen Käuferschutz an.

Sie für Antworten eine realistische Frist und sichern Sie die Kommunikation, also Mails, Briefe oder Faxe. Bei einem Rückversand achten Sie außerdem auf eine elektronische Sendungsverfolgung. Erkennt der Händler einen Fehler an oder kommt Ihnen auf Kulanzbasis entgegen, wird er Ihnen das Geld meistens zurückerstatten.

Der Händler dürfte Ihnen zwar nichts schenken, aber er hat grundsätzlich ein Interesse daran, ein formelles Erstattungsverfahren zu vermeiden. Die Kreditkartenfirmen üben über den Acquirer – den Zahlungsdienstleister, der dem Händler die Akzeptanz von Kartenzahlungen ermöglicht – starken Sanktionsdruck aus. Sind Händler zu häufig in diese „Chargeback“-Verfahren verwickelt, drohen ihnen Gebühren und Auflagen wie aufwändige Berichtspflichten. Im schlimmsten Fall kündigt der Acquirer ihnen den Akzeptanzvertrag. Zudem kostet jedes Chargeback-Verfahren den Händler Geld und Zeit.

Haben Sie den Verdacht, dass jemand Sie betrügt oder Ihre Kartendaten missbraucht, überspringen Sie den Einigungsversuch oder brechen ihn ab und wenden sich direkt an Ihr Institut. Damit verbunden ist aber stets die Pflicht, dass Sie die Karte genau wie bei einem Diebstahl unverzüglich sperren lassen – über Ihre Bank oder die zentrale Notfallnummer 116 116. Deshalb gilt außerdem: Prüfen Sie nicht nur regelmäßig Ihre Abrechnungen, sondern auch, ob Ihre Karte noch da ist. Für Abbuchungen nach der Sperre haftet grundsätzlich die kartenausgebende Bank, bei Abbuchungen davor kommt es darauf an, ob Sie Ihre Sorgfaltspflichten erfüllt haben. Weist Ihnen die Bank das Gegenteil nach, weil Sie zum Beispiel Karte und PIN zusammen aufbewahrt haben, bleiben Sie auf dem Schaden sitzen.

Verfahren einleiten

Erzielen Sie mit einem seriösen Händler keine Einigung, ist bei Mastercard- oder Visa-Karten Ihr nächster Ansprechpartner ebenfalls Ihre kartenausgebende Bank oder Sparkasse. Das gilt auch, wenn Sie nach einer fehlerhaften Auszahlung am Geldautomaten die Fremdbank nicht erreichen. Bei Ihrem Institut leiten Sie explizit (und nachdrücklich) ein „Chargeback“-Verfahren gegen die betroffene Zahlung ein, manchmal auch „Einspruch“ oder anders genannt. Bei American Express ist die Kreditkartenfirma selbst Ihr Ansprechpartner – dort heißt das Verfahren „Reklamation“. Wichtig: Sie dürfen parallel kein Rückerstattungsverfahren auf anderem Weg einleiten.

Bei vielen Banken können Sie den Prozess im Onlinebanking anstoßen. Ähnlich läuft es auch bei Kreditkarten, die Sie über Dienstleister wie Lufthansa beziehen. Meist finden Sie dafür eine Schaltfläche, wenn Sie die fragliche Buchung anklicken. Auch telefonischer Kontakt ist häufig möglich, bei vielen Sparkassen sowie Volks- und Raiffeisenbanken etwa ist das mangels Option im Onlinebanking sogar der

schnellste Weg. Bei Filialbanken können Sie zudem eine Geschäftsstelle aufsuchen. Mitunter lagern die Kreditinstitute die Chargeback-Verfahren auch aus; bei den Sparkassen kümmert sich darum beispielsweise der hauseigene Dienst PlusCard.

Ob online oder Papier: In jedem Fall müssen Sie auf dem Formular einen Grund angeben und anschließend Nachweise wie die schon erwähnten Rechnungen oder Kassenbons liefern. Gegebenenfalls gehören auch die Kommunikation mit der Gegenseite sowie eventuell Fotos von Schäden oder andere Dokumente dazu. Mitunter fordert Ihr Kreditinstitut weitere Belege nach. Reagieren Sie unbedingt darauf – Sie können eine Buchung nur einmal beanstanden, einen zweiten Versuch gibt es nicht.

Entscheidung und Rückerstattung

Für ein Chargeback- oder Reklamationsverfahren haben die Kreditkartenunternehmen feste Regeln. Bei Visa und Mastercard erkennen Kartenherausgeber und Acquirer diese in den Lizenzverträgen an. Sie reichen sie in den Karten- und Akzeptanzverträgen an Kartenkunden und Händler weiter. American Express, das ja kartenausgebende Bank und Acquirer zugleich ist, schließt seine Verträge samt Regeln hingegen direkt mit Kartenkunden und Händlern.

Bei Zahlungen mit Visa oder Mastercard prüft zunächst Ihre Bank den Fall. Aus rechtlichen Gründen muss sie Ihnen den Betrag trotzdem vorläufig erstatten. Bei Kreditkarten erhalten Sie eine Gutschrift auf Ihr Kreditkartenkonto, bei Debitkarten aufs Girokonto. Etwaige Währungsschwankungen gleicht die Bank nicht aus. Hält Ihre Bank Ihre Reklamation für zulässig, kontaktiert sie den Acquirer des Händlers und fordert dort den Zahlungsbetrag zurück. Der Acquirer befragt gegebenenfalls den Händler. Liegt der Fehler bei ihm, steht die Händlerseite in der finanziellen Pflicht, andernfalls lehnt der Acquirer das Gesuch Ihrer Bank samt Begründung ab. American Express befragt nach Prüfung Ihrer Reklamation direkt den Händler.

Kommt es in einem Chargeback- oder Reklamationsverfahren trotz Regeln zu keiner Einigung, entscheidet das Kartenunternehmen. Kann die Händlerseite einen Fehler ausschließen, Ihnen den Fehler nachweisen oder erhält sie das Plazet des Kartenunternehmens, wird man Ihnen den Betrag wieder belasten. Das passiert auch, wenn Ihr Institut Ihre Eingabe zurückweist. Einen Rechtsanspruch haben Sie nicht. Sie können anschließend immerhin noch direkt gegen den Händler den Rechtsweg beschreiten oder eine Schlichtungsstelle für Banken kontaktieren. Bei berechtigten Eingaben sind Sie durch das Chargeback-Verfahren aber normalerweise gut gegen Verluste geschützt. (mon) c't

PayPal-Schutz bei Privatgeschäften

Der Käufer- und Verkäuferschutz des meistgenutzten Zahlungsdienstleisters im Internet kann teure Verluste vermeiden. Allerdings muss man dazu seine Regeln kennen. Wir haben für Sie im Kleingedruckten gestöbert.

Von **Markus Montz**

Verkäufer und Käufer auf Kleinanzeigenportalen nutzen gerne PayPal. Der Dienst kann auch bei vielen privaten Deals auf Internet-Anzeigenseiten davor schützen, bei Fehlern im Versand- oder Bezahlprozess oder gar unseriösem Gebaren der Gegenseite finanziell im Regen zu stehen. Damit dieser Schutz greift, müssen Sie allerdings einige Bedingungen erfüllen. Wir haben die wichtigsten Punkte der AGB zusammengefasst; die vollständigen Texte finden Sie unter ct.de/w59p.

In Konfliktfällen können Sie ein solches Schutzverfahren sowohl als Käufer wie auch als Verkäufer direkt in Ihrem PayPal-Konto unter der fraglichen Zahlung einleiten. Wir empfehlen (und PayPal setzt voraus), dass Sie dennoch zunächst vorab außerhalb der Plattform Kontakt zur Gegenseite aufnehmen. Erst wenn eine einvernehmliche Klärung nicht möglich ist, entscheidet PayPal. Der Dienst ist jedoch kein öffentliches Schiedsgericht und das Verfahren nicht transparent! Seien Sie darauf gefasst, dass die Entscheidung von PayPal für Außenstehende fragwürdig ausfällt und dass ein ordentliches Gericht im Nachhinein noch anders entscheiden kann als PayPal.

Wichtig: Für die Auktions- und Marktplatz-Website eBay gelten mittlerweile eigene Regeln, da PayPal nicht mehr zu eBay gehört und der frühere Sonderstatus für PayPal-Zahlungen auf eBay nicht mehr gilt. Ähnliches gilt für „Sicher bezahlen“ auf Kleinanzeigen: Dort ist PayPal keine integrierte Bezahlmethode (siehe Artikel „Sicher bezahlen bei Kleinanzeigen“ ab S. 102). Wollen Sie dort PayPal nutzen, können Sie dies nur außerhalb der Plattform tun (siehe Artikel „FAQ: „Sicheres Bezahlen“ auf Kleinanzeigen“ ab S. 112) und unterliegen dann den normalen PayPal-Bedingungen.

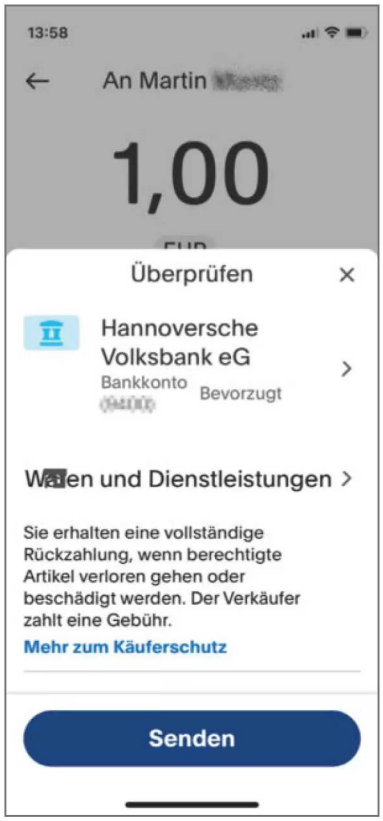
Käuferschutz

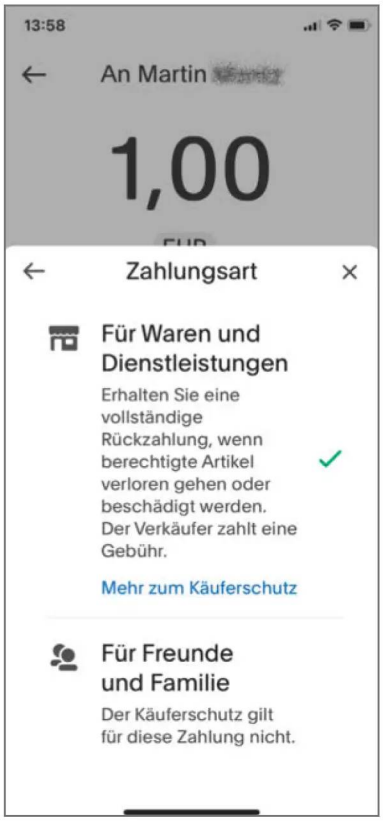
Der Käuferschutz kann (!) laut PayPal helfen, „falls die Ware nicht ankommt oder nicht mit der Angebotsbeschreibung übereinstimmt“. Geht Ihr Käuferschutzantrag durch, erstattet PayPal Ihnen den Kaufpreis plus die Versandkosten. Dafür gibt es grob vier Voraussetzungen, genau wie beim Kauf in Shops.

1. Sie haben den gekauften Gegenstand über Ihr registriertes PayPal-Konto mit der Option „Waren und Dienstleistungen“ bezahlt (für den Verkäufer kostenpflichtig).

2. PayPal hat den Artikel nicht vom Käuferschutz ausgeschlossen. Keinen Käuferschutz gibt es etwa für Alkohol, Tabakwaren, Gutscheine, Immobilien, Gold, Fahrzeuge (außer tragbare) oder Zeitschriften. Gleiches gilt für „verbotene Aktivitäten“ wie den Handel mit Rauschmitteln oder Waffen.

3. Eine der Bedingungen „Artikel nicht erhalten“ oder „entspricht deutlich nicht der Beschreibung“ muss erfüllt sein. Kann der Verkäufer eine elektronische Sendungsverfolgung mit Zustellungsbestätigung vorlegen, gilt der Artikel für PayPal normalerweise als übergeben. Dann bleiben Ihnen nur noch





Als Grundvoraussetzung für den Käufer- und Verkäuferschutz bei PayPal wählt der Käufer eine Zahlung für „Waren und Dienstleistungen" beim Abschluss. Sie ist für den Verkäufer kostenpflichtig.

die im Gesetz vorgesehenen Wege. Ein Antrag auf Käuferschutz wegen „Artikel nicht erhalten" scheidet auch aus, wenn Sie die Ware persönlich abgeholt haben oder jemand anders dies für Sie getan hat. „Entspricht deutlich nicht der Beschreibung" meint etwa falsche Gegenstände wie Tablet statt Handy, aber auch andere Ausstattung wie 32 statt 128 GByte Speicher oder gebraucht statt neu und originalverpackt. Oft müssen Sie in diesem Fall den Artikel zurückschicken – und zwar unbedingt an die von PayPal dafür genannte Adresse und auf Ihre Kosten. Den früher beliebten Retourenservice hat PayPal abgeschafft.

Paypal AGB
ct.de/w59p

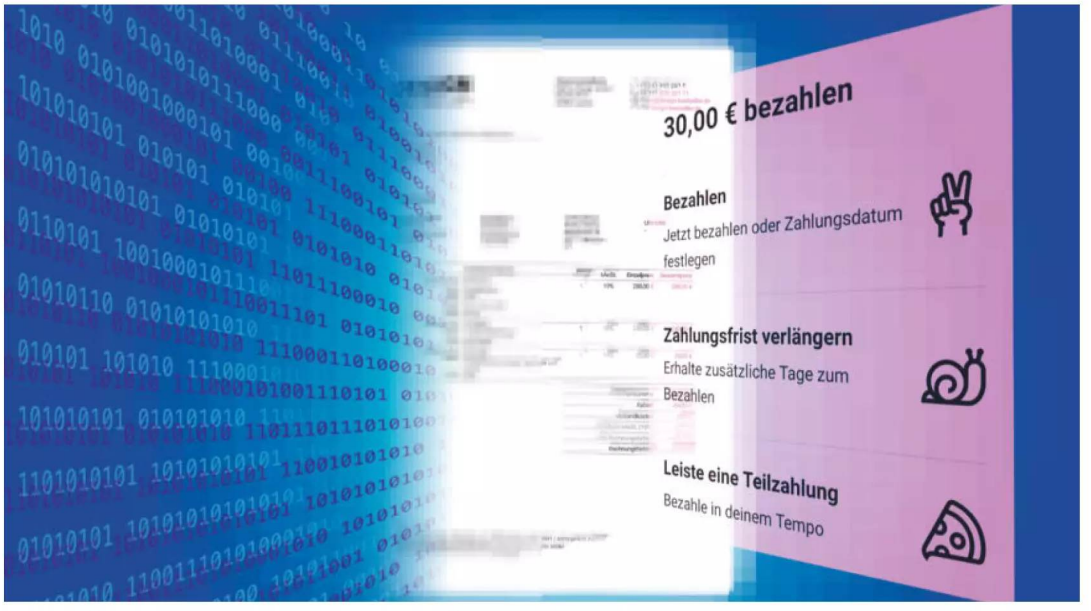
4. Sie haben das Käuferschutzverfahren spätestens 180 Tage nach dem Vertragsschluss (in der Regel das Zahlungsdatum) geltend gemacht. Außerdem haben Sie alle Fragen beantwortet, die PayPal Ihnen gestellt hat, alle angeforderten Belege – wie etwa Fotos – geliefert und alle Fristen eingehalten.

Verkäuferschutz

Der Verkäuferschutz soll Sie nach dem Versand eines Artikels gegen ausgebliebene oder zurückgerufene Zahlungen von Käufern schützen. Beispiele: Der Käufer gleicht sein PayPal-Konto über sein Girokonto aus, letzteres ist aber nicht gedeckt, oder er bucht eine Lastschrift oder Kreditkartenzahlung zurück. Der Verkäuferschutz kann auch einspringen, wenn der Käufer ein Käuferschutzverfahren verloren hat und trotzdem eine Rückbuchung gegen PayPal veranlasst. Ebenso sind Betrugsfälle abgedeckt, wenn also der eigentliche Inhaber eines PayPal-Kontos die Zahlung nicht autorisiert hat.

In allen Fällen wird PayPal den Zahlungsbetrag blockieren respektive belasten und nur freigeben, wenn der Verkäuferschutz tatsächlich greift. Das gilt auch, wenn jemand ein Käuferschutzverfahren gegen Sie eingeleitet hat. Der Verkäuferschutz greift dabei nur unter bestimmten, hier die grob aufgelisteten Voraussetzungen:

1. Der Käufer hat mit der (für Sie als Verkäufer kostenpflichtigen) Funktion „Waren und Dienstleistungen" bezahlt.
2. Die Zahlung muss in den Transaktionsdetails „abgeschlossen" sein.
3. Sie haben alle Anfragen von PayPal fristgerecht beantwortet und angeforderte Belege geliefert.
4. Der Artikel wird vom Verkäuferschutz abgedeckt.
5. Sie können PayPal eine den Richtlinien entsprechende Versandbestätigung zukommen lassen (am besten eine Sendungsverfolgung mit Online-Trackingnummer, Absender- und Empfängeradresse und Zustellnachweis). Selbstabholung des Artikels durch den Käufer schließt PayPal explizit vom Verkäuferschutz aus – dies ist ein beliebter Hebel für Betrugsmaschen vermeintlicher Käufer (siehe Artikel „PayPal-Betrug auf Kleinanzeigenportalen" ab S. 108).
6. Sie haben den Artikel an die Adresse versandt, die in den Transaktionsdetails angegeben ist.
7. Sie haben den Artikel spätestens sieben Kalendertage nach Zahlungseingang versandt. (mon) **c't**



Kostenfallen beim „Später zahlen“

Mit Diensten wie Klarna und PayPal fließt das Geld auf Wunsch erst nach einigen Wochen oder in Raten. Wir erklären, in welchen Fällen „Später zahlen“ sicher und bequem ist, wann man unnötig draufzahlt – und weshalb vor allem junge Menschen aufpassen sollten.

Von **Markus Montz**

Zu den bewährten Onlineshopping-Zahlungsarten Rechnung, PayPal, Lastschrift und Kreditkarte ist in den vergangenen Jahren eine weitere getreten: „Shoppe jetzt. Bezahle später“, wirbt zum Beispiel der schwedische Zahlungsdienstleister Klarna auf seiner Homepage. „Heute shoppen. Erst 30 Tage später zahlen“, heißt es bei PayPal. Der Vorteil liegt auf der Hand: Man zahlt nicht sofort bei der Bestellung, sondern nachdem man die Ware erhalten und geprüft hat.

Dieses „Später bezahlen“, im Fachjargon auch „Buy now, pay later“ oder einfach „Pay later“ genannt, bieten beide Konzerne außerdem als Ratenzahlung mit Kreditzinsen an. Je nach Händler, Rechnungssumme und Kunde sind auch drei zinslose Monatsraten möglich. Was der klassischen Rechnung, der Null-Prozent-Finanzierung und dem herkömmlichen Verbraucherkredit ähnelt, unterscheidet sich in der Praxis jedoch durchaus, und es gibt einige Risiken.

Auf dem sozialen Netzwerk TikTok etwa kursieren Videos junger Menschen, die sich gegenseitig mit ihren Schuldenständen bei Klarna überbieten – oft verbunden mit dem Eingeständnis, dass ihnen die Verbindlichkeiten nach dem Kaufrausch über den Kopf gewachsen sind. Auch Verbraucherschützer warnen vor Schuldenfallen und kritisieren „Später bezahlen“ als Geschäftsmodell, das Onlineshopper leichter in den ungebremsten Konsum und nachfolgende Zahlungsschwierigkeiten bringen könne.

Wir haben uns „Später bezahlen“ bei Klarna und PayPal genauer angesehen (zu weiteren Anbietern siehe Kasten „Weitere Anbieter von ‚Später bezahlen‘“ auf S. 83) und zeigen, welche Geschäftsmodelle sich dahinter verbergen, welche Bezahlmodelle aus Kundensicht sinnvoll sind, wo die Risiken liegen und welche Alternativen es gibt.

So sicher wie Rechnungskauf

Unter „Später zahlen“ fallen drei verschiedene Konzepte, Waren und Dienstleistungen zu kaufen. Beim einfachsten – und aus Kundensicht sichersten – zahlt man wie bei der klassischen Rechnung bis zu einem Fälligkeitsdatum („Zahlungsziel“). Bei PayPal geht das mit Beträgen ab 99 bis 1000 Euro. Bei Klarna haben Neukunden ein Limit von 90 Euro, das sich nach pünktlichen Zahlungen schnell deutlich erhöht. Ein fixes Maximum nennt Klarna nicht.

In der Regel prüfen die Anbieter außerdem vor der ersten Zahlung bei Schufa & Co. die Kreditwürdigkeit, sporadisch kommt das auch später noch vor. Fällt die Prüfung hinreichend positiv aus, ist die Zahlung dann erst 30 Tage nach dem Datum fällig, an dem der Händler die Rechnung erstellt hat. Bei PayPal gibt es für manche Händler auch noch eine 14-Tage-Regelung, Klarna hat diese abgeschafft.

Im Unterschied zur klassischen Rechnung, bei der man das Geld selbst überweist, benötigt man bei beiden Anbietern ein Kundenkonto, um eine Zahlung aufschieben zu können. Dort muss man seine Bankverbindung hinterlegen. PayPal holt sich den Betrag dann automatisch zum Fälligkeitsdatum vom PayPal-Guthaben oder per Lastschrift. Bei Klarna muss man selbst aktiv werden und im Kundenkonto auf der Website oder in der App die Lastschrift rechtzeitig anstoßen. Man spart sich dabei nicht nur den Wechsel ins Onlinebanking, sondern auch das Abtippen oder Kopieren der Daten wie IBAN und Rechnungsnummer.

Der größte Vorteil liegt aus Kundensicht darin, dass der Händler in Vorleistung geht. Analog zum beliebten Kauf auf Rechnung erhält man die Ware und kann sie auspacken und begutachten, bevor auch nur ein Cent fließt. Ist man nicht einverstanden und schickt etwas zurück, zahlt man dafür oftmals überhaupt nicht und muss seinem Geld nicht hinterherlaufen – anders als bei Kreditkartenzahlungen

Wie Klarna und PayPal Geld verdienen

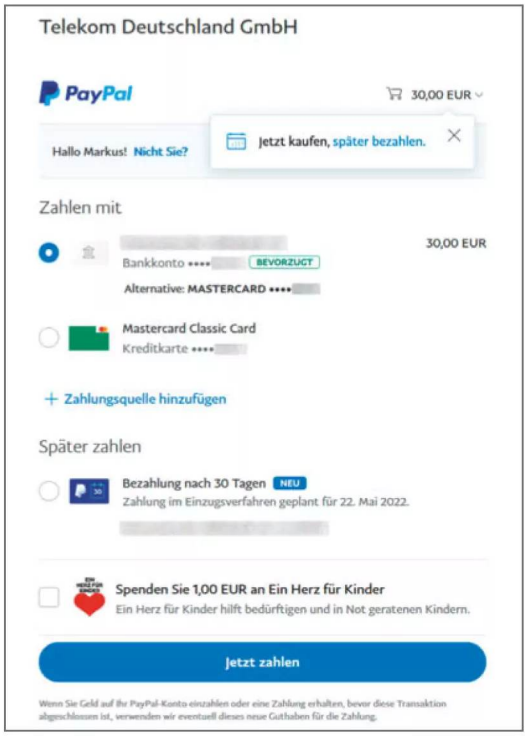
PayPal und Klarna gehören zu den größten Zahlungsdienstleistern für Onlinehändler in Europa, beide sind als Banken lizensiert (Klarna bei der strengen schwedischen Aufsicht, der US-Konzern PayPal im deutlich weniger strengen Luxemburg). PayPals wichtigster Service ist der beliebte E-Geld-Bezahldienst, es bindet aber auch andere Zahlarten für Händler ein. Klarna bietet neben Kreditkarte & Co. insbesondere den Rechnungskauf im traditionellen Stil an. In diesem Bereich hat das Unternehmen auch seine Wurzeln; es startete 2005 mit dem Ankauf und der anschließenden Abwicklung von Rechnungen (Factoring) – wobei das Unternehmen stärker als die Konkurrenz auf digitale Prozesse setzte.

Im Jahr 2022 machten Rechnungen, auch über die Tochter Billpay, und rechnungsartige „Später bezahlen“-Käufe nach Unternehmensangaben 53 Prozent der von Klarna in Deutschland abgewickelten Zahlungen aus. Zahlarten wie Kreditkarten, Lastschrift und „Sofortüberweisung“ stellten 46 Prozent, der besonders kritisierte Ratenkauf lediglich ein Prozent. PayPal schlüsselt nationale Märkte nicht auf, der Anteil der Ratenzahlungen dürfte aber noch niedriger liegen. Das ist jedoch nicht gleichbedeutend mit den Umsatzanteilen. Klarnas Geschäftsbericht für 2022 deutet bei einem Blick in die Zahlen darauf hin, dass die Zinseinkünfte gemessen an den eingenommenen Händlerentgelten grob im Verhältnis 1:3 bis 1:4 stehen. Letztere stellen also den deutlich größeren Anteil, gemessen an den ein Prozent aller Zahlungen darf man das Ratenkreditgeschäft aber keineswegs unterschätzen -- selbst dann nicht, wenn es nur einen Teil der Zinseinkünfte abwirft.

oder Überweisungen. Nur wenn die Zahlung doch schon erfolgen musste, weil die Retoure erst nach der Frist beim Händler einging, läuft die Rückzahlung über den Händler. In Streitfällen sollen die Käuferschutzprogramme von Klarna und PayPal helfen – dafür muss man aber die Paketverfolgungsnummer gut aufbewahren.

Der Nachteil ist der gleiche wie beim Rechnungskauf, jedenfalls bei Klarna: Es kann vorkommen, dass man den Zahlungstermin vergisst. Die Schweden senden zwar zwei Tage vor Ultimo eine Push-Nachricht. Die setzt aber die App voraus. Nach dem Termin gerät man in Verzug; erst dann kommen auch Mails. Zwar sind die dann folgenden Mahngebühren mit 1,85 Euro pro Mahnung erträglich, nach drei Mahnungen kommt allerdings ein teures Inkassoverfahren, das je nach Zahlungsbetrag einige Dutzend bis mehrere hundert Euro teuer sein kann.

Wichtig ist zudem, dass das Konto gedeckt ist; das wiederum gilt auch für PayPal. Platzt eine Lastschrift, fordert PayPal neben 2,80 Euro Verzugsgebühr die Gebühr zurück, die das Unternehmen an die Bank zahlen muss (in der Regel um 3 bis 4 Euro). Klarna nimmt neben den 1,85 Euro Mahngebühr pauschal 4 Euro für die Rücklastschrift. Beide Dienste lassen bis zur Klärung keine Einkäufe mehr zu und leiten unter Umständen ein Inkassoverfahren ein. Außerdem behalten sich die Anbieter vor, dem Kunden zukünftig „Später bezahlen“ ganz zu verweigern oder den maximal möglichen Betrag zu begrenzen – und ein paar Eskalationsstufen weiter auch (negative) Nachricht an Schufa & Co. zu geben.



Bei rechnungsartigem „Später bezahlen“ bekommt man die Ware, bevor das Geld fließt.

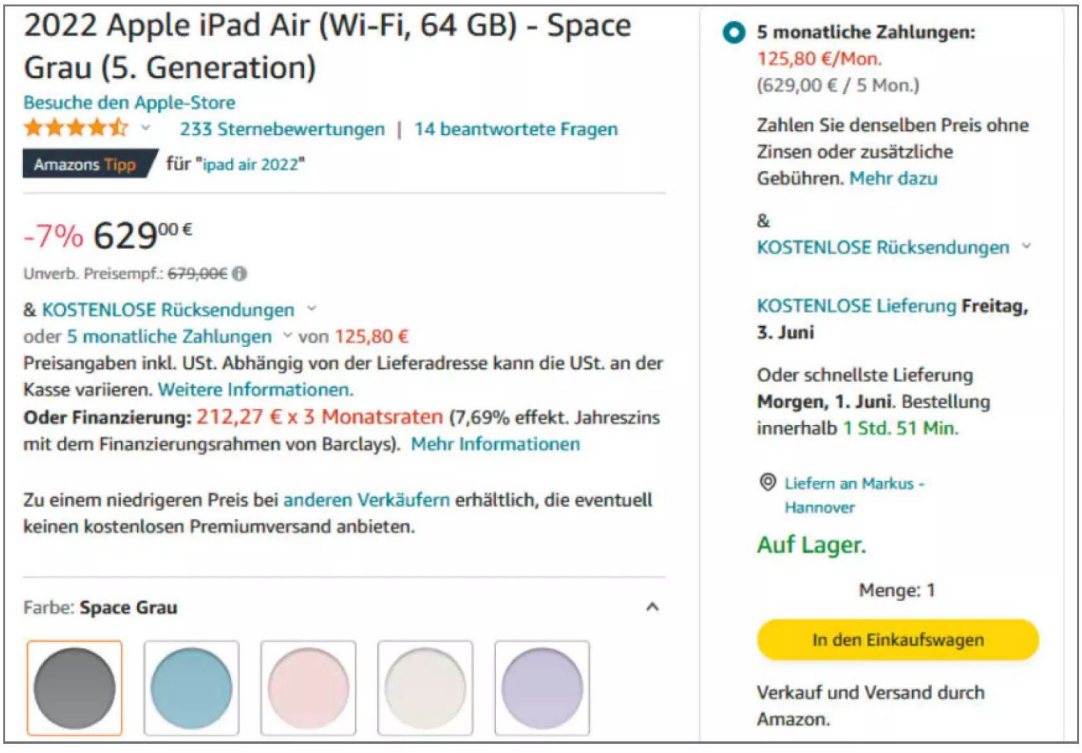
Auch wenn man es nicht so weit kommen lässt, kann der spätere Zahltermin dazu verleiten, impulsiv mehr zu kaufen als geplant. Wer dann noch das Konto überzieht, zahlt teure Dispozinsen. Was Klarna seinen Händlern als Vorteil anpreist, ist für Kunden also am Ende eine potenzielle Falle, unnötig Geld auszugeben. Mit seiner bunten, vor allem an jüngeres Publikum gerichteten Werbung macht speziell Klarna nicht den Eindruck, Impulskäufe verhindern zu wollen – so sehr die Schweden auch beteuern, ihre Kunden finanziell bilden zu wollen und an pünktlichen Zahlungen interessiert zu sein.

Auf Wunsch kann man bei beiden Anbietern die Zahlung verschieben: bei PayPal einmalig um 30 oder 54 Tage, bei Klarna einmalig um 30 oder 60 Tage. Das kostet einen Aufschlag, der sich nach dem Betrag richtet. Dieser Aufschlag sieht niedrig aus, machte bei uns auf ein Jahr hochgerechnet aber teils über 30 Prozent der Kaufsumme aus – dagegen sind selbst Dispozinsen ein Schnapper.

Zweischneidig: Zinslose Raten

Das zweite Modell von „Später bezahlen“ ist eine zinslose Ratenzahlung, oft auch „Null-Prozent-Finanzierung“ genannt. PayPal und Klarna bieten dieses Modell grundsätzlich als Zahlung in drei Raten an. Bei PayPal muss dazu allerdings auch der Händler mitspielen. Klarna setzt das nicht zwingend voraus, sondern ermöglicht auch, Rechnungskäufe auf diese Weise abzustottern. Allerdings bekommt nicht jeder Kunde für jeden Einkauf das Angebot.

Zinslose Ratenzahlungen findet man darüber hinaus in zahlreichen Shops, beispielsweise bei Amazon oder zu bestimmten Aktionszeiträumen bei Otto. Im Unterschied zu Klarna und PayPal sind deren „Später bezahlen“-Dienstleister aber oft direkt beim Händler integriert und bieten oft keine gesonderten Apps oder Web-Portale für Kunden – es sei denn, man gerät zufällig an einen der Kandidaten im Kasten „Weitere Anbieter von ‚Später bezahlen‘“



Null-Prozent-Finanzierungen, von Amazon „x monatliche Zahlungen“ genannt, können für dringend benötigte Güter nützlich sein. Man sollte aber vorab Preise vergleichen, um nicht doch draufzuzahlen.

auf Seite 83. Ansonsten läuft die Kommunikation über den Händler.

Solche „Null-Prozent-Finanzierungen“ erstrecken sich über einen Zeitraum zwischen drei und zwölf Monaten. Die erste Rate wird meistens sofort fällig, die anderen gehen monatlich als Lastschrift oder von der Kreditkarte ab. Anders als beim rechnungsartigen Kauf mit „Später bezahlen“ hat man also schon eine Teilzahlung geleistet, wenn der Einkauf ankommt, allerdings nicht den kompletten Betrag. Bei Mängeln ist das immer noch von Vorteil.

Null-Prozent-Finanzierungen können praktisch sein, wenn etwa die Waschmaschine kaputt geht und die Reserven nicht mehr reichen. Man sollte aber in jedem Fall die Preise mehrerer Händler vergleichen. Mitunter bekommt man das gleiche Produkt anderswo billiger, wenn man sofort zahlt. Bedenken sollte man außerdem, dass Kreditkarte und Rechnungskauf ebenfalls Zahlungsaufschub ohne Zinsen ermöglichen.

Noch mehr als beim rechnungsartigen „Später bezahlen“ gilt bei der Null-Prozent-Finanzierung, dass man sich vor Impulskäufen hüten, den Überblick über seine Verbindlichkeiten behalten und für Kontodeckung sorgen muss. Andernfalls drohen nach einem Kaufrausch nämlich Überziehungszinsen, Mahnungen, Inkassoverfahren und im schlimmsten Fall ein negativer Schufa-Eintrag.

Finger weg von Ratenkäufen

Anstelle der Null-Prozent-Finanzierung bieten Klarna und PayPal eine dritte Variante von „Später bezahlen“ mit verzinsten Teilzahlungen in 3 bis 24 Monatsraten an. Den Rechnungsbetrag stottert man in festen Monatsraten – bei Klarna mindestens sieben Euro – über eine feste Laufzeit ab. Man kann aber auch jederzeit den kompletten Restbetrag zurückzahlen. Dann spart man die zusätzlichen Zinsen, die für jeden weiteren Monat auflaufen. Während PayPal die Raten automatisch monatlich abbucht, muss man bei Klarna in der Voreinstellung die Lastschrift für jede Rate selbst anstoßen. Das kann man in der Klarna-App aber auf automatischen Einzug umstellen.

Die Zinsen haben es in sich: Klarna verlangte bei uns bis zu 15, PayPal um zehn bis zwölf Prozent effektiven Jahreszins. Das ist teurer als viele Dispos. Schon deshalb raten wir grundsätzlich davon ab.

Von verzinsten Ratenkrediten bei Klarna und PayPal lässt man besser die Finger. Die Zinsen sind vergleichsweise hoch.

Wer einen Ratenkauf für eine langfristige Investition wie eine neue Einbauküche plant, wird wohl ohnehin eher Vergleichsportale für Verbraucherkredite bemühen oder ein Angebot vom Verkäufer der Küche erhalten. Solide Kreditwürdigkeit vorausgesetzt, landet man dann in der Regel bei deutlich unter 10 Prozent und spart jede Menge Geld.

Doch Klarna und graduell auch PayPal sprechen noch ein anderes Kundensegment an als den wohlkalkulierenden Küchenkäufer, der seine finanziellen Möglichkeiten kennt: Menschen, die deutlich kleinere Beträge für deutlich kurzlebigere Produkte ausgeben und ein geringes Einkommen haben, vor allem Jugendliche und junge Erwachsene. Selbst die Zahlung von Bagatellbeträgen um die 30 Euro, beispielsweise für ein hippes T-Shirt, kann man bei Klarna so in die Länge ziehen. Das ist gefährlich, denn die Zinsen läppern sich eben doch.

PayPal setzt für die Ratenzahlung immerhin eine Untergrenze von 99 Euro, doch das ändert an der Kernaussage nichts. Im Endeffekt bringt „Später bezahlen“ auf Raten alle potenziellen Nachteile mit sich, die man auch in der rechnungsartigen und in der Null-Prozent-Kredit-Variante finden kann – plus die knackigen Kreditzinsen. Mit ihnen steigt das Risiko immens, in der Schuldenfalle zu landen.

Gesetzeslücke

Klarna und PayPal profitieren derzeit noch von der Gesetzeslage. Die maßgebliche EU-Verbraucherkreditrichtlinie stammt von 2008 und damit aus einer Zeit, in der Händler und Banken Verbraucherkredite deutlich sorgfältiger und nicht digital in Echtzeit vergaben. Um etwa das „Anschreiben lassen“ beim Kaufmann an der Ecke auszunehmen, hatte die EU deshalb damals eine Bagatellgrenze eingezogen: Für Beträge unter 200 Euro oder zinsfreie Darlehen

Überschuldet – und nun?

Ist man bereits in der Schuldenfalle gelandet, helfen Schuldnerberatungen. Gemeinsam mit den Betroffenen erstellen sie einen Plan, damit diese ihre Verbindlichkeiten sortieren und zurückzahlen können. Die anerkannten Beratungen von Kommunen, Wohlfahrtsverbänden wie der Caritas und den Verbraucherzentralen haben jedoch lange Wartelisten – gleichzeitig tummeln sich viele unseriöse Beratungen auf dem Markt. Die Verbraucherzentralen haben einen Leitfaden samt Checkliste zusammengestellt (siehe ct.de/wqvb).

Weitere Anbieter von „Später bezahlen“

Zu den Akteuren, die wie Klarna und PayPal eine direkte „Später bezahlen“-Kundenschnittstelle pflegen, gehören in Deutschland die Santander Bank mit „Zinia“, außerdem Scalapay, Sezzle und Riverty (das zugleich als Auskunftei und Inkassounternehmen auftritt). Hinzu kommen Zahlungsdienstleister wie Ratepay, Unzer oder Intercard, die ihr Angebot ohne direkten Kundenzugang als Whitelabel-Produkt bei Händlern integrieren.

Überdies bieten einige Banken für bestimmte Abbuchungen „Später bezahlen“-Optionen an, etwa die Neobank N26. Auch für Kreditkarten gibt es mitunter Raten-Optionen oder die oft gebührenfreie Karte kommt mit einem „revolvierenden“ Kredit anstelle der monatlichen Komplettabbuchung (siehe Glossarkasten auf S. 39) – dann steigt der effektive Jahreszins bei einigen Finanzdienstleistern allerdings auf über 20 Prozent.

muss der Kreditgeber nicht die Kreditwürdigkeit des Kunden prüfen.

Aufgrund dieser Ausnahme können Klarna und PayPal auch weniger solventen Kunden Kredite (und dazu zählt de facto auch die Zahlung auf Rechnung) anbieten. Zwar fragen beide Konzerne Daten bei Schufa & Co. ab und pflegen interne Datenbanken, mit deren Hilfe ihre Algorithmen in Sekundenschnelle Kreditentscheidungen treffen. Der hohe Zinssatz deutet aber darauf hin, dass sie Kredite vergleichsweise großzügig gewähren und ein relativ hohes Ausfallrisiko einpreisen.

Ende 2022 hat die EU jedoch eine neue Verbraucherkreditrichtlinie beschlossen. Ab 2026 müssen die Anbieter die Kreditwürdigkeit ihrer Kunden ab dem ersten Euro prüfen, auch bei zinsfreien Ratenzahlungen. Vorzeitige Rückzahlungsmöglichkeiten sind ebenso Pflicht wie eine transparente Aufstellung der Kreditkosten. Außerdem müssen Kreditanbieter vor den Belastungen warnen und dürfen nicht mit finanzieller Erleichterung werben. Die Deckelung der Kreditkosten einschließlich Mahngebühren, die Verbraucherschützer gefordert hatten, legen jedoch die Mitgliedsstaaten selbst fest. Auch EU-einheitliche Strafen für Verstöße fehlen.

Klarna hat reagiert: Ausweislich der Unterseite „Wikipink“ haben die Schweden schon Anfang 2022 die Frist für das rechnungsartige „Später bezahlen“ von 14 auf 30 Tage geändert. Mittlerweile hat das Unternehmen auch die flexiblen Ratenkredite abgeschafft, bei denen Kunden bei einer Mindestrate von sieben Euro die Tilgung extrem lange ausdehnen konnten. Die Kreditkosten zeigt Klarna nun wesentlich transparenter an; auch die Zahlung in drei zinslosen Raten dürfte der Charmeoffensive entspringen. Zudem hat der Dienst die Mahngebühren gesenkt und erinnert häufiger an offene Zahlungen als früher – allerdings vor allem nach dem Zahlungstermin. Zu den Zinssätzen oder einer konkret verschärften Prüfung der Kreditwürdigkeit verliert Klarna auf „Wikipink“ aber kein Wort.

Ein Daumen hoch, zwei runter

Können wir die „Später bezahlen“-Services von Klarna und PayPal beim Onlineshopping empfehlen? Für die rechnungsartigen Modelle von „Später bezahlen“ ist die Antwort ein klares „Ja“. Voraussetzung ist, dass man an die Fristen denkt, bei mehreren offenen Zahlungen den Überblick behält und am Fälligkeitstermin genug Geld hat – aber das kennt man ja bereits vom klassischen Rechnungskauf. Anders als beim Kauf per Kreditkarte, PayPal-Standardzahlung oder Lastschrift hält man die Ware dafür in der Hand, bevor man zahlt – und kann sie oft sogar retournieren, ohne dass Geld geflossen ist. Kundenfreundlicher geht es kaum.

Auch Null-Prozent-Finanzierungen über mehrere Monate können für unumgängliche Anschaffungen hilfreich sein. Auf der anderen Seite verlocken sie zu Impulskäufen, die man sich vielleicht gar nicht leisten kann und die womöglich ein größeres Preisschild tragen als das gleiche Produkt in anderen Shops. Für diese Art von „Später bezahlen“ fällt unser Fazit daher gemischt aus: Zur Finanzierung kurzlebiger Konsumgüter raten wir auf jeden Fall davon ab.

Von „Später bezahlen“-Ratenkäufen mit Kreditzinsen profitieren hingegen nur Klarna, PayPal und der Händler. Die Zinsen sind im Vergleich zu klassischen Verbraucherkrediten viel zu hoch, als Käufer zahlt man immer drauf. Damit ist eigentlich schon alles gesagt. Dass man sich bei Kontrollverlust auch noch überschulden kann und die Konzerne das bei unerfahrenen Kunden zumindest in Kauf nehmen, verschlimmert das Fazit noch. Der Rat fällt eindeutig aus: Hände weg – dann bleibt man finanziell auf der sicheren Seite, fördert ein fragwürdiges Geschäftsmodell nicht und kann sich mit gutem Gewissen an seinen Einkäufen freuen. (mon) c't

Leitfaden bei Überschuldung
ct.de/wqvb

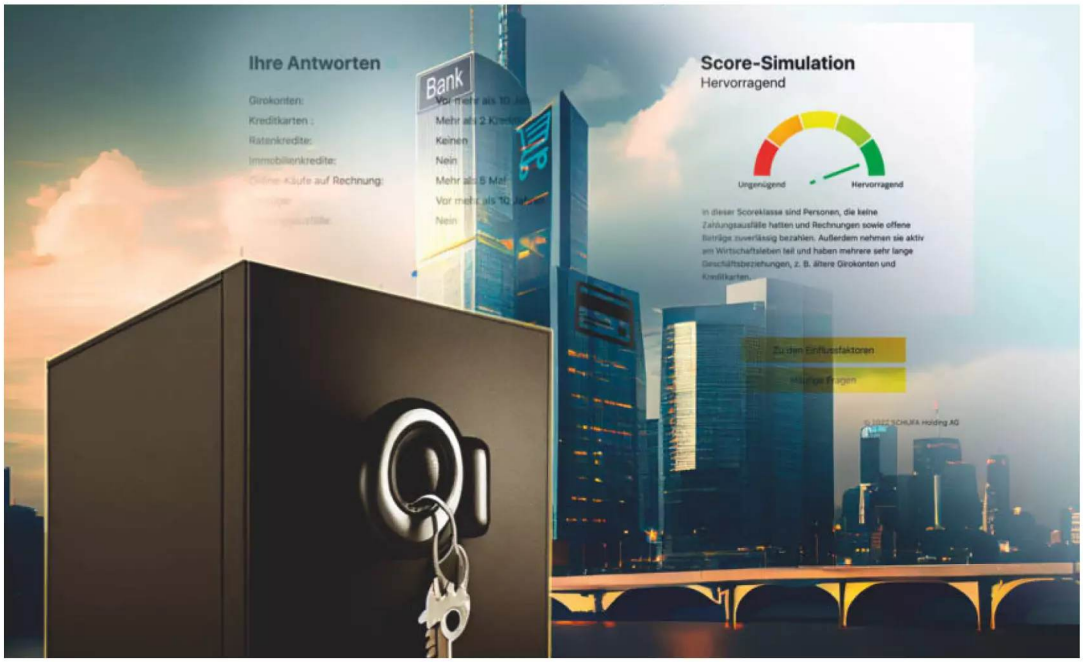


Bild: KI Midjourney | Bearbeitung: c't

Wie die Schufa Ihre Bonität berechnet

Die Auskunftei Schufa hält die Formel geheim, mit der sie Ihre Bonität ermittelt. Im Rahmen einer neuen Transparenzoffensive gewährt sie jedoch einen besseren Einblick, welche Faktoren den Score beeinflussen. Wir erklären das System und geben Tipps, wie Sie schlechte und falsche Bewertungen vermeiden.

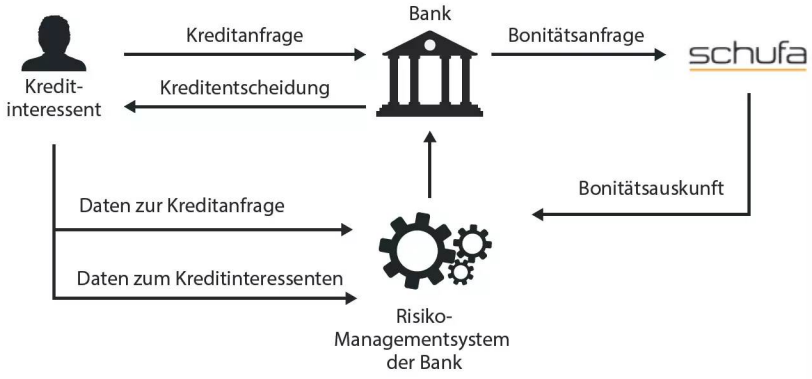
Von **Markus Montz**

Sie shoppen im Internet, gehen zur virtuellen Kasse und wählen „Kauf auf Rechnung". Das System arbeitet kurz und meldet Ihnen dann zurück, dass die gewünschte Bezahlmethode nicht zur Verfügung steht. Auf Nachfrage teilt der Händler Ihnen mit, dass wohl die Schufa-Prüfung gescheitert sei. Aha, denken Sie, die Schufa mal wieder, obwohl Sie keine offenen Rechnungen haben und auch sonst pünktlich und zuverlässig zahlen. Was haben die denn für ein Problem mit mir?

Wegen solcher Vorfälle, die sich viele Menschen nicht erklären können, haben Auskunfteien und insbesondere die Schufa einen notorisch schlechten Ruf. Dabei gehört unser Beispiel noch zu den eher harmlosen Folgen, wenn etwas schiefläuft. Im schlimmsten Fall hat die Schufa falsche Informatio-

Kreditwürdigkeitsprüfung

Bei einem Kreditwunsch schickt die Bank Name, Adresse und Geburtsdatum der Person an die Schufa. Die sendet Informationen über vertragsgemäß abgewickelte oder laufende Geschäfte der Person zurück, zum Beispiel Ratenkredite oder Girokonten. Die Schufa meldet der Bank außerdem Zahlungsstörungen oder öffentliche Negativeinträge wie eine Privatinsolvenz sowie auf Anfrage einen Score. Die Bank reichert diese Informationen mit eigenen Daten an. Dazu zählen Kreditlaufzeit und -höhe, aber auch Einkommen oder Beruf der Person.
Im Risikomanagement entscheidet die Bank nun, ob sie den Kredit gewährt.



nen über Menschen gespeichert, denen dadurch existenzielle Geschäfte wie eine Kontoeröffnung oder ein Mietvertrag für eine Wohnung versperrt sind. Schufa & Co. haben kräftig zu ihrem schlechten Ruf beigetragen, denn die Fehlerkultur ließ lange stark zu wünschen übrig. Ihre Arbeit erklärte sie, wenn überhaupt, nur für Fachjuristen verständlich.

Wir zeigen, wie und auf welcher Grundlage die Schufa arbeitet und warum sie wichtig ist. Außerdem erklären wir, wie Sie sich gegen falsche Einträge wehren und wie Verbraucher- und Datenschützer erwirken, dass die Schufa allmählich offener kommuniziert.

Was tun Auskunfteien?

Kreditgeschäfte sind Vertrauensgeschäfte. Wer anderen Geld leiht, muss darauf zählen, dass er die Kreditsumme plus Zinsen zurückbekommt, egal ob Dispo, Kreditkarte oder Ratenkredit. Ähnliches gilt für Rechnungskäufe (Warenkredite), Mietverträge oder Mobilfunk-Laufzeitverträge, kurzum: immer dann, wenn der Kunde bereits gelieferte Waren oder Dienstleistungen noch bezahlen muss.

So etwas klappt aber erfahrungsgemäß nicht einmal unter Freunden oder beim Bierdeckel in der Kneipe immer zuverlässig. Noch schwieriger wird es, wenn sich beide Seiten nicht kennen. Nun braucht der Kreditgeber eine belastbare Auskunft darüber, ob der Kreditnehmer aller Voraussicht nach zahlen wird oder nicht.

An dieser Stelle kommen Wirtschaftsauskunfteien ins Spiel. Sie sammeln für solch eine Prognose Informationen über das Zahlungsverhalten einer Person: Hat die Person Kredite vertragsgemäß getilgt oder Rechnungen trotz mehrfacher Mahnung nicht bezahlt? Auskunfteien halten außerdem Identitäts- und Adressdaten vor. All das führen sie in einer Datenbank zusammen. Wenn ein Kreditgeber anfragt, stellt ihm die Auskunftei die erforderlichen Daten zur Verfügung. Sie bestätigt einem Händler oder einer Bank aber beispielsweise auch nur die Identität einer Person.

Auf Basis der Daten befindet der Kreditgeber über den Kredit oder dessen Zinsen. In Zeiten des Internets stellen ihm Auskunfteien die Daten in Echtzeit bereit, sodass er in Sekunden automatisch entscheiden kann. Außerdem errechnen Auskunfteien die Wahrscheinlichkeit, ob jemand zahlt oder nicht. Die Beweggründe sind unerheblich: Ob er von vornherein nicht zahlen will, unvorhergesehen in Not gerät,

vergesslich ist oder seine Möglichkeiten überschätzt, spielt keine Rolle. Auf die Rückzahlungsprognose hat es mathematisch dieselbe Wirkung.

Auskunfteien helfen daher prinzipiell auch dem Kreditnehmer. Im Idealfall bewahren sie ihn vor Überschuldung und Zahlungsunfähigkeit und halten die Zinsen für alle auf einem erträglichen Level. Denn die Kreditgeber preisen die statistisch zu erwartenden Zahlungsausfälle ein. Ohne verlässliche Prognosen gäbe es mehr Zahlungsausfälle und die Zinsen wären für alle Kreditnehmer höher.

Die Wahrscheinlichkeit, dass der Kreditnehmer zahlt oder zurückzahlt, bilden Auskunfteien in einem „Score“ ab, der die Kreditwürdigkeit (Bonität) ausdrückt. Die Bonität errechnen Auskunfteien aus den vorliegenden Daten und stellen ihren Auftraggebern beides auf Anfrage zur Verfügung. In der Regel ermitteln sie für verschiedene Branchen eigene Scores. Bei der Schufa gibt es beispielsweise neben einem „Basisscore“ mindestens drei „Bankenscores“ für Sparkassen, Genossenschaftsbanken und Privatbanken sowie Scores für Onlinehandel, stationären Handel und Telekommunikation.

Viele Kreditgeber analysieren zusätzlich eigene Daten, bevor sie eine Entscheidung treffen. Die Hausbank dürfte einen Blick auf das Girokonto werfen, ein Onlinehändler auf die Zahlungsmoral bei bisherigen Einkäufen. Die Risikobereitschaft und das Geschäftsmodell des Kreditgebers spielen ebenfalls eine Rolle. Wo eine Sparkasse lieber keine Risiken eingeht, steht beim „Buy now, pay later“-Konzept von Klarna vielleicht der Abschluss im Vordergrund (siehe Artikel „Kostenfallen beim Später zahlen“ auf S. 78).

Wer ist die Schufa und was sammelt sie?

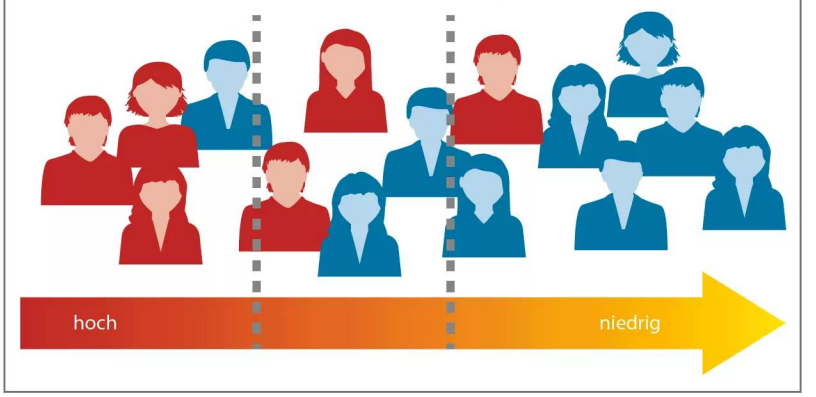
Die mit Abstand größte und wichtigste Wirtschaftsauskunftei in Deutschland ist die „Schutzgemeinschaft für allgemeine Kreditsicherung“ (Schufa) mit Sitz in Wiesbaden. Das Unternehmen ist mehrheitlich im Besitz der Kreditwirtschaft und speicherte im Jahr 2022 nach eigenen Angaben 1,1 Milliarden Informationen zu 69 Millionen Menschen und 6,3 Millionen Unternehmen. Über 10.000 Unternehmenskunden konnten bei der Schufa aktiv Daten abrufen und einspeisen, 2,3 Millionen Privatkunden besorgten sich Bonitätsauskünfte. Insgesamt gab die Schufa 198,3 Millionen Auskünfte und Nachmeldungen wie zum Beispiel Adressänderungen oder neue Einträge an berechtigte Unternehmenskunden weiter. Das macht über 543.000 pro Tag, davon 320.000 Bonitätsauskünfte. Verbraucher riefen demgegenüber nur insgesamt 3,7 Millionen Auskünfte ab, meist über sich selbst.

Datenquelle der Schufa sind vor allem ihre Vertragspartner, darunter Kreditinstitute, Versandhändler und Mobilfunkanbieter, aber auch Energieversorger und Inkassobüros. Sie melden der Schufa vor allem positive Informationen, solange Verbraucher ihre Verträge einhalten. Dazu zählen Girokonten, Kreditkarten, Rechnungskäufe, Raten- und Immobilienkredite oder Leasingverträge. Laut Schufa hat sie zu mehr als 90 Prozent aller dort verzeichneten Personen nur Positivdaten. „Positiv“ bedeutet nicht, dass sich der Eintrag sofort positiv auf den Score auswirkt – dazu gleich mehr.

Die Vertragspartner melden der Schufa außerdem Zahlungsausfälle, die „weichen“ Schufa-Negativinformationen. Anders als die „positiven“ Daten wirken sie auf jeden Fall negativ auf den Score. Als weiche Negativinformationen gelten zum Beispiel nicht bezahlte Raten oder Rechnungen. Auch gekündigte Kredite oder gekündigte Girokonten, die im Minus sind und die der Kunde nicht ausgeglichen hat, zählen dazu. Wichtig: Die Bank oder der Händler muss den Schuldner vor solch einem Eintrag ausreichend (in der Regel zweimal) gemahnt und ihm genügend Zeit gegeben haben, zu zahlen – zwischen erster

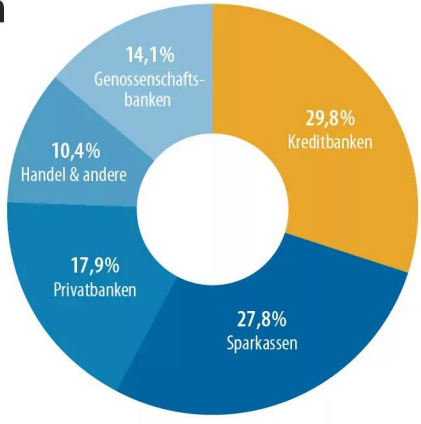
Risikobereitschaft

Der Bonitätswert von Schufa & Co. soll Händler und Banken prinzipiell nur bei der Entscheidung unterstützen, ob sie einen Kredit vergeben. Eine risikoaverse Institution (Grenze weiter rechts) geht auf Sicherheit und nimmt in Kauf, relativ viele kreditwürdige Menschen abzulehnen. Risikoaffine Institutionen preisen zugunsten des Geschäftsabschlusses mehr Zahlungsausfälle ein (Grenze weiter links).



Aktionärsgruppen der Schufa

Die Schufa ist ein Privatunternehmen. Aus dem einstigen Verein ist im Jahr 2000 eine Aktiengesellschaft geworden, deren Anteile zu etwa 90 Prozent die Kreditwirtschaft hält.



und zweiter Mahnung müssen mindestens vier Wochen liegen. Außerdem muss der Gläubiger auf den drohenden Schufa-Eintrag hinweisen und der Schuldner darf die Mahnungen nicht bestreiten. Tut er das doch, muss erst ein Gericht den Fall klären. Einen negativen Schufa-Eintrag gibt es außerdem, wenn man ein Girokonto oder eine Kreditkarte missbräuchlich genutzt hat.

Darüber hinaus gibt es „harte" Negativinformationen. Dazu durchforstet die Schufa öffentliche Bekanntmachungen wie die Schuldnerverzeichnisse der Amtsgerichte. Dort sucht sie nach Personen, die eine Vermögensauskunft abgegeben haben oder sich in einem Verbraucherinsolvenzverfahren befinden. Egal ob harte oder weiche Negativinformationen: Solche Einträge belasten immer die Bonität.

Darf die das?

Um diese Daten zu erheben und an Vertragspartner weiterzugeben, braucht die Schufa keine Einwilligung der betroffenen Person. Als Rechtsgrundlage dient das „berechtigte Interesse" an der Datenverarbeitung nach Artikel 6, Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO). Dieses besteht immer dann, wenn ein Vertrag zwischen einer Person und einem Vertragspartner der Schufa geschlossen werden soll. Grundsätzlich darf man der Schufa die Datenweitergabe zwar untersagen. Der Händler oder die Bank könnte den Einkauf oder die Kreditanfrage dann aber unter Verweis auf die AGB ablehnen.

Die DSGVO lässt offen, wie lange Auskunfteien Daten speichern dürfen. Gemeinsam mit den zuständigen Aufsichtsbehörden hat der Verband „Die Wirtschaftsauskunfteien e.V." verbindliche „Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten" erarbeitet (ct.de/w2f1). Die Schufa ist der Vereinbarung beigetreten und setzt sie nach Angaben von Daten- und Verbraucherschützern auch um; Verbraucher können sich darauf berufen.

So löscht die Schufa beispielsweise Daten aus Schuldnerverzeichnissen, sobald sie dort verschwinden. Einträge über Pfändungs- und Basiskonten tilgt sie unmittelbar nach deren Auflösung oder Kündigung, Kreditanfragen nach zwölf Monaten. Sie löscht aber auch korrekt abbezahlte Kredite nach exakt drei Jahren, „störungsfreie" Verträge sogar sofort nach deren Ende oder Kündigung. Die alte Adresse speichert die Schufa nach einem Umzug noch mindestens drei Jahre; zieht man in diesem Zeitraum nicht erneut um, hält sie die alte Anschrift in vielen Fällen drei weitere Jahre vor, um Identitäten zweifelsfrei zu überprüfen.

Die datenschutzrechtliche Aufsicht liegt beim hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI). Zusätzlich hat die Schufa selbst einen Ombudsmann.

Was den Score warum beeinflusst

Um den Score und damit die Kreditwürdigkeit zu ermitteln, nutzen Auskunfteien wie die Schufa stochastische Verfahren. Die Schufa berechnet also die Wahrscheinlichkeit, dass eine bestimmte Person ihren Zahlungsverpflichtungen nachkommt. Dafür bezieht sie alle Informationen ein, die ihr zur Zahlungshistorie dieser Person vorliegen, und bewertet diese.

Wichtig sind beispielsweise Giro- oder Kreditkartenkonten, also Konten, die ins Minus rutschen können. Je mehr man davon besitzt, desto wahrscheinlicher ist ein Zahlungsausfall. Wenn man ein Girokonto schon viele Jahre ohne Zwischenfälle führt, gilt es hingegen als wahrscheinlich, dass man zuverlässig zahlt.

Den Kontostand und die Kontobewegungen kennt die Schufa nicht. Also weiß sie auch nicht, ob und wie viel jemand verdient oder ob jemand regelmäßig seine Miete zahlt. Aus demselben Grund besitzt die Schufa auch keine Informationen zu Sparkonten, die man ja nicht überziehen kann, oder zum Vermögen.

Die Schufa speichert auch Immobilien- und Ratenkredite. Immobilienkredite, die man vertragsgemäß bedient, wirken sich positiv aus: Schließlich hat eine Bank sie nach eingehender Prüfung vergeben

und die Immobilie dient als Sicherheit. Ratenkredite wirken sich zunächst negativ aus, weil sie immer das Risiko eines Zahlungsausfalls bergen. Je mehr laufende Ratenkredite jemand ansammelt, desto schlechter. Schon deshalb sollte man häufiges „Buy now, pay later“ (siehe Artikel „Kostenfallen beim „Später zahlen“ auf S. 78) vermeiden. Wer hingegen seine Ratenkredite pünktlich bedient, sammelt spätestens nach der letzten Rate Pluspunkte.

Ähnliches gilt auch für Rechnungen: Fragen Händler und Zahlungsdienstleister die Schufa beim Rechnungskauf nach Informationen und Score des Käufers, vermerkt sie das im Konto des Betroffenen. Geschieht das häufig, wirkt es negativ, weil das Risiko eines Zahlungsausfalls steigt. Auch bei Leasing- oder Mobilfunkverträgen besteht immer das Risiko, dass jemand nicht regelmäßig zahlt – vor allem, wenn er mehrere solche Verträge hat. Erfüllt er aber all seine Verpflichtungen über längere Zeit, wirkt das positiv.

Eine Rolle spielt außerdem der Erstwohnsitz, den Vertragspartner der Schufa melden. Zieht man um, hat das meist eine negative Wirkung auf den Score. Menschen, die häufig in kurzer Zeit den Wohnsitz wechseln, zahlen statistisch gesehen häufiger nicht. Wer lange am gleichen Ort wohnt, wird wahrscheinlicher zahlen.

Die Wohngegend berücksichtigt die Schufa nach eigenen Angaben in 99,7 Prozent aller Berechnungen nicht. In den übrigen 0,3 Prozent führt sie für bestimmte Onlinehändler solch ein „Geoscoring“ durch. Voraussetzung sei, dass zu der Person keine anderen Informationen bei der Schufa vorlägen. Das Verfahren ist rechtlich zulässig, sofern das

Was tun bei falschen und unberechtigten Einträgen?

Fehlen der Schufa Daten oder sind dort falsche Daten gespeichert, kann sich das negativ auf Ihre Bonität auswirken. Im Zweifelsfall oder besser noch regelmäßig sollten Sie daher eine kostenlose (Selbst-)Auskunft bei der Schufa einholen (dort auch „Datenkopie“ genannt). Die Auskunft können Sie über ein Online-Kontaktformular, per Mail, per Fax, telefonisch oder per Post anfordern – nicht nur einmal, sondern auch mehrmals im Jahr. Sie kommt grundsätzlich per Briefpost.

Das ist ihre Pflicht: Nach Artikel 15 der DSGVO kann jede Privatperson bei Unternehmen eine kostenlose Auskunft anfordern, ob sie Daten über sie speichern und welche. Auch alle anderen Auskunfteien sowie Inkassobüros sind dazu verpflichtet. Im Selbstversuch klappte das bei Schufa, Crif und Creditreform-Boniversum gut über Kontaktformulare, umständlicher war die Infoscore Consumer Data.

Die Schufa-Auskunft enthält zum Beispiel Kredite, Bankkonten, Mobilfunkverträge sowie Zahlungsstörungen. Sie informiert außerdem darüber, woher die Daten stammen und an welche Unternehmen die Schufa diese weitergeleitet hat. Außerdem finden Sie alle Bonitätsanfragen von Unternehmen aus den letzten zwölf Monaten und die Scores, die diese von der Schufa erhalten haben.

Prüfen Sie die Datenkopie und melden Sie Fehler direkt an das Kundencenter. Die Schufa versichert, dass sie es begrüßt, wenn Verbraucher solche Auskünfte anfordern und Fehler melden. Schließlich helfe dies, dass sie korrekte Daten speichert und weitergibt sowie korrekte Scores berechnet. In Streitfällen wenden Sie sich an den Schufa-Ombudsmann oder den hessischen Datenschutzbeauftragten.

Die „Datenkopie“ alias „Schufa-Auskunft“ ist nicht zu verwechseln mit der kostenpflichtigen Schufa-Bonitätsauskunft, die tagesaktuelle Scores enthält. Sollen Sie dieses 30 Euro teure Dokument bei einem Vermieter vorlegen, reicht das Zertifikat (erstes Blatt mit Hologramm auf dickerem Papier). Darauf ist nur vermerkt, ob Sie am Tag der Ausstellung ausschließlich positive oder auch negative Einträge hatten. Ihre Scores und die Anfragen Dritter gehen den Vermieter nichts an; überlassen Sie ihm das Zertifikat auch nicht im Original.

Wenn Sie mehr als eine solche Bonitätsauskunft pro Jahr brauchen oder regelmäßig über Änderungen in Ihren Schufa-Daten informiert werden möchten, lohnt sich das kostenpflichtige Abo „MeineSchufa“ (derzeit ab 4 Euro im Monat). Bei Anfragen und neuen Einträgen von Unternehmen informiert Sie die Schufa per Mail. Außerdem können Sie sämtliche Einträge und Ihren Basisscore einsehen. Vom kostenlosen Schufa-Dienst Bonify raten wir derzeit hingegen ab.

Alle Links haben wir Ihnen unter ct.de/w2f1 zusammengestellt.

Unternehmen weitere Daten mitschickt und die Schufa diese einbezieht.

Das zeigt ein weiteres Problem auf: Besitzt die Schufa wenige Daten über eine Person, kann sie deren Zahlungsverhalten nur schlecht vorhersagen. Daher startet ein junger Mensch, der nur ein frisch eröffnetes Girokonto besitzt, meist im Mittelfeld („akzeptabel“, siehe Grafik rechts). Solche Personen dürfen anfangs oft nicht auf Rechnung zahlen oder Kredite aufnehmen.

Eindeutig negativ wirken Einträge über Zahlungsausfälle. Wer einfach nur eine Rechnung vergessen und erst nach der ersten Mahnung zahlt, muss noch keine Konsequenzen fürchten. Ist die Forderung aber berechtigt und zweimal angemahnt, sollte man schnell zahlen, um keinen Eintrag für einen Zahlungsausfall zu riskieren. Dann droht nur noch eine Zahlungsstörung“. Sie wirkt schwächer, obwohl auch sie für drei Jahre die Bonität verschlechtert.

Auf unberechtigte Forderungen muss man schnell reagieren. Wie man vorgeht, erklären Leitfäden der Verbraucherzentralen (ct.de/w2f1). Zusätzlich holt man sich spätestens jetzt regelmäßig schriftliche Auskünfte bei der Schufa (siehe Kasten „Was tun bei falschen und unberechtigten Einträgen?“). Das sollten Betroffene auch während einer Privatinsolvenz oder nach einer Vermögensauskunft bei einem Gerichtsvollzieher tun. Denn diese führen automatisch zu „ungenügender“ Bonität.

Sensible Daten wie Nationalität, Religion oder politische Gesinnung erhebt und speichert die Schufa nach eigenen Angaben nicht und bezieht sie auch nicht in den Score ein. Dasselbe gelte für den Familienstand. Alter und Geschlecht nimmt sie nach eigener Darstellung zwar in die Datenbank auf, berücksichtige sie aber selbst nicht. Ebenso wenig nutze sie Daten aus sozialen Netzwerken.

Berechnung und Entscheidung

Als Grundlage für den Score führt die Schufa die Daten einer Person in einer Art Matrix zusammen. Bestimmte Kombinationen ordnet sie verschiedenen Vergleichsgruppen zu (siehe Grafik „Bonitätsberechnung“ auf der nächsten Seite). Für diese Vergleichsgruppen ermittelt sie aus historischen Daten laufend die Quote der Personen, die zuverlässig zahlen. Für Statistik-Experten: Die Schufa nutzt als Analyseverfahren die logistische Regression. Die einzelnen Variablen gewichtet sie dabei unterschiedlich stark.

Folglich kann sich der Schufa-Score sogar dann ändern, wenn man selbst weder umgezogen ist noch Zahlungen versäumt hat. Es genügt, wenn man sich in einer Vergleichsgruppe befindet, die statistisch auf- oder absteigt.

Den eigentlichen Score, also die Zahlungsprognose, errechnet die Schufa daraus mit einer geheim gehaltenen Formel. Diese kennen außer der Schufa nur einige Fachwissenschaftler sowie der hessische Datenschutzbeauftragte. Mithilfe der Formel kombiniert sie die Werte der jeweiligen Vergleichsgruppen und ermittelt daraus die Wahrscheinlichkeit, dass eine Person vertragsgemäß zahlt.

Insgesamt kann die Schufa deutlich über hundert Scores für jede Person berechnen. Viele davon sind aber auf einzelne Unternehmenskunden zugeschnitten. Die erwähnten Branchen-Scores fallen stets unterschiedlich gut aus, da die Schufa branchenspezifische Merkmale darin stärker gewichtet als im Basisscore. Dieser liefert aber zumindest einen Hinweis: Den größten Anteil am Basisscore haben nach Angaben der Schufa nämlich die verschiedenen Scores der Banken.

Die abschließende Entscheidung über die Kreditvergabe oder Erlaubnis zum Rechnungskauf trifft das anfragende Unternehmen selbst, jedenfalls formal (siehe Kritik). Die meisten Unternehmenskunden reichern die Informationen und den Score

Rückzahlungswahrscheinlichkeit

Den Score drückt die Schufa auf einer prozentualen Skala von 0 bis 100 aus. Im Bereich „Hervorragend“ sollte man nahezu alle Kredite bekommen.

Hervorragend	> 97,21
Gut	97,2 – 93,53
Akzeptabel	93,52 – 85,88
Ausreichend	< 85,88
Ungenügend	Negativ-Informationen (Zahlungsstörungen)

mit eigenen Daten an. Banken verlangen von ihren Kunden meist zusätzliche Belege wie Kontoauszüge oder Vermögensnachweise. Auch die Erfahrung von Bankmitarbeitern spielt oft eine Rolle. Versandhändler wiederum kennen die Bestellhistorie ihrer Kunden. Zusätzlich liefern Warenkörbe Hinweise: Wer bei der ersten Bestellung ein teures Handy ordert, wird meist genauer geprüft.

Mängel und Kritik

Die Schufa bekommt es regelmäßig mit Daten- und Verbraucherschützern zu tun. In Gerichtsverfahren geht es vor allem um die Praxis, mit der die Schufa Daten erhebt, speichert, auswertet und weitergibt – und die Konsequenzen, die falsche Bonitätsangaben für Verbraucher haben. Denn trotz Verbesserungen hat die Schufa immer noch nicht das Transparenzniveau erreicht, das sich Verbraucher- und vor allem Datenschützer wünschen. Da sich auch die Fehlerkultur erst allmählich bessert, schlägt der Schufa nach wie vor großes Misstrauen entgegen. Zudem legt sie weiterhin nur einen Teil der Variablen offen, die in ihre Berechnungen einfließen: zum Beispiel im Score-Simulator (siehe Kasten „Der Schufa-Score-Simulator“ auf der nächsten Seite).

Auf ihrer Homepage bemüht sich die Schufa mittlerweile zwar um eine verständlichere Sprache, sie ist aber immer noch von juristischen Formulierungen durchzogen und für viele Menschen nach wie vor sehr kompliziert. Das bereitet weiterhin einen fruchtbaren Boden für Gerüchte und Mythen rund um Arbeitsweise und Einfluss der Schufa – und für Gerichtsverfahren.

Gegenstand von Klagen war beispielsweise die Formel, mit der die Schufa Scores berechnet. 2014 urteilte der BGH, dass die Schufa die genaue Scoreberechnung als Geschäftsgeheimnis nicht offenlegen muss. Allerdings verpflichtete er sie, so weit wie möglich über das Zustandekommen von Scores zu informieren. Die Daten- und Verbraucherschützer, mit denen wir sprachen, halten dies im Grundsatz für sinnvoll: Personen, die die Formel kennen, könnten ihren Score für kriminelle Zwecke manipulieren. Die Transparenz halten jedoch insbesondere Datenschützer für stark ausbaufähig.

Klagen ziehen auch regelmäßig die Menge und der Umfang der gespeicherten Daten nach sich. Unvollständige, falsche oder der falschen Person zugeordnete Schufa-Informationen können existenzgefährdend für Menschen werden, die zum Beispiel eine Wohnung suchen. Bei den anfänglich schwachen Scores von jungen Menschen wiederum ist selbst mithilfe von Selbstauskünften (siehe Kasten „Was tun bei falschen und unberechtigten Einträgen?“) nichts zu machen: Wer keine Einträge hat, kann auch keine korrigieren lassen. Eine Selbstauskunft zu beantragen, ist trotz aller Vereinfachungen überdies für viele Menschen eine Hürde.

Die Schufa schürt das Misstrauen aber auch selbst, wie etwa im „Check Now“-Skandal 2020. Unter diesem Titel wollte O2/Telefónica in Kooperation mit der Schufa auch solchen Kunden Mobilfunkverträge anbieten, deren Bonität das eigentlich nicht zuließ. Diese Kunden konnten der Schufa einen Einblick in ihr Girokonto gewähren. Die sah im Idealfall dann Umsätze wie Gehalt oder regelmäßige Zahlungen und O2 bot den Vertrag am Ende doch an. Das Verfahren an sich war durch die zweite europäische Zahlungsdiensterichtlinie (PSD2) gedeckt. Viele Datenschützer hielten die Einwilligung, die die Schufa respektive O2 von den Kunden einholte, aber nicht für informiert im Sinne von Artikel 7 der DSGVO. Das galt besonders für eine zweite Option, mit der die Kunden der Schufa erlaubten, die Daten über mehrere Monate zu speichern. Nach massiver medialer Kritik stellten O2 und Schufa das Projekt ein.

Auch aktuell sind drei Grundsatzverfahren anhängig, eines beim Bundesgerichtshof (BGH) und zwei beim Europäischen Gerichtshof (EuGH). Im ersten EuGH-Verfahren geht es um die Frage, ob die Schufa automatisierte Entscheidungen nach

Bonitätsberechnung

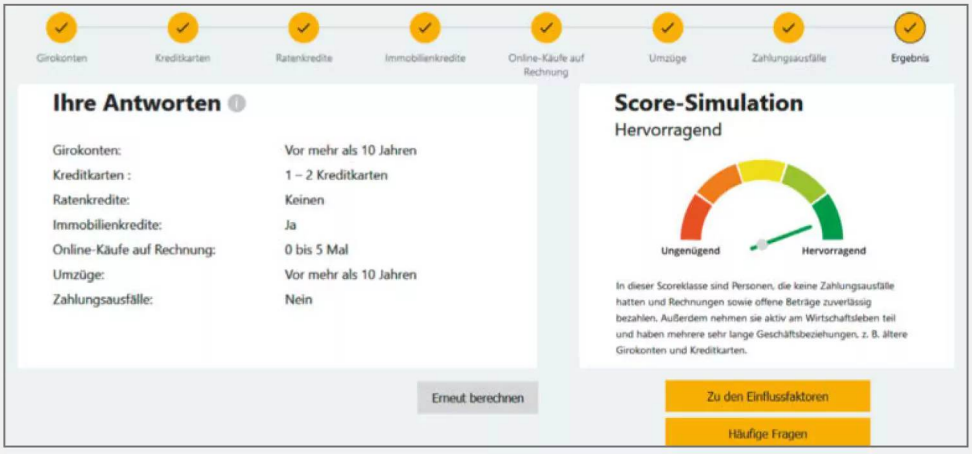
Auskunfteien kombinieren für den Bonitätsscore verschiedene Wahrscheinlichkeitswerte für einen Zahlungsausfall. Dazu ermitteln sie zunächst, wie hoch die Ausfallwahrscheinlichkeit in Vergleichsgruppen mit denselben Merkmalen in der Vergangenheit war. Das Schema ist hier vereinfacht dargestellt – tatsächlich kombinieren Auskunfteien für jede Person dutzende Merkmale und mehrere Vergleichsgruppen in einer Matrix. Die abgebildeten Werte sind daher fiktiv.

	0-2 Ratenkredite	3-5 Ratenkredite	> 5 Ratenkredite
Hauptgirokonto über 0-5 Jahre	**7,2 % Ausfall**	**8,9 % Ausfall**	**10,9 % Ausfall**
Hauptgirokonto über 5 Jahre	**3,1 % Ausfall**	**5,9 % Ausfall**	**7,9 % Ausfall**

Der Schufa-Score-Simulator

Mit einem Tool möchte die Schufa nachvollziehbar machen, wie sie individuelle Scores berechnet. Im „Score-Simulator“ – der nach ihren Angaben keine persönlichen Daten weitergibt – fragt sie dafür insgesamt sieben Kriterien für einen „Bankenscore“ ab: Wie lange man sein ältestes Girokonto führt, wie viele Kreditkarten man besitzt, wie viele Ratenkredite man derzeit bedient und ob man einen Immobilienkredit aufgenommen hat, wie oft man im zurückliegenden Jahr online auf Rechnung eingekauft hat, wie lange der letzte Umzug zurückliegt und ob man in den letzten drei Jahren Schufa-relevante Zahlungsausfälle hatte. Die einzelnen Fragen erklärt sie auf Wunsch. Nach der Auswertung – die lediglich die einzelnen Bonitätsstufen, aber keinen konkreten Score wiedergibt – erhält man weitere Informationen, was den Score wie beeinflusst.

Das Tool ist rudimentär gehalten. Allein für den Bankenscore zieht die Schufa im echten Leben 17 Kriterien heran. Sie argumentiert, dass sie die wichtigsten sieben versammelt habe. Dennoch ist die Aussagekraft begrenzt. Immerhin kann man verschiedene Variablen kombinieren und ein Gefühl dafür bekommen, wie sich Änderungen grob auf den eigenen Score auswirken.



Der Score-Simulator der Schufa vermittelt einfach und mit guten Erklärungen, wie ein Bankenscore zustande kommt. Er bildet aber nicht die Realität ab und liefert auch keinen Punktwert.

Artikel 22 DSGVO trifft oder nicht. Der Generalanwalt argumentiert, dass der Score faktisch über die Kreditvergabe entscheidet, zumal auch das nachfragende Unternehmen die Formel nicht kenne. Die Schufa hält dem entgegen, dass ihre Vertragspartner die Entscheidungen treffen. Verlöre die Schufa, und dafür spricht viel, müsste sie ihre mathematischen Verfahren wohl deutlich detaillierter erklären als bisher.

Das BGH- und das zweite EuGH-Verfahren drehen sich um Löschfristen – speziell bei Restschuldbefreiungen nach Privatinsolvenzen. In Schuldnerverzeichnissen bleiben diese sechs Monate lang öffentlich, die Schufa speichert sie drei Jahre lang. Das hielt der EuGH-Generalanwalt in seinem Antrag vom März 2023 für unzulässig. Die Schufa hat ihre Praxis bereits geändert, zumal der EuGH selbst dem Antrag wahrscheinlich folgen wird.

Ausblick

2022 verkündete die Schufa eine „Transparenzoffensive“. Sie will nach eigener Darstellung fortan nicht nur ihre Arbeitsweise besser erklären, sondern Bürgern auch niedrigschwellige Angebote machen. Dabei lege sie insbesondere die Kriterien zugrunde, die das Gutachten „Verbrauchergerechtes Scoring“ (ct.de/w2f1) des Sachverständigenrates für Verbraucherfragen beim Bundesjustizministerium fordert. Nach dem Score-Simulator, der rudimentär das Zustandekommen der Bonitätsbewertung erklärt, können Verbraucher ihren Basisscore mittlerweile kostenlos beim Dienst „Bonify“ der Schufa-Tochter Forteil einsehen. Dessen Start trübte allerdings eine Sicherheitslücke. 2024 will die Schufa mit einem eigenen Service loslegen und hat dann hoffentlich mehr Fortune. (mon) c't

Kontaktformulare, Dokumente
ct.de/w2f1

Fake Shops erkennen und Ärger vermeiden

Beim digitalen Einkauf betrügerischen Läden auf den Leim zu gehen, ist ärgerlich und teuer. Mit ein paar Grundregeln und hilfreichen Tools vermeidet man das. Wir stellen sie vor und erklären, was im Schadensfall noch möglich ist.

Von **Nick Akinci**

Bild: Orapun - stock.adobe.com

Über vier Millionen Deutsche sind schon einmal auf einen Fake Shop hereingefallen. Das schätzt das von der Bundesregierung geförderte Marktbeobachtungsinstitut „Marktwächter digitale Welt“. Besonders häufig bieten solche Shops nach Angaben des Instituts Sportartikel, Elektronik sowie Haushaltsartikel, Bekleidung und Fahrräder, aber auch Brillen und Schmuck.

Wir zeigen, wie Sie Ihnen unbekannte Shops anhand verlässlicher Kriterien und mit hilfreichen Tools auf Seriosität prüfen, wie Sie Zahlungen absichern und was Sie im Schadensfall tun können.

Was ist ein Fake Shop?

Fake Shops sind Online-Shops, mit denen Kriminelle Kunden ihr Geld abnehmen wollen, ohne ihnen die versprochene Ware zu liefern. In der einfachsten Variante erhalten Kunden überhaupt keine Ware. Etwas perfidere Betrüger versenden leere Kartons. Im Nachhinein behaupten sie, dass die Ware auf dem Versandweg abhandengekommen sein müsse. Mitunter verschicken sie auch Ware, die in keiner Weise der Produktbeschreibung entspricht.

Viele Fake Shops sind nur für einen relativ kurzen Zeitraum online, da sie fast immer auffliegen und der Hoster sie im besten Fall vom Netz nimmt. In diesem Zeitfenster versuchen die Betrüger, möglichst viel Geld zu ergaunern. Sitzt der Hoster im Ausland, können sich solche Shops auch über Jahre halten.

Prüfender Blick

Fake Shops sind häufig nicht auf den ersten Blick als solche zu erkennen. In Zeiten von Baukastensystemen wie Shopify & Co. klicken Betrüger professionell aussehende Online-Shops in wenigen Stunden zusammen. Es gibt jedoch eine Reihe von Indizien, die für einen Fake Shop sprechen.

Um Kunden anzulocken, bieten die Täter die Ware in Fake Shops oft deutlich günstiger an als in anderen Online-Shops. Insbesondere beliebte und häufig gehandelte Markenware preisen sie unter dem Marktwert an. Schnäppchenjäger schauen auf Preisvergleichsseiten, ob der Preis realistisch ist (siehe Artikel „Onlinekauf-Checkliste Preisvergleich“ auf S. 10).

Als Nächstes schaut man in das Impressum. Fake Shops haben oft keines, obwohl dies in Deutschland gesetzliche Pflicht ist – die Betrüger wollen ihre Identität verschleiern. Aber Achtung: Manche Fake Shops enthalten ein echt aussehendes Impressum, welches jedoch schlicht falsche, unvollständige oder von anderen Websites kopierte Angaben enthält. Ein erstes Indiz, ob die Firma an der angegebenen Adresse sitzt, liefert Google Maps. Den Unternehmensnamen und die zugehörige Handelsregisternummer prüft man auf handelsregister.de [1].

Abgesehen vom Impressum fehlen in vielen Fake Shops auch Telefonnummern oder E-Mail-Adressen, um Kontakt aufzunehmen. Ebenfalls kein gutes Zeichen ist es, wenn sich Kontaktmöglichkeiten beschränken auf ausschließlich Handy- oder kostenpflichtige Nummern, Postfachadressen oder lediglich ein Kontaktformular. Misstrauen ist geboten, wenn AGB und Datenschutzerklärung sowie Widerrufsbelehrungen und Versandbedingungen fehlen.

Gütesiegel sind ein Hinweis auf vertrauenswürdige Shops, doch in Fake Shops trifft man immer wieder einfach hineinkopierte oder frei erfundene Varianten an. Letztere ähneln teils bekannten Gütesiegeln – wie etwa dem von Trusted Shops.

Verfügt der Online-Shop über ein Gütesiegel, kann man auf der Homepage der Organisation prüfen, ob es sich um ein tatsächlich anerkanntes Gütesiegel handelt und ob der Online-Shop es rechtmäßig erworben hat. Durch einen Klick auf das Siegelsymbol muss man auf die Seite der dahinterstehenden Organisation gelangen. Verbreitet und vertrauenswürdig ist außer Trusted Shops auch das EHI Retail Institute („Geprüfter Online-Shop“). Als zuverlässig gilt außerdem das in Kopenhagen ansässige Bewertungsportal Trustpilot (alle unter ct.de/wmq8).

Zahlmethoden

Als Zahlart bieten viele Fake Shops ausschließlich Vorkasse per Banküberweisung an, da man solche Zahlungen in der Regel nicht rückgängig machen kann. Mitunter wollen betrügerische Händler Kunden auch gerne zu PayPal-Zahlungen in der Variante „Freunde und Familie“ verleiten. Die beinhaltet aber keinen Käuferschutz (siehe Artikel „Onlinekauf-Checkliste Shop-Auswahl“ auf S. 14 und „PayPal-Schutz bei Privatgeschäften“ auf S. 76). Manchmal bietet der Fake Shop auch zum Schein weitere Zahlarten an, um Vertrauen zu schaffen. Die funktionieren dann aber aus vorgeschobenen Gründen nicht.

Auch bei vermeintlich sicheren Bezahlmethoden gibt es Haken. Der PayPal-Käuferschutz ist abgesehen von der Zahlung für „Waren und Dienstleistungen“ an Bedingungen wie Paketversand mit elektronischer Sendungsverfolgung geknüpft. Ähnlich halten es Amazon oder Klarna. Manche Betreiber

Der Fakeshop-Finder der Verbraucherzentralen überprüft Shop-Websites. Die rote Ampel markiert nahezu sicher einen Fake Shop.

von Fake Shops schicken die Pakete daher an Adressen von Strohleuten, um Kunden über die Sendungsverfolgung erst in Sicherheit zu wiegen und anschließend Käuferschutzverfahren zu erschweren. Mehr zu Vor- und Nachteilen von Zahlarten haben wir im Artikel „Onlinekauf-Checkliste Bezahlmethoden“ auf S. 24 zusammengetragen.

Blacklists und Prüftools

Bleibt man unsicher, helfen Tools von Verbraucherschützern und anderen Organisationen. Zunächst lohnt sich ein Blick auf Blacklists. Hierbei handelt es sich um Listen von Online-Shops, die bereits als Fake Shops eingestuft oder die mehrfach als solche gemeldet worden sind. Solche Listen finden sich zum Beispiel auf der Website der Verbraucherzentrale Hamburg, der Präsenz des Siegel-Anbieters Trusted Shops oder auf der Watchlist Internet. Der Fake-Shop-Kalender der Verbraucherzentrale Bundesverband macht zusätzlich auf zeitweise besonders häufig betroffene Branchen aufmerksam (alle Seiten unter ct.de/wmq8). Darüber hinaus kann sich der Besuch der Preisvergleichsseiten Geizhals und Idealo lohnen (Hinweis: Geizhals gehört wie c’t zu Heise Medien). Sie listen nur geprüfte Online-Shops sowie Händler auf Marktplätzen mit starkem Käuferschutz. Mehr zu den Eigenheiten von Marktplätzen wie Amazon und eBay finden Sie im Artikel „Onlinekauf-Checkliste Shop-Auswahl“ auf S. 14.

Hilfreich bei der Recherche ist außerdem der Fakeshop-Finder der Verbraucherzentralen. Dort gibt man die URL des zu prüfenden Online-Shops in eine Eingabemaske ein. Anschließend ordnet das Tool ihn nach einem Ampelsystem einer Kategorie zu. Zeigt die Ampel Rot, so ist der betreffende Shop bereits als Fake Shop aufgefallen. Bei gelber Ampelfarbe hat die automatische Prüfung allgemeine Indizien für betrügerische Absichten, aber auch Indizien für seriöses Gebaren gefunden und listet sie samt Erklärung auf. Entdeckt die Prüfroutine beispielsweise kein Impressum, kann das auch heißen, dass der Betreiber des Shops es lediglich für automatisierte Abfragen gesperrt hat. Das muss man dann selbst nachsehen. Die Einstufung „Grün“ bedeutet, dass der Shop den Verbraucherzentralen „bisher nicht negativ aufgefallen“ ist; man soll aber trotzdem auf eine sichere Zahlungsmethode und die Rücksendekonditionen achten.

Schäden begrenzen, Shops melden

Ist das Kind bereits in den Brunnen gefallen, hat man im besten Fall eine sichere Zahlungsmethode verwendet und veranlasst über seine Bank oder den Zahlungsdienstleister eine Rückerstattung. Bei einer Banküberweisung wird es hingegen schwierig. Meldet man sich sofort bei seiner Bank, kann diese die Überweisung manchmal noch stoppen.

In jedem Fall sollte man Strafanzeige bei der Polizei oder Staatsanwaltschaft erstatten. Dies geht heutzutage unkompliziert über die „Onlinewache“ (ct.de/wmq8). Zusätzlich kann man einen Rechtsanwalt damit beauftragen, den Rückzahlungsanspruch auf zivilrechtlicher Ebene durchzusetzen. Der Anwalt beantragt Einsicht in die Ermittlungsakte der Strafverfolgungsbehörden und findet im besten Fall die Identität des Betrügers heraus.

Wer einen Fake Shop erkannt hat oder darauf hereingefallen ist, kann dazu beitragen, dass der Shop aus dem Internet verschwindet. Hat man als Betroffener Strafanzeige erstattet, kümmern sich meist Polizei und Staatsanwaltschaft darum, dass der Hoster den Shop abschaltet. Ansonsten meldet man den Fake Shop dem Hoster oder Shopsystemanbieter sowie den Verbraucherzentralen, zum Beispiel über das Onlineformular der Verbraucherzentrale Hamburg (ct.de/wmq8). (mon) c't

Literatur

[1] Jo Bager, Gefährliche Offenheit, Online-Handelsregister lädt zum Datenmissbrauch ein, c’t 24/2022, S. 134

Nützliche Websites

ct.de/wmq8

Neue Masche beim Kartenbetrug

Mit einem neuen Trick gelingt es Kriminellen, die Kredit- oder Debitkarte ihres Opfers in Apple Pay oder Google Pay zu missbrauchen – mithilfe eines digitalen Abbilds.

Von **Markus Montz**

Das Landeskriminalamt (LKA) Niedersachsen warnt weiterhin vor einer Betrugsmasche, mit der Kriminelle Kredit- und Debitkartenbesitzer übers Ohr hauen. Das Schema funktioniert mit Visa, Mastercard und American Express ebenso wie mit der Girocard. Die Täter verleiten das Opfer dazu, ihnen Daten zu übermitteln und die Karte für ihre Smartphones freizuschalten. Mit Apple Pay oder Google Pay können die Täter dann die Karte oder das Konto des Betroffenen leerräumen.

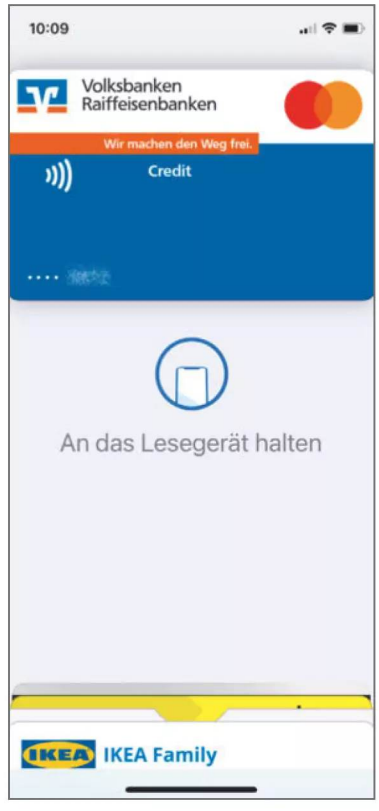
Ausgangspunkt ist in aller Regel eine Phishing-Mail, die vermeintlich von der eigenen Bank oder Sparkasse stammt. Die Mail fordert das Opfer dazu auf, die Kartendaten auf der Homepage des Kreditinstituts aus einem vorgeschobenen Grund zu bestätigen, zu verifizieren oder zu aktualisieren – beispielsweise wegen eines Missbrauchs der Karte, technischen Schwierigkeiten oder einer neuen Rechtslage. Mitunter zeigen auch Suchmaschinen oder andere Webseiten solche Aufforderungen. Ein Link führt das Opfer direkt auf eine präparierte, scheinbar offizielle Internetseite seines Finanzinstituts. Dort soll es die Kartendaten einschließlich Ablaufdatum sowie seine Telefonnummer eingeben.

Kommt das Opfer dem nach, ruft innerhalb kurzer Zeit einer der Täter an und gibt sich als Bankmitarbeiter aus. Während des Gesprächs fordert er dazu auf, eine Push-Nachricht der Bank auf dem Smartphone zu bestätigen, eine TAN einzugeben oder ihm eine TAN zu nennen. Damit gibt das Opfer den digitalen Platzhalter der Karte auf dem Smartphone der Täter frei. Diese können damit nun ohne die PIN der echten Karte nach Belieben einkaufen oder Geld abheben.

Der Rat von LKA und c't: Weder Banken und Sparkassen noch andere Stellen wie Polizei oder Behörden verschicken Mails, in denen sie Kunden respektive Bürger dazu auffordern, Kartendaten zu bestätigen. Daher sollte man niemals darauf eingehen und auf keinen Fall auf Links in solchen Mails klicken. Bei einem tatsächlichen Missbrauchsverdacht sperren die Geldhäuser die Karte. Nach einer Sperre setzen sie sich mit den Betroffenen in Verbindung, per Brief, telefonisch oder im Onlinebanking-Postfach. Ähnliches gilt bei technischen oder rechtlichen Problemen.

Echte Bankmitarbeiter werden dabei aber nie Passwörter oder PINs abfragen oder eine Push-Bestätigung oder TAN anfordern – auch nicht über SMS, WhatsApp oder Mail. Generell sollte man sorgfältig den Verwendungszweck prüfen, bevor man eine Zahlung oder Aktion mit seiner Karte per Push-Nachricht oder TAN freigibt. Ruft jemand an und das Telefon zeigt die Nummer der Bank an, ist das außerdem keine Echtheitsgarantie, denn Telefonnummern kann man leicht fälschen.

Da die Opfer die Karte selbst freigeschaltet haben, können sie nicht auf Kulanz des Kreditinstituts hoffen. Bemerken sie unberechtigte Abbuchungen, zum Beispiel auf der Kartenabrechnung oder im Onlinebanking, müssen sie die Karte so schnell wie möglich sperren und sollten Anzeige bei der Polizei erstatten. (mon) *c't*



Bei dem neuen Betrugsschema erbeuten die Täter Kartendaten über Phishing und verleiten das Opfer anschließend dazu, ihnen die Karte dauerhaft für Apple Pay oder Google Pay freizugeben.

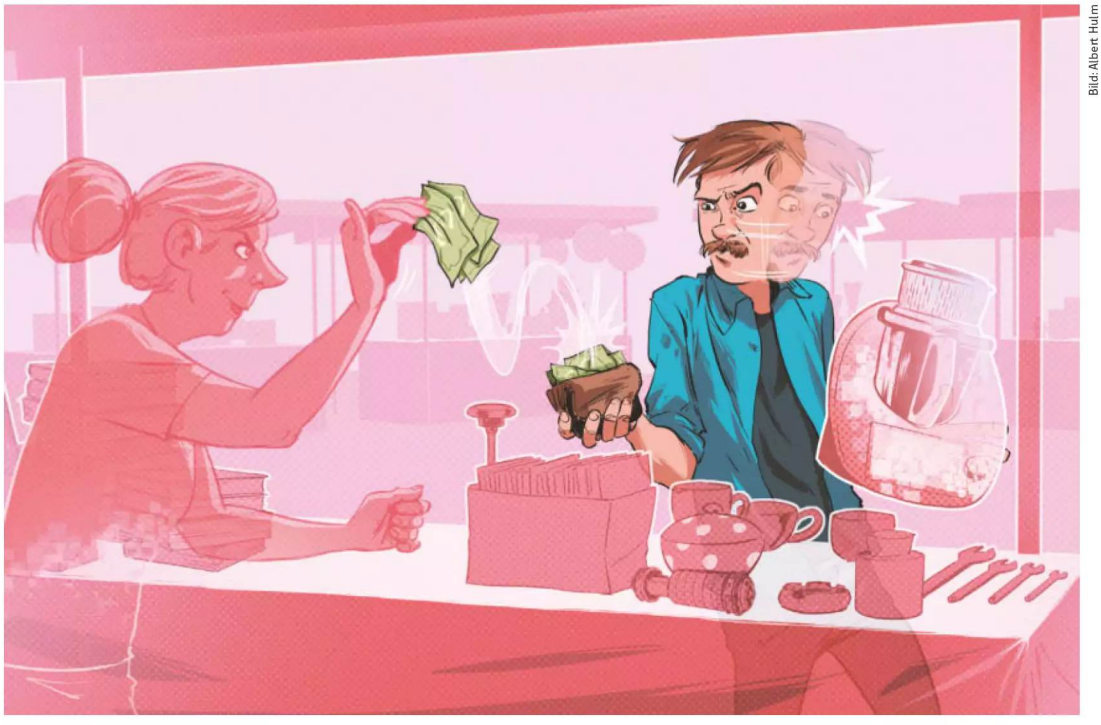


Bild: Albert Hulm

Theaterspiel mit Betrugsabsicht

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: „Selbst schuld“ war keines der Opfer. Im Gegenteil hatten alle auf grundsätzliche Unstimmigkeiten geachtet. Sie tappten vielmehr in Fallen, die nicht auf den ersten Blick erkennbar waren. Wir zeigen, wie Sie diese erkennen, und geben Tipps, wie Sie die Täter ins Leere laufen lassen.

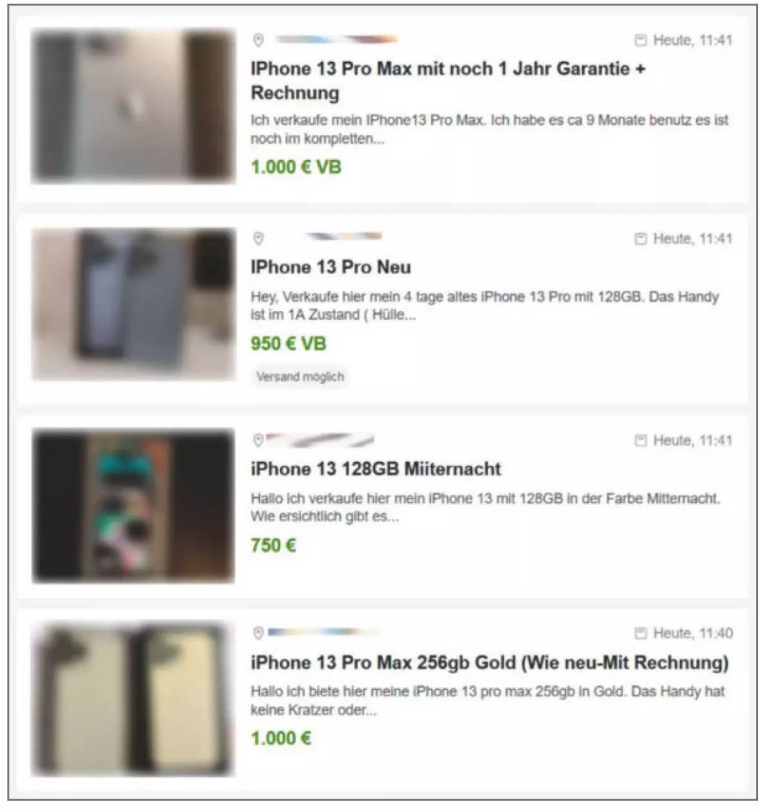
Seriös wirkende Angebote

Klaus G. suchte auf dem Portal 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 eine neue Küche bestellt, sich aber aus Geschmacksgründen doch für ein anderes Modell entschieden. Interessenten könnten die Maschine abholen, Rechnung und Garantie lägen vor. Klaus G. 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 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 ei-



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

nigte 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 sich daraufhin 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 Kleinanzeigen (siehe Artikel „‚Sicher bezahlen‘ bei Kleinanzeigen“ auf S. 102) 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. Doch die Täter hatten dessen Daten einfach an anderer Stelle kopiert und 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 ebenfalls 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 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.

Kein Einzelfall

Klaus G. recherchierte weiter. Über die im Impressum angegebene Adresse erreichte er schließlich die echte Nina P. Sie zählte ebenfalls zu den Geschädig-

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 [1]. Auch dann haben Sie mitunter Möglichkeiten, Teile des Dokuments zu schwärzen.

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.

ten: 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. Nina P. hatte deshalb bereits Anzeige erstattet.

Allein der c't bekannte Schaden beträgt zwischen 15.000 und 20.000 Euro. Nur wenige Geschädigte hatten Glück und bekamen ihr Geld zurück. Die gefakte Website, die ausweislich der Nameserver-Angaben beim Website-Dienstleister Jimdo gehostet war, lässt sich nicht mehr aufrufen. 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.

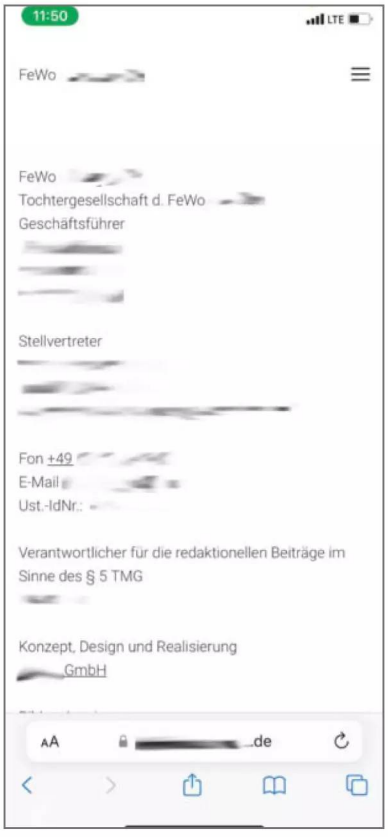
Köder und falsche Nummern

Den Ausgangspunkt bildeten in diesem und allen anderen Fällen Nutzerkonten auf Kleinanzeigen, die die Täter entweder gekapert oder unter falscher Identität eröffnet haben. Die Täter bieten dort meist schwer erhältliche, höherpreisige oder aber besonders begehrte 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 das gesuchte iPhone prüfte („neun von zehn waren Fake"), hat uns nicht überrascht. Lassen Sie daher besonders bei höherwertigen oder stark nachgefragten 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 mehr.

Im zweiten Schritt erfragen die Täter eine Mobilfunknummer, um die Interessenten vom Portal herunter zu locken. Manche Portale ermöglichen auch, diese im Profil zu hinterlegen und automatisch in eine Anzeige oder Anfrage einzubinden. Davon raten wir dringend ab; Kleinanzeigen hat diese Möglichkeit aus gutem Grund abgeschafft. Findet die Kommunikation abseits der Plattform statt, hebelt dies die Schutzmechanismen aus, die beispielsweise 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 im Artikel "Telefonbetrug trotz zweitem Faktor" auf S. 116). 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 Messengernach-



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

richten 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 „Keine Ausweiskopien verschicken" auf S. 98). 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 (siehe Artikel „PayPal-Betrug auf Kleinanzeigenportalen“ auf S. 108). 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. Die nutzen sie dann für die nächsten Betrugsversuche.

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.

Abgezockt

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 Kleinanzeigen, PayPal oder auch Kreditkarte nicht möglich sei (siehe die Artikel „‚Sicher bezahlen‘ bei Kleinanzeigen“ ab S. 102, „PayPal-Schutz bei Privatgeschäften“ ab S. 76 und „Kartenabbuchungen rückabwickeln“ ab S. 72). 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 – oft haben ahnungslose Strohleute die Konten eröffnet und den Tätern die Zugangsdaten überlassen [2]. 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 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 (siehe Artikel „PayPal-Schutz bei Privatgeschäften“ auf S. 76). 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. Als Echtheitsbeweis sollte sie einen Löffel daneben legen. Als die Täterin nach Ausflüchten suchte, brach Nina P. die Verbindung ab.

Geschädigt – 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/ws7u) finden. Jimdo versicherte uns auf Nachfrage, entsprechende 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) c't

Literatur

[1] Joerg Heidrich, Datensparsam ausweisen, Was Sie beachten sollten, bevor Sie eine Perso-Kopie weitergeben, c't 4/2023, S. 174

[2] Markus Montz, Vom Bankentester zum Geldwäscher, Wie Cyberkriminelle arglose Jobsucher rekrutieren, c't 3/2023, S. 126

DENIC-Whois
ct.de/ws7u

Bild: Albert Hulm

„Sicher bezahlen“ bei Kleinanzeigen

Die Bezahlfunktion „Sicher bezahlen“ der Verkaufsplattform Kleinanzeigen soll für mehr Sicherheit und Vertrauen sorgen. Doch Betrüger locken Nutzer auf gefälschte Webseiten und zocken sie dort ab. Wir erklären, wie Sie sich gegen die Masche wappnen.

Von **Markus Montz**

Stellen Sie sich vor, Sie wollen einen teuren Kopfhörer oder Konzertkarten über Kleinanzeigen (das frühere „eBay Kleinanzeigen“) verkaufen. Am Ende haben Betrüger Sie stattdessen um mehrere tausend Euro erleichtert, ohne dass der Kopfhörer oder die Tickets jemals den Besitzer gewechselt hätten. Nicht vorstellbar? Beim SMS- oder Messenger-Phishing passiert genau das.

Mit gefälschten Benachrichtigungen locken die Täter ihre Opfer auf Fake-Websites und hebeln sogar

die bei Kreditkartenzahlungen obligatorische Zwei-Faktor-Authentifizierung aus. Das Perfide dabei: Die Betrüger haben Ihnen erfolgreich vorgegaukelt, dass Sie einen besonders sicheren Zahlungsmodus über ein Treuhandkonto nutzen, den Kleinanzeigen unter dem Namen „Sicher bezahlen“ anbietet. Allerdings ist dieser zu keiner Zeit im Spiel gewesen.

Unser Artikel stellt Ihnen diese Phishing-Methode am Beispiel von Kleinanzeigen vor und klärt zugleich darüber auf, wie „Sicher bezahlen“ tatsächlich funktioniert. Außerdem werfen wir einen Seitenblick auf weitere aktuelle Betrugsmaschen auf Kleinanzeigenportalen.

Nachrichten-Phishing

Ein Phishing-Angriff über SMS oder WhatsApp auf Kleinanzeigen beginnt stets damit, dass Sie einen zumeist höherpreisigen, stark nachgefragten oder zeitkritischen Gegenstand wie eine Kamera, ein Smartphone oder Tickets für ein baldiges Konzert auf Kleinanzeigen einstellen. Ein vermeintlicher Interessent meldet sich daraufhin über die Nachrichtenfunktion von Kleinanzeigen bei Ihnen und fragt an, ob Ihr Angebot noch zu haben sei – oft auch schlicht „das Produkt“. Schon bei solchen unspezifischen Anfragen, womöglich noch ohne Namensnennung und in schlecht übersetztem Deutsch, ist Misstrauen angebracht.

Bereits an dieser Stelle abbrechen sollten Sie, wenn schon die erste Anfrage über SMS, WhatsApp oder eventuell per Mail kommt, ohne dass Sie Ihre Telefonnummer oder Mailadresse jemals im Chat mitgeteilt haben. Dann kann die Gegenseite Ihre Kontaktdaten nur auf zweifelhaften Wegen erhalten haben. Daraus folgt außerdem: Geben Sie sensible Daten wie Telefonnummern oder Mailadressen nicht leichtfertig preis.

Falls Sie auf die Anfrage reagieren und sich mit dem vermeintlichen Käufer handelseinig werden, schlägt dieser vor, die Treuhand-Bezahlfunktion „Sicher bezahlen“ von Kleinanzeigen zu nutzen (siehe Kasten „So funktioniert „Sicher bezahlen“ auf Kleinanzeigen“ auf S. 104). Daraufhin folgt innerhalb kurzer Zeit eine weitere Nachricht: Der Betrüger schreibt Ihnen, dass es Probleme gäbe und er beispielsweise den Bezahlvorgang nicht habe abschließen können. Spätestens jetzt müssen Ihre Alarmglocken schrillen.

Kurz darauf nämlich erhalten Sie eine SMS oder WhatsApp-Nachricht (oder eventuell eine Mail). Diese stammt vorgeblich von Kleinanzeigen oder von dessen Zahlungsdienstleister OPP. Die angezeigte Rufnummer ist jedoch technisch manipuliert, das sogenannte Caller ID Spoofing. Mails haben analog einen falschen Absender. Auch diese Nachricht macht Sie auf ein angebliches Problem bei der Zahlung aufmerksam. Oft gaukelt der Inhalt Ihnen vor, dass Sie sich für „Sicher bezahlen“ noch freischalten müssen – dabei setzen die Täter darauf, dass Sie die Funktion bislang nicht kennen und sich unter Zeitdruck wähnen.

Ob einfaches Zahlungsproblem oder Freischaltung, in allen Fällen fordert die Nachricht Sie auf, auf einen Link zu klicken und Ihre Kreditkartendaten oder Zugangsdaten für das Onlinebanking einzugeben (Phishing). Die URL des Links ist so gewählt, dass Sie erst bei genauerem Hinsehen oder auf Handys nach genauer Prüfung erkennen, dass Sie auf eine Phishing-Seite gelangen. Bei eventuellen Mailanhängen müssen Sie zudem mit Schadcode rechnen.

Bild: Landeskriminalamt Niedersachsen

Mit Vorschlägen zur Bezahlweise versuchen Betrüger, Nutzer von Kleinanzeigen auf Phishing-Seiten zu ziehen.

So funktioniert „Sicher bezahlen“ auf Kleinanzeigen

Normalerweise können sich Verkäufer und Käufer auf Kleinanzeigenplattformen nicht vertrauen. Um das Risiko eines Betrugs zu reduzieren, nutzen beide Parteien häufig PayPal, wenn der Verkäufer etwas verschickt, und Barzahlung, wenn der Käufer etwas vor Ort abholt.

Bargeld bei persönlicher Übergabe ist übrigens aus Käufer- wie Verkäufersicht die sicherste Bezahlmethode: Der Käufer kann die Ware in Ruhe prüfen, der Verkäufer bekommt direkt sein Geld.

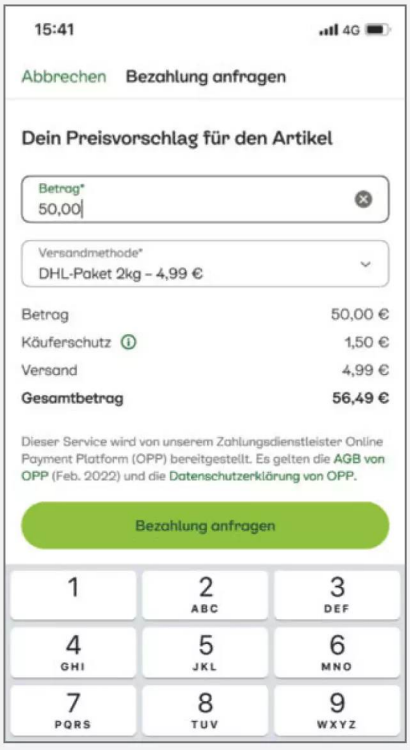
PayPal kann durch den Käufer- und Verkäuferschutz für mehr Sicherheit sorgen. Allerdings muss man die Bedingungen und Ausnahmen dabei kennen (mehr dazu in den Artikeln „PayPal-Schutz bei Privatgeschäften“ ab S. 76 und „PayPal-Betrug auf Kleinanzeigenportalen“ ab S. 108).

Mit „Sicher bezahlen“ bietet Kleinanzeigen für viele Produktkategorien eine eigene Treuhänderfunktion für Zahlungen bis 2000 Euro an. Sie gilt ausschließlich für materielle Waren, die per Paket versandt werden. So will Kleinanzeigen verhindern, dass eine Seite die Ware respektive das Geld unterschlägt. Dazu kooperiert das Unternehmen mit dem niederländischen Zahlungsdienstleister OPP (Online Payment Platform). Dieser wird von den dortigen Behörden nach denselben EU-Vorgaben kontrolliert, die auch in Deutschland gelten.

Als Grundvoraussetzung für die Nutzung von „Sicher bezahlen“ muss sich der Verkäufer vorab über „Einstellungen/Zahlungen“ in seinem Kleinanzeigen-Nutzerkonto bei OPP registrieren. Dort erhält er dann zusätzlich ein eigenes OPP-Nutzerkonto, um Zahlungen zu verwalten.

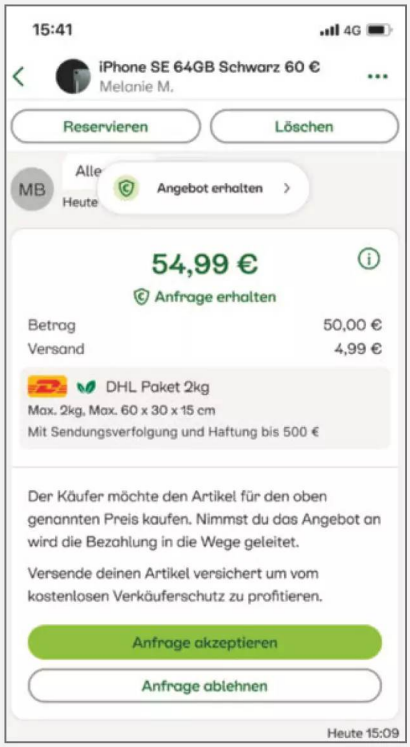
Der Käufer startet „Sicher bezahlen“ über eine der Schaltflächen unterhalb des Chats.

Will der Käufer nun dem Verkäufer über „Sicher bezahlen“ sein Geld zukommen lassen, klickt er wahlweise auf „Direkt kaufen“ oder „Angebot machen“ im Chat auf Kleinanzeigen. Anschließend gibt er den verhandelten Preis oder ein Angebot ein und fragt die Bezahlung an. Hat der Verkäufer den Preis bestätigt, gibt der Käufer eine verbindliche Rechnungs- und Versandadresse an und zahlt per SEPA-Überweisung, Kreditkarte oder Klarna-Sofortüberweisung. Anschließend wandert das Geld auf ein Treuhandkonto von OPP.

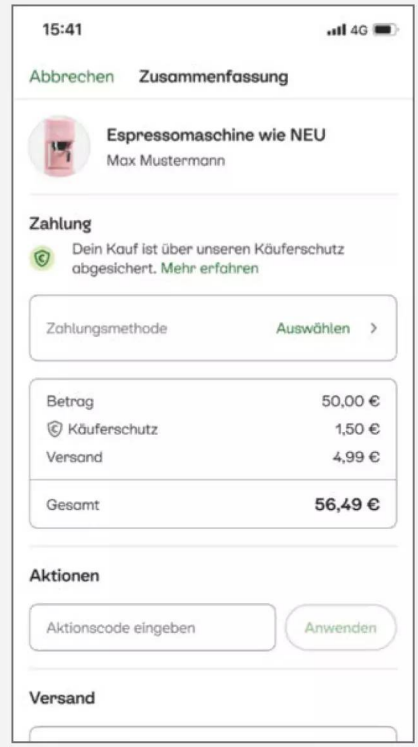


Bei „Angebot machen“ gibt er einen Vorschlag ein, den der Verkäufer im Rahmen des Chats erhält.

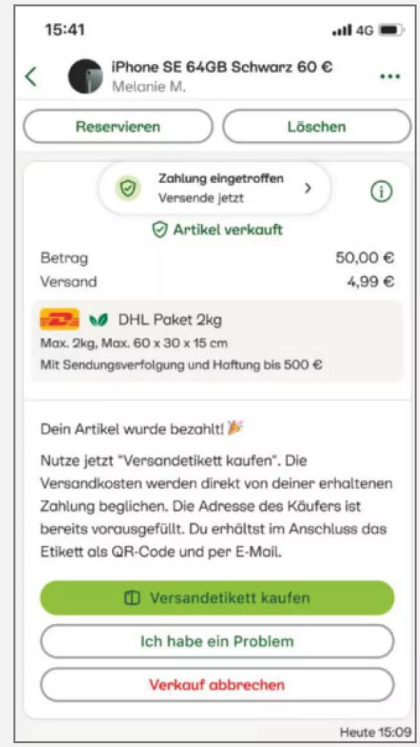
Ist es dort angekommen, erhält der Verkäufer die Nachricht, dass er die Ware verschicken kann. Ein Paket mit Sendungsverfolgung und Versicherung ist Pflicht, zum Beispiel ein DHL-Standardpaket, dessen Inhalt bei Verlust bis 500 Euro abgedeckt ist. Andernfalls – insbesondere bei persönlicher Übergabe – erlischt der Verkäuferschutz. Der Käufer bestätigt auf dem Portal schließlich den Empfang und OPP überweist das Geld auf ein Girokonto, das der Verkäufer spätestens beim ersten Geldempfang angeben muss. Gibt es Unstimmigkeiten, können beide Seiten ein Käufer-



Der Verkäufer bekommt nun eine Anfrage, ob er das Angebot akzeptiert.



Nach der Einigung erhält der Käufer eine Übersicht und wählt Bezahlart und Adresse.



Zum Schluss willigt der Verkäufer ein und Kleinanzeigen fordert ihn zum Versand auf.

oder Verkäuferschutzverfahren einleiten. Bestätigt der Käufer den Paketempfang nicht, bekommt er automatisch nach 14 Tagen sein Geld zurück. War er unehrlich, muss er aber mit Schwierigkeiten bis hin zu einer Anzeige wegen Betrugs oder Unterschlagung rechnen.

Allerdings ist dieser Service für den Käufer nicht kostenlos. Er zahlt eine Provision in Höhe von 35 Cent plus 4,5 Prozent des Verkaufspreises an OPP. Das ist happig, dafür sinkt das Betrugsrisiko drastisch. Außerdem kann man mit vielen Verkäufern vorab eine Kostenteilung oder einen Preisnachlass vereinbaren, schließlich haben ja beide Seiten etwas davon. Etwas misslich ist, dass Kleinanzeigen die Preise und Bedingungen nicht gut sichtbar im Vorfeld des Kauf- und Verkaufsprozesses anzeigt: Man lernt sie entweder im Hilfebereich oder erst während des Bezahlvorgangs kennen.

Beide Seiten sollten sich im Vorfeld in Ruhe über den Ablauf und alle (!) Bedingungen informieren und Verkäufer ihre Bankverbindung unabhängig von einem laufenden Verkaufsprozess hinterlegen. Neben der Bankverbindung fordert OPP als Nachweis auch ein Foto der zugehörigen Girocard oder eines Kontoauszuges. Ab 250 Euro Verkaufswert (auch kumuliert) muss man zusätzlich eine vollständige Personalausweiskopie ohne Schwärzungen hinterlegen. Damit kommt OPP zwar den niederländischen Regeln für die Geldwäscheprävention nach, doch auch das sollten Nutzer idealerweise schon im Vorfeld erfahren.

Für mehr Details inklusive weiterer Screenshots haben Kleinanzeigen und OPP Hilfeseiten eingerichtet, die wir unter ct.de/wued verlinkt haben.

Öffnen Sie also weder Links noch Anhänge und brechen Sie spätestens mit Erhalt solch einer Nachricht den Kontakt ab. Die Grundregel lautet: Weder Banken noch Zahlungsdienstleister klären Zahlungsmodalitäten, indem sie Links oder Mailanhänge verschicken, also auch Kleinanzeigen und OPP nicht. Denkbar ist maximal der Hinweis, dass es neue Nachrichten im Postfach gibt. Ob solch eine Nachricht echt ist, prüfen Sie direkt im Nutzerkonto. Rufen Sie dazu selbst durch Eingabe der URL oder über ein eigenes Bookmark die Website von Kleinanzeigen auf und loggen Sie sich ein. Existiert dort keine passende Nachricht, können Sie getrost von einem Phishing-Versuch ausgehen.

Schutzmechanismen ausgehebelt

Haben Sie die bisherigen Warnzeichen nicht erkannt und klicken auf den Link der Betrüger, landen Sie auf einer Fake-Webseite, die wie ein offizielles Formular von Kleinanzeigen, OPP oder Ihrer Bank aussieht. Dort sollen Sie Ihre Kreditkartendaten (Name, Nummer und Ablaufdatum) inklusive der Kontrollnummer eingeben, also CVC oder CVV. Andere Fake-Websites fordern Sie im Stil Ihrer Bank auf, Ihre Onlinebanking-Zugangsdaten einzugeben. Parallel öffnet sich meist ein Livechat-Fenster, in dem der „Support“ Ihnen angeblich den verwirrenden Prozess erklärt. Tatsächlich will er Sie aber nur ablenken und zu Fehlentscheidungen verleiten, indem er für alle Ungereimtheiten Gründe erfindet.

Es folgt in der Regel die Zwei-Faktor-Authentifizierung. Zielen die Täter auf Ihre Kreditkarte, nennt sie sich auch 3-D Secure oder je nach Karte „Visa Secure“, „Mastercard Secure Code“ oder „American Express SafeKey“. Dabei zeigt Ihnen die zugehörige App auf dem Handy oder das Onlinebanking gewöhnlich einen Zahlungsbetrag und einen Empfänger an, obwohl Sie ja eigentlich nur die „Daten bestätigen“ sollen. Der Empfänger heißt zudem seltsamerweise nicht Kleinanzeigen oder OPP, sondern er trägt einen mehr oder weniger erkennbar anderen Namen oder fehlt ganz. Der Livechat erklärt Ihnen allerdings scheinbar plausibel, warum alles seine Richtigkeit habe.

Geschenk- und Geldbotendienst-Trick

Das Landeskriminalamt Niedersachsen warnt vor zwei weiteren, relativ stark verbreiteten Maschen, mit denen Verkäufer übers Ohr gehauen werden.

Beim Geldbotendienst-Trick teilt der vorgebliche Käufer dem Verkäufer mit, dass er einen Kurierdienst wie FedEx oder UPS (eventuell auch andere, etwa DHL) mit dem vereinbarten Betrag zu dessen Adresse schicken werde. Er könne das Geld prüfen und dem Boten die Ware mitgeben. Anschließend schicken die Täter eine Fake-Mail im Namen des Dienstes, die eine „Vorleistung“ beispielsweise in Form von Guthabenkarten-Codes von Steam oder Amazon verlangt. Der Käufer versichert, dass der Bote die Differenz mitbringe. Teilt man dem „Kurierdienst“ die Codes mit, ist man das dafür gezahlte Geld in aller Regel los – und der Kurierdienst taucht nie auf.

Guthabenkarten spielen auch beim Geschenktrick eine Rolle: Der angeblich aus dem Ausland stammende Kaufinteressent bittet den Verkäufer, die oft lediglich mit Allgemeinplätzen bezeichnete Ware als Geschenk an einen Freund oder Verwandten zu schicken. Als „Überraschung“ solle man eine Guthabenkarte mitschicken, für die der Fake-Käufer selbstredend bezahlen will. Egal, wie die Betrüger den Trick im Detail aufziehen: Im besten Fall ist nur der Kartencode weg, im schlechtesten auch die Ware, ohne dass man Geld dafür sieht. Gehen Sie daher auf solche Anfragen niemals ein.

Haben Sie bestätigt, gaukelt Ihnen die Seite anschließend einen Fehlversuch oder Abbruch vor und fordert Sie auf, den Vorgang zu wiederholen. Wer eine Banking-App mit Benachrichtigungsfunktion für die Kreditkarte auf dem Handy hat, erhält zwar ganz anders lautende Push-Nachrichten – darin ist von drei- oder vierstelligen Abbuchungsbeträgen die Rede. Für beides erfindet der Livechat aber Erklärungen. Dieses Spielchen treiben die Betrüger so lange, bis Sie aufgeben oder Ihnen ein Licht aufgeht.

Dann ist es allerdings zu spät, denn in Wahrheit haben die Täter mit Ihrer Karte im Hintergrund Kryptowährungen oder Waren gekauft. Die Fehlversuche gab es gar nicht, stattdessen haben Sie jedes Mal echte Abbuchungen von Ihrer Karte freigegeben. Das merken Sie im schlimmsten Fall aber erst, wenn Sie Ihre Umsatzliste kontrollieren. Das Perfide daran: Da Sie die Zahlung mittels Zwei-Faktor-Authentifizierung bestätigt haben, wird sich Ihre Bank bei einer Reklamation häufig querstellen. Sie bleiben also vermutlich auf dem Schaden sitzen.

Noch schlimmer kann es kommen, wenn Sie Ihre Onlinebanking-Zugangsdaten preisgegeben und eine Zwei-Faktor-Authentifizierung durchgewunken haben. Auf diesem Weg versuchen die Täter oft, ein eigenes Smartphone freizuschalten. Damit besitzen sie dann die volle Kontrolle über Ihr Onlinebanking und können per Echtzeitüberweisung tausende Euro stehlen, bevor entweder Sie oder Ihre Bank stutzig werden und das Konto sperren. Auch in diesem Fall müssen Sie davon ausgehen, dass Ihnen niemand den Schaden ersetzt.

Dass Ihre Kamera niemand kaufen will, bleibt nur vordergründig eine Randnotiz. Da Sie die Plattform verlassen haben, wird auch der Support von Kleinanzeigen oder OPP nichts finden, was Sie dort reklamieren könnten. Eine Restchance haben Sie nur, wenn Sie sofort Ihr zuständiges Kreditinstitut kontaktieren. Dabei geht es allerdings oft um Minuten. Selbst dann gibt es keine Gewissheit, ob das Geld nicht doch schon geflossen ist. Bei Echtzeitüberweisungen haben Sie überhaupt keine Chance mehr. So oder so sollten Sie unverzüglich die Karte und das Konto sperren lassen; bei vielen Banken geht das außerhalb der Geschäftszeiten über die bundesweite Notrufnummer 116 116.

Hilfeseiten von Kleinanzeigen und OPP

ct.de/wued

Auch Käufer betroffen

Zwar sind laut dem Landeskriminalamt Niedersachsen vor allem Verkäufer von dieser Masche betroffen. Leser haben uns aber auch berichtet, dass sie als Käufer zum Ziel geworden sind. In dieser Variante übernehmen die Täter die Rolle des Verkäufers und richten entweder selbst Fake-Nutzerkonten ein oder kapern die Nutzerkonten ahnungsloser Dritter. Als Aufhänger dienen meist vermeintliche Schnäppchen oder genau wie bei Maschen gegen Verkäufer begehrte Produkte wie Smartphones oder Karten für ausverkaufte Veranstaltungen.

Als Kaufinteressent bekommen Sie die SMS oder WhatsApp-Nachricht, mitunter auch Mail, sobald Sie auf ein Angebot eingehen und Ihre Kontaktdaten preisgegeben haben. Mitunter haben sich die Täter Ihre Telefonnummer oder Mailadresse aber auch auf anderen Kanälen besorgt. Besonders dreiste Banden schicken über die Nachrichtenfunktion von Kleinanzeigen einen vermeintlichen Bezahllink, oft als Kurzlink. Zwar sind die Links nicht klickbar, die Täter denken sich dafür aber vorgeschobene Gründe aus. Auch bei dieser Masche gaukeln die Betrüger Ihnen vor, dass dieser Sie auf „Sicher bezahlen“ leitet. Die Grundregel ist die gleiche wie bei Verkäufern: Lassen Sie sich unter keinen Umständen vom Portal weglocken und brechen Sie den Kontakt an dieser Stelle ab.

Was tun?

Die Warnungen der Polizei, Berichte über Betrugsopfer in der Tagespresse sowie Zuschriften von c’t-Lesern zeigen, dass die Masche psychologisch raffiniert eingefädelt ist – und dass die Opfer nicht unbedingt zu naiv waren, sondern die Täter sie eher auf dem falschen Fuß erwischt hatten. Deren Vorgehen zu kennen und sich insbesondere nicht von der Plattform und deren Chatfunktion locken zu lassen, bietet Ihnen zumindest einen Grundschutz. Nehmen Sie sich Zeit, informieren Sie sich über die Einrichtung und den Ablauf von „Sicher bezahlen“ und ähnlichen Schutzfunktionen und aktivieren Sie diese möglichst bereits in Ruhe, bevor Sie etwas verkaufen wollen.

Sind Sie doch auf die Masche hereingefallen, zeigen Sie die Tat auf jeden Fall bei der Polizei an. Melden Sie betrügerisch handelnde Nutzerkonten dem Plattformbetreiber, sperren Sie betroffene Kreditkarten – und bei rascher Reaktion können Sie ungewollte Zahlungen mit Glück noch bei Ihrer Bank stornieren. Ein Leser hat uns außerdem darauf aufmerksam gemacht, dass einige Hausratversicherungen Phishing-Schäden abdecken. Es kann sich also lohnen, die Bedingungen zu studieren. (mon) c't

Bild: Albert Hulm

PayPal-Betrug auf Kleinanzeigenportalen

Der Käufer- und Verkäuferschutz macht PayPal zum beliebten Zahlungsweg für Kleinanzeigengeschäfte. Nepper nutzen Besonderheiten im Kleingedruckten jedoch für Betrugsmaschen. Wir zeigen, wie Sie sich schützen.

Von **Markus Montz**

Timo S. war erstaunt: Er hatte über das Internet in Großbritannien einen Schrank aus dem 19. Jahrhundert gefunden und bestellt. Nachdem er wie vereinbart über PayPal bezahlt hatte, bekam er auch ein Möbelstück per Spedition geliefert – allerdings nicht den Schrank, der in der Anzeige beschrieben und abgebildet war. Also kontaktierte er den Verkäufer und bat um Rückabwicklung.

Der Verkäufer zeigte sich einverstanden und schlug ihm per Mail eine Spedition vor; auch eine Zieladresse schickte er mit. Timo S. beauftragte daraufhin die vorgeschlagene Spedition; wenige Tage später holte ein Fahrer den Schrank ab und hinterließ einen Abholbeleg mit der Zieladresse.

Tags darauf die nächste Überraschung: Der Verkäufer hatte ein Verkäuferschutzverfahren eingelei-

tet und darin eine andere Rücksendeadresse als jene auf dem Abholbeleg angegeben. Deshalb reichte PayPal der Abholbeleg der Spedition nicht als Nachweis für den ordnungsgemäßen Rückversand. Obwohl mehrere Kundendienstmitarbeiter S. helfen wollten, schloss PayPals System den Fall schließlich zu seinen Ungunsten. Daraufhin wandte sich S. an c't, doch auch PayPals Pressestelle konnte auf unsere Anfrage nur noch bestätigen, dass es keine Revisionsmöglichkeit mehr gebe.

Es blieb die vage Hoffnung, dass der Schrank doch noch ankommt – und siehe da, der Verkäufer bestätigte den Eingang. Er machte allerdings einen Transportschaden geltend. Immerhin bot er S. eine Rückzahlung von 1300 Pfund an. 200 Pfund plus 300 Euro Transportkosten hatte S. dennoch verloren, er akzeptierte diese Lösung aber als kleineres Übel gegenüber einem Totalverlust.

Fälle wie der von Timo S. geschehen immer wieder, insbesondere bei höherwertigen oder stark nachgefragten Artikeln. Die unseriösen Handelspartner setzen dabei darauf, dass viele PayPal-Nutzer die Bedingungen des Dienstes für den Käufer- und Verkäuferschutz nicht oder nur unzureichend kennen – in diesem Fall für den Rückversand eines Artikels, der nicht der Beschreibung entspricht (siehe Artikel „PayPal-Schutz bei Privatgeschäften“ ab S. 76 und [1]).

Dazu gehört insbesondere, dass die Rücksendung an die Adresse gehen muss, die der Verkäufer bei PayPal hinterlegt hat. Als Käufer finden Sie diese in den Transaktionsdetails; eine abweichende Adresse sollten Sie auf keinen Fall akzeptieren. Außerdem müssen Sie die Sendung möglichst elektronisch nachverfolgen können, am besten bis zur Übergabe an den Empfänger. Daher sollten Sie die Spedition für den Rücktransport anhand dieser Kriterien immer selbst bestimmen oder einen Vorschlag zumindest sorgfältig prüfen. Schauen Sie dabei genau hin: Oft haben Nepper gut gemachte Fake-Websites gar nicht existenter Speditionen erstellt.

Speditionsbetrug

Eine Variante des Falls von Timo S. richtet sich gegen Verkäufer – der „Speditionsbetrug“ oder „Schifffahrtsgesellschafts-Betrug“, vor dem weiterhin auch das Landeskriminalamt (LKA) Niedersachsen warnt. Der Ablauf: Sie stellen zum Beispiel auf Kleinanzeigen einen höherwertigen Gegenstand zum Verkauf ein. Das kann eine Uhr sein, aber auch ein Möbelstück. Rasch meldet sich ein Interessent (der Betrüger) über die Chatfunktion der Plattform bei Ihnen. Auffällig: Meist spricht er dabei nur vom „Produkt“ oder „Artikel“, geht aber nicht auf das konkrete Angebot ein – diese Nachricht ist wie alle nachfolgenden ein Textbaustein, oft mit typischen sprachlichen Merkmalen eines Übersetzungsprogramms.

Antworten Sie auf die Nachricht, wird der „Interessent“ Ihnen im nächsten Schritt eine Geschichte auftischen: Er wohne im Ausland und arbeite auf Montage, auf einer Bohrinsel oder auf einer archäologischen Ausgrabung und sei daher berufsbedingt verhindert. Er könne nicht persönlich vorbeikommen, würde den Artikel aber auch ungesehen zu Ihrem Preis kaufen. Anschließend schlägt der „Interessent“ Ihnen eine Spedition, „Reederei“ oder „Schifffahrtsgesellschaft“ vor – letztere sind etwas ungelenke automatische Übersetzungen von „shipping company“. Außerdem fordert er Bezahldaten an. Meistens will er PayPal nutzen, weil er dort gleich Ihre Mailadresse erfährt. Mit Ihren Girokontodaten funktioniert der Trick aber unter Umständen auch. Außerdem erfragt der „Interessent“ Ihre Handynummer und die Abholadresse.

Schicken Sie die Daten, folgt eine weitere Mail des „Interessenten“: Er habe Ihnen den Kaufpreis plus das Speditionsentgelt via PayPal geschickt. Allerdings sei die Zahlung blockiert worden, PayPal werde sie aber in Kürze freigeben. Außerdem habe die Spedition ihre Zahlungsmöglichkeiten überraschend auf Banküberweisung umgestellt. Daher nennt der Betrüger Ihnen eine (ausländische) Bankverbindung der Spedition und bittet Sie, die Spedition darüber zu bezahlen.

In Ihrem PayPal- oder Bankkonto werden Sie jedoch keinen Hinweis auf eine geblockte Zahlung finden. Allerdings erhalten Sie eine – gefälschte! – Mail in PayPal- oder Bank-Optik, die Ihnen dies suggerieren soll und die die Kontoverbindung der „Spedition“ oder „Schifffahrtsgesellschaft“ enthält. Auch diese Mail ist oft in sehr ungelenkem Deutsch formuliert. Brechen Sie spätestens jetzt ab! Überweisen Sie das Geld dennoch, können Sie es nur noch mit viel Glück und einer sehr schnellen Meldung an Ihre Bank zurückholen.

Das LKA listet mehrere Indizien auf, anhand derer Sie die Masche im Vorfeld erkennen können: Werden Sie misstrauisch, wenn ein „Interessent“ nicht konkret auf Ihre Anzeige eingeht und offensichtlich Textbausteine (womöglich aus einem Übersetzungsprogramm) schickt. Ein Alarmzeichen ist auch, dass der „Interessent“ bei einer Kleinanzeige (!) im Ausland sein will oder einen Versand dorthin wünscht und dass er den teuren Artikel angeblich nicht selbst

PayPal

Sie haben eine sofortige Zahlung erhalten

Lieber [redacted],

Sie haben eine PayPal Zahlung von **€690,00 EUR** von **Julia** [redacted] (j[redacted]@gmail.com).

Wir haben einen temporären Halt auf die Mittel dieser Transaktion.

Wie bereits in der Entgegennahme der Zahlung und als neue PayPal Zahlung Politik der Ware, haben wir voll belastet den Gesamtbetrag (oben) aus dem Konto des Käufers, die die Transport/Versandkosten inbegriffen (EMS Shipping Company).

HINWEIS: Um Diese Transaktion abzuschließen und die Mittel in Ihrem Konto genehmigt zu bekommen, Wir beraten Sie, gehen Sie zu einem nächstgelegenen Bank und senden Sie die überschüssige Summe von **€390,00 EUR** anden Transport-Agent. Das solltest du dann senden Sie uns eine gescannte Kopie/Foto von Ihrem Banküberweisung Quittungsbeleg (JPG-Format). Sie können die Überweisung auch online vornehmen, wenn Sie möchten. Das Geld wird in Ihrem Konto freigegeben, sobald wir bestätigen, dass Sie die Zahlung an den Spediteur gemacht haben.

HINWEIS: Dies ist wichtig als Sicherheitsmaßnahme, um die Sicherheit des Betriebs zu gewährleisten.

Bitte Nachfolgend finden Sie die Bankkontodaten, die für die Zahlung an die Reederei erforderlich sind.

Spedition: "EMS Shipping Company"
Verantwortlicher Spediteur: [redacted] Wagner

Screenshot: LKA Niedersachsen

Gefälschte PayPal-Mail: Bereits das schlechte Deutsch sollte Sie misstrauisch machen. Wenn das Problem außerdem nicht parallel in Ihrem PayPal-Konto sichtbar ist, will Sie jemand übers Ohr hauen.

anschauen und abholen kann. Brechen Sie den Kontakt spätestens dann ab, wenn er Ihnen ein Transportunternehmen aufschwatzen will und vorgibt, Ihnen für den Transport ungefragt zusätzliches Geld überwiesen zu haben.

Will ein seriöser Käufer etwas selbst abholen, kommt er persönlich zu Ihnen und ist bereit, unter Zeugen bar zu zahlen – und das Geld bei höheren Beträgen auf Ihren Wunsch hin und unter Ihrer Anwesenheit aus dem Geldautomaten zu ziehen. Damit verhindern Sie, Falschgeld ausgehändigt zu bekommen. Bei einem Versand geben Sie als Verkäufer die Bedingungen vor. Wenn Sie dabei PayPal nutzen, beachten Sie die Verkäuferschutzrichtlinie (siehe Artikel „PayPal-Schutz bei Privatgeschäften“ ab S. 76 und ct.de/wcm8). Bereits den Versuch eines Betruges sollten Sie der Polizei oder dem LKA melden. Das dient nicht nur der Statistik. Manchmal haben die Ermittler Glück oder erkennen ein Muster. Erwischte Serientäter können zudem nur als solche angeklagt werden, wenn der Staatsanwaltschaft genug Fälle aktenkundig sind.

Dreiecksbetrug

Eine weitere Masche, die sich gegen Verkäufer richtet, ist der Dreiecksbetrug. Der Ablauf: Sie möchten beispielsweise ein gebrauchtes Smartphone zu Geld machen und stellen es auf einem Kleinanzeigenportal oder einer Plattform wie eBay ein. Kurz darauf meldet sich ein Interessent über die Chatfunktion des Portals. Nachdem Sie sich handelseinig geworden sind, wird der Interessent Sie nach Ihren PayPal-Kontodaten fragen, also der verknüpften Mailadresse oder Telefonnummer. Außerdem möchte er bereits jetzt oder in einer weiteren Nachricht Ihre Adresse wissen – angeblich würde er selbst vorbeikommen oder jemanden schicken, um das Smartphone bei Ihnen zu Hause abzuholen.

Einige Tage darauf geht das Geld auf Ihrem PayPal-Konto ein, als Zahlung für „Waren und Dienstleistungen“ mit Käuferschutz. Wenig später erkundigt der Interessent sich, ob das Geld angekommen sei. Sie bejahen, woraufhin er selbst oder sein Vertreter wenig später vor Ihrer Tür steht. Sie übergeben ihm das Gerät.

In einer Variante haben Sie zunächst Versand vereinbart. Der vorgebliche Käufer zahlt daraufhin brav per PayPal mit „Waren und Dienstleistungen“. Kurz darauf erzählt er Ihnen, dass er selbst oder ein Freund zufällig gerade oder in wenigen Tagen in der Nähe sei. Er würde die Ware abholen und Sie könnten sich den Versand sparen. Stimmen Sie zu, kommt jemand vorbei und holt das Gerät ab.

Einige Tage später meldet sich ein Unbekannter per Mail bei Ihnen und fragt, wo das von ihm per PayPal bezahlte Smartphone bleibe. Von der Übergabe weiß er nichts. Folgerichtig leitet er ein Käuferschutzverfahren bei PayPal ein. Da Sie weder einen Versandbeleg noch eine Zustellbestätigung eines Paketdienstes vorweisen können, verlieren Sie und müssen dem Unbekannten sein Geld zurückerstatten.

Literatur

[1] Harald Bühring, Garantiert kompliziert, Von Amazon bis Trusted Shops: Garantiesysteme als Konfliktschlichtungsinstanz, c't 15/2020, S. 172

[2] Harald Bühring, Geleimt – was nun? Kleines Panoptikum der Internet-Betrügereien, c't 20/2018, S. 138

PayPal-Regeln für Käufer- und Verkäuferschutz
ct.de/wcm8

Was ist passiert? Nach dem ersten Kontakt mit dem „Interessenten“ hat dieser selbst ein Inserat geschaltet. Es enthielt die Beschreibung und Fotos Ihrer ursprünglichen Annonce sowie den gleichen Preis. Darauf ging der Unbekannte (das zweite Opfer) ein. Der erste, betrügerisch handelnde „Interessent“ schickte ihm dann Ihre PayPal-Daten. Nichtsahnend überwies der Unbekannte Ihnen das Geld. Das Smartphone holte jedoch der Trickbetrüger bei Ihnen ab. Der unbekannte Zahler erhielt es nicht und wandte sich deshalb an den Inhaber des PayPal-Kontos, nämlich Sie.

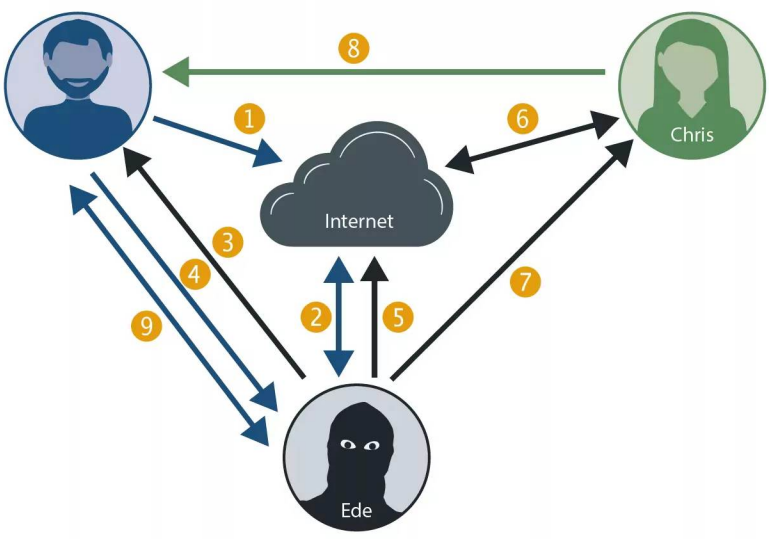
Der Unbekannte ist also ebenso Opfer. Den finanziellen Schaden haben allerdings Sie. An dieser Stelle ist unabhängig von PayPal auch die Gesetzeslage eindeutig: Erstatten Sie dem anderen Opfer das Geld nicht zurück, machen Sie sich einer ungerechtfertigten Bereicherung schuldig. Der unbekannte vermeintliche Käufer hat nach § 812 BGB einen Herausgabeanspruch gegen Sie. Auch bei PayPal ist die Sache klar: Der Verkäuferschutz fällt laut AGB bei persönlicher Übergabe explizit weg (siehe Artikel „PayPal-Schutz bei Privatgeschäften“ ab S. 76 und ct.de/wcm8).

Auch im Verlauf eines Dreiecksbetrugs gibt es Punkte, an denen Sie misstrauisch werden sollten. Gehen Sie bei PayPal-Zahlungen nicht auf persönliche Übergabe ein (damit verlieren Sie den Verkäuferschutz). Bestehen Sie stattdessen auf Barzahlung unter Zeugen. Außerdem gilt wie beim Speditionsbetrug: Vorsicht, wenn der Interessent nicht konkret auf den Artikel und dessen Zustand eingeht! Laut Polizei Köln sind außerdem Freemail-Adressen wie web.de, gmx.de oder hotmail.com ein Indiz. Da die Provider keine Identitätschecks ihrer Nutzer durchführen, können diese in der Anonymität des Netzes untertauchen. Das PayPal-Konto des Betrügers hilft Ihnen ebenfalls nicht. Er wird es entweder kurzfristig unter falschem Namen eröffnet haben oder hat sich die Zugangsdaten einer dritten Person verschafft.

Auch als zweites Opfer hätten Sie vielleicht misstrauisch werden können: Seien Sie auf der Hut, wenn der Name in der Kleinanzeige nicht zur Mailadresse passt, insbesondere jener, die mit dem PayPal-Konto verknüpft ist. Brechen Sie lieber ab, wenn Sie Zweifel an der Seriosität eines Inserenten bekommen.

Dreiecksbetrug

1 Alex schaltet Verkaufsanzeige über 300 Euro für ein Handy. 2 Ede (Betrüger) zeigt Interesse an dem Handy. 3 Ede bietet Alex an, mit PayPal (Option „Waren und Dienstleistungen“) zu bezahlen. 4 Alex übermittelt seine PayPal-Daten an Ede. 5 Ede schaltet eigene Verkaufsanzeige für Alex’ Handy. 6 Chris geht auf die Anzeige von Ede ein. 7 Ede schickt Chris die PayPal-Bezahldaten von Alex. 8 Chris zahlt die 300 Euro über PayPal an Alex, glaubt aber, an Ede zu zahlen. 9 Ede (persönlich oder ein Strohmann) holt das Handy bei Alex an der Haustür (!) ab und verschwindet auf Nimmerwiedersehen.



Standardmaschen

Auch ohne das Dreiecksgeflecht gilt grundsätzlich: Bei PayPal genießen Sie keinen Käufer- oder Verkäuferschutz, sobald die Übergabe des Verkaufsgegenstandes persönlich erfolgt. Das Dreieck verschleiert lediglich die Absichten des Betrügers besser. Außerdem hinterlassen die Täter keine Spuren, weil sie für die Masche kein eigenes PayPal-Konto benötigen.

Darüber hinaus hören wir bei c’t immer wieder von Fällen, bei denen vermeintliche Privatverkäufer oder Betreiber von Fake-Shops ihre Opfer dazu gebracht haben, einen Artikel oder eine Dienstleistung bei PayPal mit der Option „Freunde und Familie“ zu bezahlen. Im Prinzip gleicht dies einer Vorkasse per Überweisung: Geraten Sie an einen Betrüger, ist das Geld weg, da der PayPal-Käuferschutz dann grundsätzlich entfällt. Deshalb können wir „Freunde und Familie“ wirklich nur für private Transfers empfehlen – auch wenn man PayPals Preispolitik gegenüber Verkäufern bei der Option „Waren und Dienstleistungen“ und die komplizierten Geschäftsbedingungen durchaus kritisieren kann. (mon) ct

„Sicheres Bezahlen“ auf Kleinanzeigen

Kleinanzeigen ist die meistgenutzte Privatverkaufsplattform in Deutschland. Das lockt auch Kriminelle an. Wir beantworten häufige Fragen zu Betrugsmaschen sowie zu sicheren Zahlungsarten.

Von **Markus Montz**

Die Maschen der Betrüger

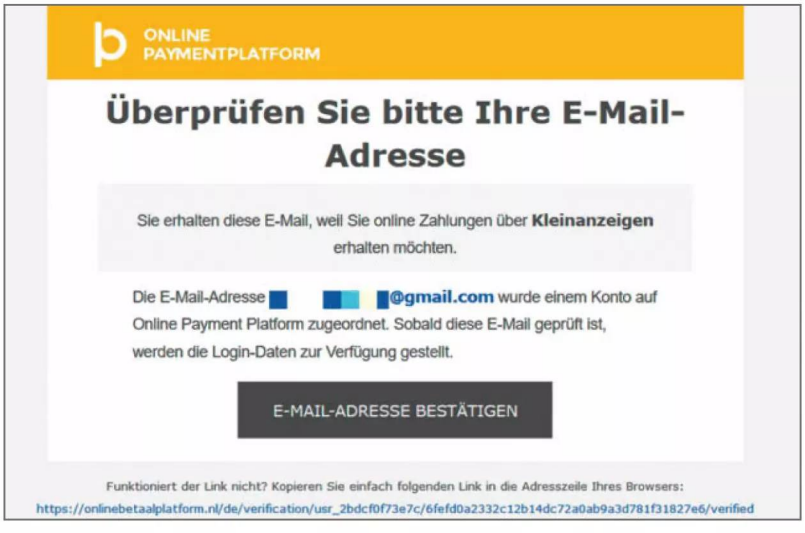
Woran erkenne ich Betrugsabsichten?

Betrügerische Absichten treten fast immer erst im Verlauf der Kommunikation zutage. Nahezu alle Maschen setzen direkt oder indirekt am Bezahlweg an. Dafür brauchen die Täter zunächst Ihre Mailadresse oder Telefonnummer, vorzugsweise Ihre Handynummer. Damit können sie außerhalb der Plattform mit Ihnen kommunizieren und umgehen so deren Sicherheitsmechanismen. In Kombination mit zeitlichem und emotionalem Druck sollen Sie Fehler machen. Unsere Grundregel lautet: Geben Sie Daten nur bei unbedingtem Bedarf weiter und kommunizieren Sie ausschließlich über den Kleinanzeigen-Chat.

Kennen Kriminelle Ihre Mailadresse oder Telefonnummer, können sie dorthin Mail-, Messenger- oder SMS-Nachrichten verschicken. Deren Absender-Adressen oder -Telefonnummern sind oft gefälscht (siehe Artikel „Telefonbetrug trotz Zwei-Faktor-Prinzip“ ab S. 116) und die Täter geben sich als Kleinanzeigen, deren Dienstleister OPP, Polizei, Zoll, Bank, PayPal oder Paketdienst aus.

Solche (oft täuschend echt aussehenden) Nachrichten enthalten beispielsweise falsche Versand- oder Zahlungsbestätigungen. Auch gefälschte Fehlermeldungen zu angeblichen Zahlungsflüssen sind beliebt, selbstverständlich samt Handlungsanweisungen und Links zur „Behebung“. In der Regel verweisen die Links auf gefälschte Seiten, auf denen die Betrüger Ihre Kontozugangs- oder Kreditkartendaten abgreifen wollen (Phishing). Manche Nachrichten enthalten auch mit Schadsoftware verseuchte Anhänge.

Klicken Sie nicht auf Links und öffnen Sie keine Anhänge. Prüfen Sie den Wahrheitsgehalt solcher Nachrichten immer zusätzlich im jeweiligen Nutzerkonto, etwa bei Ihrer Bank, PayPal oder bei Kleinanzeigen und deren Zahlungsdienstleister OPP selbst. Die URL tippen Sie selbst ein oder nutzen Ihr Bookmark. Tatsächliche Probleme oder laufende Prozesse werden Ihnen dann auch dort angezeigt.


ONLINE PAYMENTPLATFORM

Überprüfen Sie bitte Ihre E-Mail-Adresse

Sie erhalten diese E-Mail, weil Sie online Zahlungen über **Kleinanzeigen** erhalten möchten.

Die E-Mail-Adresse [redacted]@gmail.com wurde einem Konto auf Online Payment Platform zugeordnet. Sobald diese E-Mail geprüft ist, werden die Login-Daten zur Verfügung gestellt.

E-MAIL-ADRESSE BESTÄTIGEN

Funktioniert der Link nicht? Kopieren Sie einfach folgenden Link in die Adresszeile Ihres Browsers:
https://onlinebetaalplatform.nl/de/verification/usr_2bdcf0f73e7c/6fefd0a2332c12b14dc72a0ab9a3d781f31827e6/verified

Bild: Online Payments Platform

Während Sie „Sicher bezahlen“ (unaufgefordert!) in Ihrem Kleinanzeigen-Nutzerkonto einrichten, bekommen Sie zwei Mails des Zahlungsdienstleisters OPP in diesem Stil. Alles andere ist sicher gefälscht.

Nur wenn Sie selbst (!) aktiv in Ihrem Nutzerkonto (!) auf der Website oder in der App von Kleinanzeigen die Registrierung für „Sicher bezahlen“ angestoßen haben (siehe nächste Seite), leitet Kleinanzeigen Sie auf die Seite von OPP weiter. OPP schickt Ihnen Mails zur Bestätigung. Die Freischaltung dauert aber eine Weile, weil man Ihre Bankdaten dort zunächst prüft.

Es trifft auch erfahrene User

? Ich kenne mich doch aus. Warum glaubt Ihr, ich könnte Geld an Betrüger bezahlen?

! Weil die Täter psychologisch gut geschult sind und nach unserer Erfahrung selbst Fachleute auf dem falschen Fuß erwischen können. Bereits mit den Handlungsanweisungen oder Fehlermeldungen im Zahlungsfluss wollen die Täter Sie unter zeitlichen oder emotionalen Druck setzen und zu Fehlern verleiten (Social Engineering).

Mitunter verstärken sie dies mit frei erfundenen Geschichten à la „Ich habe noch andere Interessenten“ oder „Ich brauche das Geld für meine kranke Mutter“. Sie schicken Mails, Nachrichten oder rufen sogar an, um über stimmig klingende Geschichten Vertrauen zu erzeugen (siehe Artikel „Theaterspiel mit Betrugsabsicht“ ab S. 96). Dabei versuchen sie beispielsweise, Sie zu einer Überweisung oder Zahlung mittels „Freunde und Familie“ bei PayPal zu bewegen. Schöpfen Sie ebenso Verdacht, wenn die Gegenseite Abmachungen plötzlich ändert oder sich über Regeln von Bezahl- oder Verkaufsplattformen hinwegsetzen will („Sie können sich das Paket doch sparen, ich schicke jemanden vorbei“). Auffällig sind auch zusätzliche Wünsche („kaufen Sie noch eine Gutscheinkarte dazu, ich bezahle sie auch“). Andere Adressaten oder Bevollmächtigte deuten ebenfalls auf unlautere Absichten hin (siehe Artikel „PayPal-Betrug auf Kleinanzeigenportalen“ ab S. 108).

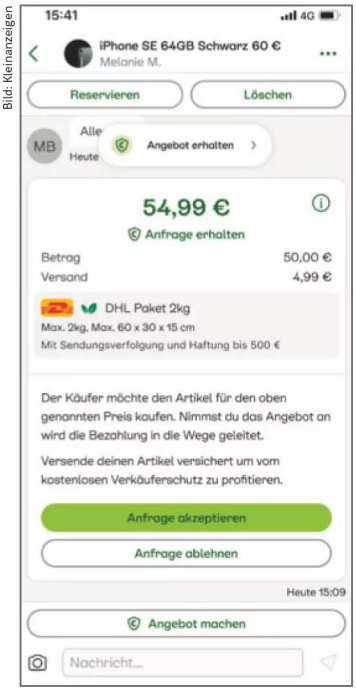
Brechen Sie den Handel in solchen Fällen lieber einmal zu oft ab. Wollen Sie trotzdem weitermachen, gehen Sie in Ruhe vor, achten Sie sorgfältig auf die Regeln für den Käufer- oder Verkäuferschutz und lehnen Sie Abweichungen konsequent ab. Kriminelle verschwinden dann meistens von selbst.

Empfohlene Bezahlmethoden

? Wir sind uns handelseinig. Was sind denn sichere Bezahlmethoden?

Zahlungen mit „Sicher bezahlen“ finden ausschließlich innerhalb des Chats von Kleinanzeigen (Website oder App) statt.

Bild: Kleinanzeigen



! Die sicherste Bezahlmethode ist Barzahlung bei Abholung. Sie bekommen den Verkäufer zu Gesicht, können die Ware prüfen und ihm das Geld direkt aushändigen. Als Verkäufer haben Sie die Knete sofort in der Hand. Bleibt Ihnen nur Versand als Option, bietet das für den Käufer kostenpflichtige Treuhandsystem „Sicher bezahlen“ von Kleinanzeigen einen guten Schutz vor Betrug. Auch PayPal ist mit seinem Käuferschutz sehr sicher. Wichtig ist immer, dass Sie die Regeln des jeweiligen Systems kennen und einhalten.

Cash vor Ort

? Was muss ich bei Barzahlung und Abholung beachten?

! Bei kleineren Summen ist das Risiko vernachlässigbar. Geht es um größere Beträge (je nach Ihrer Schmerzgrenze), sollten Sie als Käufer wie Verkäufer bei der Übergabe einen oder mehrere Zeugen haben. Verkäufern droht zusätzlich Falschgeld als Gefahr. Um das zu vermeiden, können Sie vorab und verbindlich mit dem Käufer vereinbaren, ihn zur Bank oder einem Bankautomaten zu begleiten. Setzen Sie unter Umständen einen Kaufvertrag auf. Für

Autos gibt es zum Beispiel vom ADAC Standardvordrucke (ct.de/w946). Notieren Sie sich Autokennzeichen und etwaige Auffälligkeiten.

„Sicher bezahlen“

? Worauf achte ich bei „Sicher bezahlen“ von Kleinanzeigen?

! „Sicher bezahlen“ ist eine für den Käufer kostenpflichtige Treuhand-Transaktion auf Kleinanzeigen. Diese führt der niederländische Dienstleister OPP im Auftrag der Plattform durch, bei dem Sie dafür aus Ihrem Kleinanzeigen-Konto heraus ein Nutzerkonto eröffnen. Anschließend wickeln Sie „Sicher bezahlen“ entweder in der Smartphone-App oder auf der Kleinanzeigen-Homepage im Browser ab (siehe Screenshot nächste Seite und Artikel „‘Sicher bezahlen‘ bei Kleinanzeigen“ auf S. 102). Dort richten Sie „Sicher bezahlen“ auch ein.

Kriminelle zielen gerne auf Menschen, die „Sicher bezahlen“ noch nicht kennen. Machen Sie sich daher in Ruhe damit vertraut (ct.de/w946) und richten Sie es unabhängig von einem Kauf oder Verkauf ein. Extern versandte Nachrichten mit Zahlungsaufforderungen, 3-D-Secure-Bestätigungen für Kreditkarten oder Links zur Registrierung bei „Sicher bezahlen“ sind immer gefälscht! Das gilt ebenso für angebliche Mails, SMS oder Messenger-Nachrichten Ihrer Bank, die mit „Sicher bezahlen“ oder Kleinanzeigen in Zusammenhang stehen. Ihre Bank schickt Ihnen allenfalls eine Push-Nachricht für die Zwei-Faktor-Authentifizierung über Ihre Banking-App, wenn Sie den Kauf auch tatsächlich bezahlen wollen.

PayPal

? Welche Fußangeln gibt es bei PayPal?

! PayPal bietet einen Käufer- und einen Verkäuferschutz an, die das Unternehmen jedoch an Regeln knüpft (alle Regeln unter ct.de/w946). Wichtig: Die Zahlungsart muss „Waren und Dienstleistungen“ sein. Dafür zahlt der Verkäufer eine Provision. Lassen Sie sich nicht auf „Freunde und Familie“ ein, solange es sich nicht tatsächlich um vertrauenswürdige Freunde oder Familienmitglieder handelt. Zwar ist das kostenlos, damit entfällt der Käufer- und Verkäuferschutz aber.

Die Ware müssen Sie oder der Verkäufer zudem mit einem versicherten Paket samt elektronischer Sendungsverfolgung versenden. Das bieten zum Beispiel DHL Paket oder das Einschreiben der Post. Aufgepasst: Bei persönlicher Übergabe gibt es keinen Käufer- und keinen Verkäuferschutz, auch nicht für „Waren und Dienstleistungen“! Vielmehr können die Täter den Käufer- oder Verkäuferschutz dann sogar gegen Sie arbeiten lassen (siehe Artikel „PayPal-Betrug auf Kleinanzeigenportalen“ ab S. 108). Lassen Sie sich bei persönlicher Abholung gar nicht erst auf PayPal ein, sondern bestehen Sie auf Barzahlung. Hat ein Käufer bereits mit „Waren und Dienstleistungen“ bezahlt, bestehen Sie auf Versand. Bietet er Ihnen spontan an, doch abzuholen, lehnen Sie dies ab. Andernfalls wird er jedes Käuferschutzverfahren gegen Sie gewinnen, weil Sie keine Sendungsverfolgung haben.

Provisionen

? Gibt es bei Versand keinen kostengünstigeren Weg, sicher zu bezahlen?

! Nein. Die Provisionen sind in der Tat happig: PayPal nimmt für „Waren und Dienstleistungen“ 2,5 Prozent des Preises plus 35 Cent von privaten Verkäufern, Kleinanzeigen für „Sicher bezahlen“ 4,5 Prozent plus 35 Cent vom Käufer. Das ist das Geschäftsmodell, die Provision deckt aber ähnlich einer Versicherungsprämie auch den Aufwand von PayPal und OPP für Käuferschutzverfahren ab. Zudem kann man sich mit einem seriösen Gegenüber fast immer auf eine faire Verteilung der Kosten einigen.

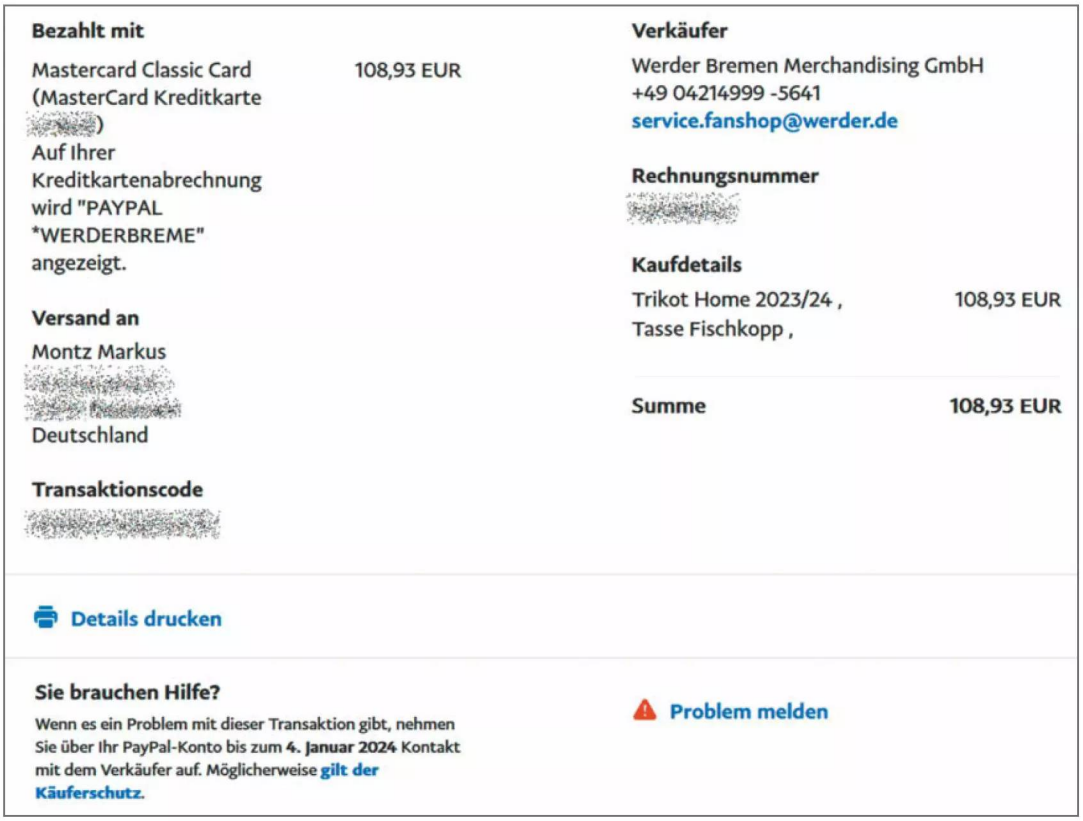
SEPA-Überweisung

? Warum ratet Ihr von der viel billigeren SEPA-Überweisung ab? Ich passe auf, bei mir ist das noch immer gut gegangen.

! Normalerweise kennen Sie Ihr Gegenüber nicht und für Kriminelle sind Überweisungen ein Geschenk. Wenn Sie eine Überweisung abgeschickt haben, ist das Geld bei einem Betrug fast immer verloren. Nur wenn Sie innerhalb kürzester Zeit handeln und Ihr Kreditinstitut um einen Überweisungsrückruf bitten, können Sie Glück haben. Ihre Bank oder Sparkasse führt die Überweisung in der Regel innerhalb von drei bis maximal 24 Stunden durch. Mitunter geht es noch schneller.

Zwar können Sie bei Betrug Ihre Bank um Hilfe bitten oder den Rechtsweg beschreiten. Betrüger nutzen aber normalerweise gekaperte Konten oder sol-

Bild: LKA Niedersachsen



Bezahlt mit

Mastercard Classic Card (MasterCard Kreditkarte [redacted])
108,93 EUR

Auf Ihrer Kreditkartenabrechnung wird "PAYPAL *WERDERBREME" angezeigt.

Versand an

Montz Markus
[redacted]
Deutschland

Transaktionscode

[redacted]

Verkäufer

Werder Bremen Merchandising GmbH
+49 04214999 -5641
service.fanshop@werder.de

Rechnungsnummer

[redacted]

Kaufdetails

Trikot Home 2023/24 , 108,93 EUR
Tasse Fischkopp ,

Summe 108,93 EUR

Details drucken

Sie brauchen Hilfe?

Wenn es ein Problem mit dieser Transaktion gibt, nehmen Sie über Ihr PayPal-Konto bis zum **4. Januar 2024** Kontakt mit dem Verkäufer auf. Möglicherweise **gilt der Käuferschutz.**

Problem melden

Um ein PayPal-Käuferschutzverfahren einzuleiten, rufen Sie einfach die Transaktion auf.

che von Strohleuten. Eingegangenes Geld schicken die direkt weiter, Betroffene sehen es selten wieder.

Zweifellos gibt es trotzdem viele ehrliche Handelspartner. Letztendlich müssen Sie selbst abwägen, ob Sie das Risiko eingehen wollen oder nicht. Aus unserer Sicht sprechen die kaum mögliche Rückabwicklung und ihre Beliebtheit bei Betrügern aber gegen die Überweisung.

Rückabwicklung

? Jemand hat mir ein falsches oder beschädigtes Produkt oder gar nichts geschickt. Wie bekomme ich mein Geld zurück?

! Dokumentieren Sie die Sendung mit Fotos und die Kommunikation mit Screenshots. Versuchen Sie zunächst, sich mit dem Verkäufer zu einigen und setzen Sie eine Frist.

Passiert nichts, nutzen Sie den Käuferschutz. Wie das geht, beschreiben Kleinanzeigen und PayPal, aber zum Beispiel auch eBay jeweils auf Ihren Websites (ct.de/w946). Bei Kleinanzeigen geben Sie außerdem die Zahlung nicht frei. Reagieren Sie weder dort noch bei PayPal auf Mails, die Kontozugangs-, Bank- oder Kartendaten abfragen. Kommen Sie aber allen Rückfragen zur Sache und zu Belegen unverzüglich nach.

Den Transportdienst für den Rückversand beauftragen allein Sie, gegebenenfalls nach den Vorgaben von PayPal oder Kleinanzeigen, auch bei der Adresse. Davon abweichende Empfehlungen oder gar Aufforderungen der Gegenseite deuten meistens auf unlautere Absichten hin. (mon) c't

FAQs und Bedingungen der Dienste, ADAC-Vordruck
ct.de/w946

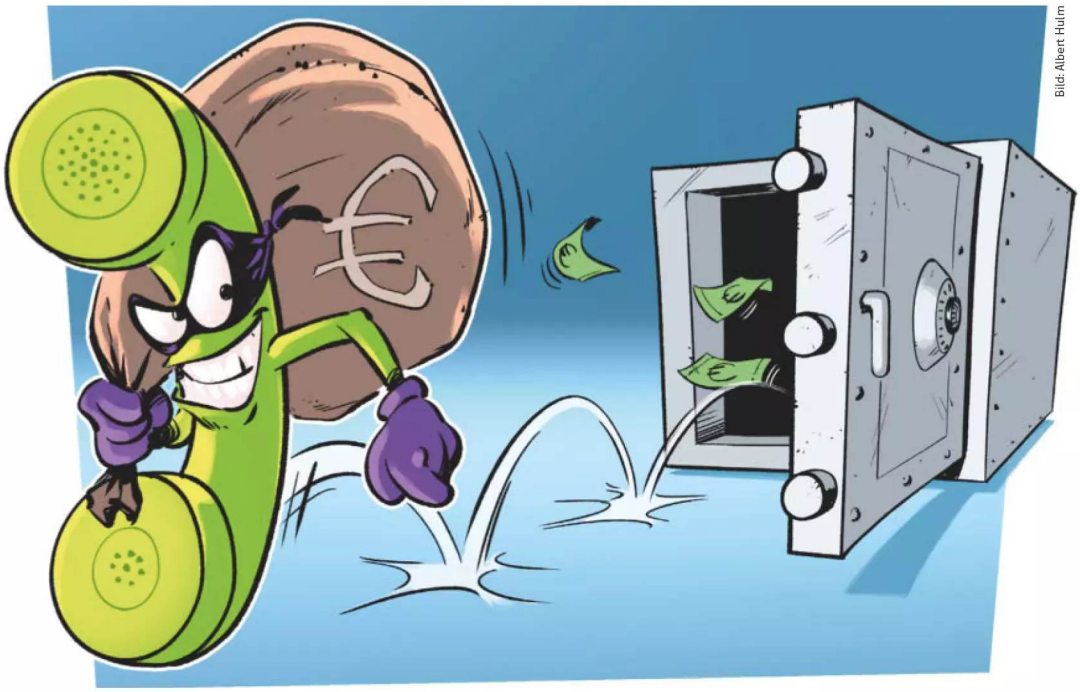


Bild: Albert Hulm

Telefonbetrug trotz zweitem Faktor

Ein dringender Anruf von der Hausbank: Gauner seien gerade dabei, Ihr Geld zu klauen, es gehe um Minuten. Dabei geht die wahre Gefahr vom bestens geschulten Anrufer aus. Wir haben uns von Online-Banking-Betrügern ausbilden und fast abzocken lassen.

Von **Mirko Dölle**

Online-Banking-Betrug sollte heute eigentlich völlig unmöglich sein: Schließlich erfordert gemäß der EU-Richtlinie PSD2 (Payment Service Directive 2) seit Anfang 2021 jede Überweisung eine Zwei-Faktor-Autorisierung. TAN-Listen haben ebenso ausgedient wie das SMS-TAN-Verfahren, an ihre Stelle sind sehr sichere Authentifizierungsverfahren wie pushTAN oder photoTAN getreten. Diese Authentifizierung knacken? Ziemlich aussichtslos.

Stattdessen haben die Betrüger den Menschen als Schwachstelle für sich entdeckt. Statt Zwei-Faktor-Autorisierungen anzugreifen, setzen sie mit psychologischen Tricks bei den Konteninhabern an – mit Erfolg. Dabei spielt ihnen die vermeintliche Kunden-

freundlichkeit verschiedener Banken in die Hände. Wir haben die aktuellen Betrugsmaschen beim Online-Banking-Betrug untersucht, haben uns zum Betrüger schulen lassen und dabei zugesehen, wie andere uns betrügen wollten.

Die Grundlage für den Online-Banking-Betrug ist Phishing, damit sich die Täter auf Ihren Konten umsehen können. Dabei profitieren die Kriminellen von Finanzinstituten, die die Sicherungsanforderungen auf das gesetzliche Mindestmaß absenken und nur alle 90 Tage nach dem zweiten Faktor fragen. Das wird häufig mit Kundenfreundlichkeit begründet oder damit, dass man den Kunden keine zu hohen Hürden auferlegen wolle, die Online-Angebote zu nutzen. Insbesondere bei Sparkassen ließen sich aber auch höchst sensible Informationen wie Name, vollständige Anschrift, Festnetz- und Mobilfunkrufnummer, die E-Mail-Adresse, Kontoauszüge und sogar Dokumente wie die Kontoeröffnung und der Name des Kundenberaters allein mit Benutzernamen und Passwort abrufen. Inzwischen haben die Sparkassen nach geschärft und Verlangen beim Login eine TAN.

Es gibt noch etliche weitere Banken, die auf eine Zwei-Faktor-Autorisierung bei der Anmeldung verzichten. Darunter sind viele Volks- und Raiffeisen-Banken, Spardabanken, die GLS-Bank und Comdirekt. Phisher erhalten so allein mit Benutzername und Passwort ein komplettes Personen- und Finanzprofil ihres Opfers. Und selbst wenn die Kriminellen zufällig einmal nach dem zweiten Faktor gefragt werden sollten, brechen sie einfach das Login ab und warten, bis der Kontoinhaber sich das nächste Mal regulär angemeldet hat. Danach haben sie wieder für Wochen oder gar Monate freie Bahn.

Hinzu kommt, dass Banken bei der Auswahl der Benutzernamen mitunter wenig kreativ sind. Oft genügt die Angabe der Kontonummer, manche Sparkasse verwendet sogar das erste Initial des Vornamens plus den Nachnamen des Kunden als Benutzernamen fürs Online-Banking. Das ist für Angreifer schon die halbe Miete. Auch die Anforderungen an das Passwort sind nur vermeintlich kundenfreundlich, manche Sparkassen erlauben einfache fünfstellige Ziffernfolgen.

Erst abgephisht …

Eine übliche Vorgehensweise der Kriminellen ist, zunächst die Zugangsdaten über eine fingierte E-Mail oder SMS abzuphishen. Dabei landen die Opfer über einen präparierten Link auf einer mehr oder weniger gut nachgemachten Fake-Bankseite. Auch vorgebliche SMS-Nachrichten vom Zoll, wonach ein kleiner Betrag zu begleichen wäre, dienen dem Betrug: Die auf der angeblichen Zoll-Homepage hinterlegten Links zu den Online-Zugängen der Banken führen tatsächlich zu Phishing-Seiten.

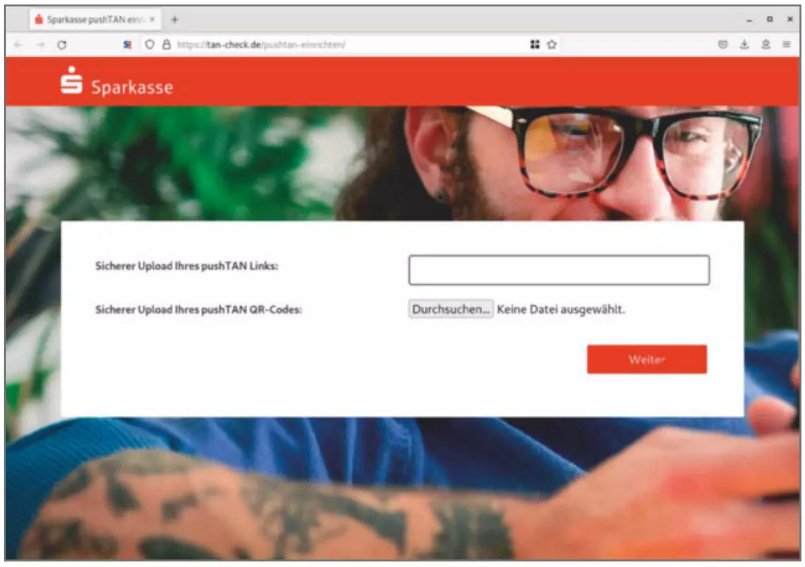
Um die Spur von den Phishern zu den Telefonbetrügern zu verfolgen, arbeiteten wir bei unseren Recherchen mit der Journalistin Maja Helmer vom Autorenwerk in Berlin zusammen. Sie eröffnete ein Girokonto bei der Sparkasse in Osnabrück, deponierte ein Guthaben von 5000 Euro als Köder und gab ihre Zugangsdaten für das Online-Banking auf mehreren bekannten Phishing-Seiten ein. Deren Adressen veröffentlicht zum Beispiel die Polizei Niedersachsen auf ihren Präventionsseiten.

Nach einigen Wochen gab es nächtliche Logins über den Online-Banking-Zugang, die Phisher überprüfen wohl die Zugangsdaten. Das ist typisch, an einem erfolgreichen Betrug sind mehrere Tätergruppen beteiligt: Phisher sind auf die Beschaffung von Personen- und Zugangsdaten spezialisiert und verkaufen sie etwa an Online-Banking-Betrüger weiter. Dort wird das Kundenprofil um weitere Details angereichert und dann wiederum an Abschließer oder Verwerter weiterverkauft, die dann bei den Opfern anrufen und sie um ihr Geld bringen.

Ein solcher Anruf erfolgt aber erst dann, wenn sich die Gauner bereits auf Ihrem Konto umgesehen und Sie als potenzielles Opfer ausgewählt haben. Das bestätigen auch unsere Datenabfragen bei der Sparkasse Osnabrück: Der Zugang des Lockvogelkontos wurde mehrfach zu unterschiedlichen Zeitpunkten von IP-Adressen aus aller Welt benutzt. Dabei wird nicht nur der Kontostand, sondern auch die hinterlegten persönlichen Daten bis hin zu Adresse und Telefonnummer abgerufen.

… dann ausgenommen

Schließlich bekommt Maja Helmer einen Anruf auf dem Handy: Eine Frau gibt sich als Anita Schwarz von der Sparkasse Berlin aus, die angezeigte Rufnummer ist jedoch die der Sparkasse Osnabrück, wo das Konto geführt wird. Offenbar hat die Anruferin das mit der hinterlegten Anschrift verwechselt. Maja Helmer ignoriert diesen offenkundigen Lapsus und geht auf alles ein, was Frau Schwarz erzählt: Um das angeblich gehackte Konto abzusichern, müsste das pushTAN-Verfahren aktualisiert werden. Der Bestätigungslink, der gleich zugestellt werde, müsse aber aus Sicherheitsgründen auf der Internetseite tan-check.de eingegeben werden.



Weil der Online-Banking-Zugang angeblich gehackt wurde, müsse das pushTAN-Verfahren aktualisiert werden. Den Bestätigungslink dafür solle man aus Sicherheitsgründen auf der Website tan-check.de eingeben, die natürlich den Betrügern gehört.

Statt des geforderten Bestätigungslinks gibt Helmer etwas anderes ein. Das gefällt Frau Schwarz überhaupt nicht, sie bricht das Gespräch ab. Eine Datenabfrage bei der Sparkasse Osnabrück ergibt im Nachgang, dass die Täter tatsächlich versucht haben, ein neues pushTAN-Gerät anzumelden. Damit hätten sie nach Belieben über das Konto und das Guthaben verfügen oder Google- oder Apple Pay einrichten können.

Spurensuche

Virtuelle Zahlungskarten via Google Pay und Apple Pay sind für Online-Banking-Betrüger der schnellste Weg, um an das Geld ihrer Opfer zu kommen: Sie starten eine große Shopping-Tour quer durch Lebensmittel-, Technik- und Möbelmärkte und leeren so das Konto. Dabei müssen die Gauner nicht einmal damit rechnen, erwischt zu werden, denn die Aufzeichnungen von Überwachungskameras etwa an den Kassen dürfen nur wenige Tage aufbewahrt werden. Bis der Betrug auffliegt, das Opfer Anzeige erstattet, Polizei und Staatsanwaltschaft mit den Ermittlungen beginnen und schließlich bei den einzelnen Läden anklopfen, sind die Videos längst gelöscht.

Wir schauen uns die inzwischen vom Netz genommene Seite tan-check.de genauer an, auf der Maja Helmer den Bestätigungslink eintragen sollte. Unter der Haube steckt ein gewöhnliches WordPress-CMS, die Logos und Bilder wurden offenkundig von Websites der Sparkassen geklaut. Wie wir mit diebischer Freude feststellen, haben die Betrüger schlampig gearbeitet und sowohl das JSON-API als auch die XML-RPC-Schnittstelle des WordPress sperrangelweit offen gelassen. So konnten wir feststellen, dass die Website tan-check.de bis Ende 2022 unter der Adresse psd2-2022.de lief.

Laut Datenbank fand die Erstinstallation sogar weitaus früher statt, seit dem 1. August 2021 gibt es die WordPress-Seite bereits, danach wurde sie mindestens zweimal auf neue Server kopiert. Bei der Erstinstallation hatte der Server allerdings noch keinen Hostnamen, sondern wurde unter der IP-Adresse 195.178.120.144 betrieben. Dies könnte ein interessanter Ermittlungsansatz für die Behörden sein; vielleicht hatte damals ein Bandenmitglied unter seinem echten Namen den Server angemietet. Wir haken bei allen Providern nach, die wir aus der Historie der WordPress-Installation ermitteln können, bekommen aber keinerlei Auskünfte. Damit endet für uns die Datenspur.

Unter Hochdruck

Betrüger verwenden auch andere Methoden, um Konten abzuräumen. Eine Variante kommt ohne verdächtige pushTAN-Geräte oder virtuelle Debitkarten aus. Dabei bauen die Betrüger besonders viel Druck

auf die Kontoinhaber auf. Hierbei stehen Kunden der Sparkassen im Fokus, die ihre Konten für Auslandsüberweisungen freigeschaltet haben.

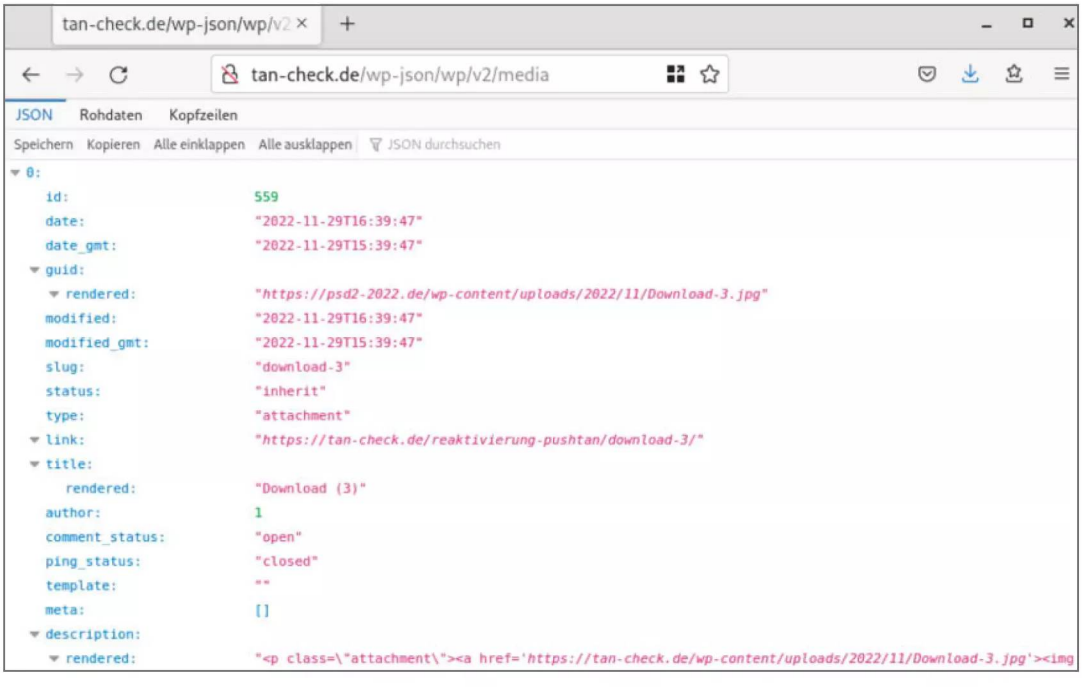
Die Masche beruht darauf, dass Sparkassen besonders im ländlichen Raum einen vergleichsweise engen Kontakt zu ihren Kunden pflegen. Es ist durchaus normal, dass der individuelle Kundenberater der örtlichen Filiale bei auffälligen Kontobewegungen zum Telefon greift und die Kunden anruft. Überweist man etwa 20.000 Euro an das Finanzamt und hat eigens dafür das Tageslimit erhöht, so kann es passieren, dass die Überweisung zurückgehalten wird und man einen Anruf der Sparkasse erhält.

Genau in diese Kerbe schlagen die Betrüger: Sie rufen außerhalb der Öffnungszeiten, bevorzugt am späten Nachmittag vor einem Wochenende oder Feiertag, an und geben sich als Kollege des eigentlichen Kundenberaters aus. Als Beleg für ihre Glaubwürdigkeit führen sie, genau wie die echten Kundenberater der Sparkassen, die angezeigte Rufnummer an, die zur Filiale des Kunden passt.

Der Grund für den Anruf sei eine auffällige Überweisung in Höhe des Tageslimits an ein ausländisches Konto, die man vorliegen habe und die zum vorgeblichen Tagesabschluss um 17 Uhr ausgeführt werde. Man wolle sich nur vergewissern, dass mit dieser Überweisung alles in Ordnung sei, denn noch seien ein paar Minuten Zeit, um sie zu stoppen.

Tatsächlich gibt es diese Überweisung nicht, die Betrüger haben lediglich mit den abgephishten Zugangsdaten eine Überweisungsvorlage erstellt. Daher wird der Kontoinhaber bestreiten, diese Auslandsüberweisung veranlasst zu haben, und tappt damit in die Falle: Der Anrufer erklärt dann, dass der Kunde die Stornierung der Überweisung innerhalb der nächsten Minuten mit einer pushTAN autorisieren müsse. Dabei würden ihm das ausländische Zielkonto und der Betrag der zu stornierenden Überweisung angezeigt, um sicherzugehen, dass es sich auch um die richtige Überweisung handele. Die Autorisierungsdaten müsse man dann nur auf einer speziellen Internetseite der Bank in ein Formular eintragen, deren URL der Anrufer ebenfalls nennt.

Das Perfide an der Masche: Äußert man im Gespräch Zweifel an der Echtheit des Anrufers oder dem Vorgehen, so wird der Anrufer sofort anbieten, dass man auch nach dem Wochenende in der Filiale vorbeischauen und mit seinem Kundenberater den Fall klären könne. Die Überweisung sei dann zwar schon ausgeführt, aber vielleicht habe man ja Glück



Bei der Phishing-Seite für Sparkassen-Zugangsdaten handelte es sich um ein WordPress-CMS, bei dem die Betrüger vergessen hatten, das JSON-API zu schützen. So konnten wir die frühere Domain psd2-2022.de ermitteln.

und könne das Geld aus dem Ausland wieder zurückbuchen. Da der Anruf außerhalb der Öffnungszeiten der Sparkassenfiliale erfolgt, wird der Betrüger auch erklären, dass ein Rückruf etwa zur Verifizierung der Nummer erst nach dem Wochenende wieder möglich ist, weil die Zentrale nicht mehr besetzt sei. Typisch für die Masche ist auch, dass immer wieder an den vermeintlichen Tagesabschluss zur vollen Stunde und die nur noch wenigen verbleibenden Minuten für die Stornierung erinnert wird.

In Wahrheit führen die Betrüger im Hintergrund die Überweisungsvorlage aus, sodass der Sparkassenkunde via pushTAN wie angekündigt Zielkonto und Betrag genannt bekommt. Die ebenfalls übermittelte TAN dient jedoch nicht zur Stornierung der Überweisung, sondern zur Freigabe. Gibt der Kontoinhaber die Daten auf der vom Anrufer genannten Website ein, ist er das Geld los und bekommt es auch nicht ersetzt, wenn er nach dem Wochenende bei seiner Sparkassenfiliale nachhakt, wieso die beauftragte Stornierung denn nicht erfolgt sei.

Betrüger in Ausbildung

Wir wollen herausfinden, wieso diese Maschen häufig auf Kunden der Sparkassen zielen und wie es Call-Center-Agenten immer wieder gelingt, ihren Opfern das Geld regelrecht abzuschwatzen. Wir beschließen, die Betrüger selbst zu befragen: Auf CrimeNetwork und im Darknet finden wir verschiedene Lehrunterlagen und Schulungsangebote. Online-Banking-Tutorials gibt es ab 100 Euro, eine individuelle Schulung durch einen Mentor kostet 800 Euro. Dort soll man in die Kunst des Online-Banking-Betrugs eingeführt und in der Gesprächsführung trainiert werden. Ein Monitoring der ersten Gespräche mit anschließendem Feedback gehört ebenfalls zum Angebot – was wir selbstverständlich nicht in Anspruch nahmen.

Das Lehrmaterial zielt direkt auf Kunden von Sparkassen sowie Volks- und Raiffeisenbanken ab. Kern der Argumentation ist, dass es sich hierbei um Bankenverbunde handelt, anders als bei den privaten Großbanken wie zum Beispiel Commerzbank oder Deutsche Bank. So weisen Sparkassen regionale Unterschiede auf und sind an regional unterschiedliche Rechenzentren angebunden, während es bei den großen Privatbanken keine regionalen Spezialitäten im Online-Banking gibt.

Diese Unterschiede soll es, so steht es in den Unterlagen und so wird es uns ebenfalls von Kontaktpersonen berichtet, auch bei der Betrugsprävention geben. So hätten die privaten Großbanken deutschlandweit aktive Anti-Fraud-Abteilungen (AFS), sodass etwa mehrere betrügerische Überweisungen auf ein bestimmtes Konto schnell zur generellen Sperrung von Transfers zu diesem Zielkonto führen würden. Bei Sparkassen würden sich solche Sperrungen nur regional auswirken und auch deutlich später erfolgen.

Thomas Rienecker, Pressesprecher des Deutschen Sparkassen- und Giroverbands e.V., dem Dachverband der Sparkassen, weist diese Vorwürfe als falsch zurück. Unsere Unterlagen seien nicht aktuell: „Die einzelnen Sparkassen setzen tatsächlich auf einem einheitlichen Sicherheitssystem auf. Die Konfiguration erfolgt zum Großteil zentral.“ „Es gibt bei uns sowohl dezentrale als auch zentrale Einheiten, die sich mit der Betrugs- und Schadensvermeidung befassen.“ Details zu den Systemen oder Standorten könne man aber aus Sicherheitsgründen nicht nennen. Die Betrüger haben dessen ungeachtet weiterhin vor allem Sparkassenkonten im Visier.

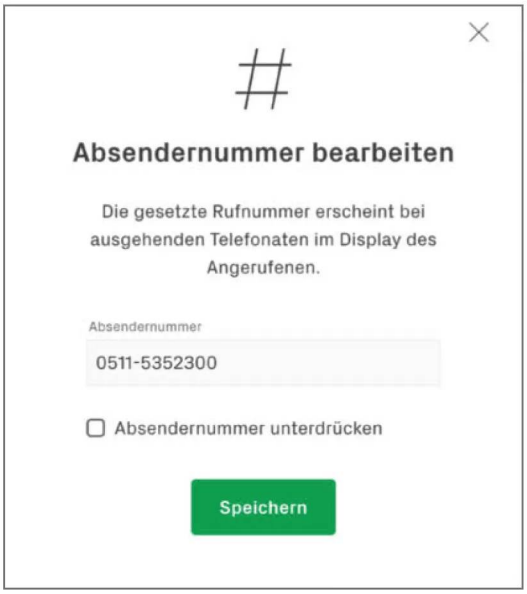
Zahlenzauber

Entscheidend für den Erfolg von Telefonbetrug ist die akribische Vorbereitung. Die erste Pflicht eines (angehenden) Betrügers ist, das sogenannte „Vic“ (Victim, Opfer) so umfangreich wie möglich auszuspähen. Dazu gehören neben Kontostand und Finanzhistorie auch der Name des Kundenberaters und die Telefonnummer der Bank. Mit den eingekauften Login-Daten lassen sich diese Informationen leicht beschaffen.

Eine zentrale Rolle spielt die Telefonnummer der Bank, denn diese dient als Authentifizierungsmerkmal beim späteren Anruf. Die Betrüger nutzen Caller-ID-Spoofing, um einen Anruf der Bank vorzutäuschen. Die zuvor gesammelten Details zu Konto und persönlichen Daten nutzen sie ebenfalls, um dem Opfer vorzuspiegeln, dass es sich um einen authentischen Anruf eines Kundenberaters handelt.

Neu ist, dass diese Anrufe nicht mehr aus dem Ausland kommen, sondern über Telefonprovider in Deutschland. Das liegt an der Verschärfung des §120 TKG (Telekommunikationsgesetz), wonach bei Anrufen aus dem Ausland keine deutschen Telefonnummern mehr übermittelt werden dürfen. Die Kriminellen nutzen deshalb deutsche Voice-over-IP-Anschlüsse (VoIP) für ihre Zwecke. Die Rufnummer zu fälschen ist kinderleicht, dazu genügen meist wenige Klicks im Web-Frontend des VoIP-Providers.

Die Rufnummer zu fälschen ist kinderleicht, praktisch alle VoIP-Provider bieten diese Option. So können Mitarbeiter im Homeoffice unter ihrer Büro-Telefonnummer auftreten – aber auch Telefonbetrüger als Bankberater.



Auf die gleiche Weise änderte auch die Betrügerin, die an das Geld auf dem eigens dafür eingerichteten Lockvogelkonto heranwollte, die Rufnummer des von ihr genutzten VoIP-Anschlusses in die der Sparkasse Osnabrück, als sie bei Maja Helmer anrief. Durch eine Fangschaltung ließ sich die Spur nach Tangermünde in Sachsen-Anhalt zurückverfolgen. Der Anschlussinhaber ist nach unserer Überzeugung jedoch kein Komplize, sondern selbst Opfer einer anderen Betrugsmasche: Er wurde als App-Tester rekrutiert und sollte, so wurde ihm das glaubhaft gemacht, für Banken und Firmen Authentifizierungsverfahren testen.

In Wirklichkeit nutzten die Auftraggeber die im Rahmen dieser vorgeblichen Tests entstandenen Bankkonten und Zugänge für kriminelle Zwecke, darunter auch den VoIP-Anschluss, der bei easybell in Berlin registriert worden war. Einen Hinweis darauf, wo die wahren Täter sitzen, gibt es nicht; einen solchen VoIP-Anschluss kann man von überall auf der Welt benutzen.

Fazit

Allein mit technischen Maßnahmen wie Zwei-Faktor-Autorisierung oder gesetzlichen Vorschriften wie PSD2 lässt sich das Problem Online-Banking-Betrug nicht lösen. Ist ein technisches Verfahren sicher oder zu kompliziert auszuhebeln, dann suchen sich Betrüger eine andere Schwachstelle – und setzen bei den Menschen an.

Die Call-Center-Agenten der Betrüger sind darauf trainiert, die Kontoinhaber unter Druck zu setzen und jede Schwäche gnadenlos auszunutzen; schließlich arbeiten sie auf Provisionsbasis. Dem begegnen Sie am besten, indem Sie skeptisch bleiben und bei Anrufen von der Bank grundsätzlich immer zurückrufen. Denn Telefonnummern sind nur Schall und Rauch, jeder kann sie mit wenigen Mausklicks fälschen. (mid) c't

Präventionsseite
ct.de/wcz1

Vorschau: c't Desinfec't 2023/24

Ab 22. September im Handel und auf ct.de

Das Sicherheitstool der c't-Redaktion ist seit über 15 Jahren im Einsatz und hilft Windows-Nutzern bei einem Schädlingsbefall aus der Patsche. Damit Windows nicht noch mehr Schaden nimmt, startet Desinfec't als eigenständiges Betriebssystem von einer DVD oder einem USB-Stick und prüft aus sicherer Entfernung potenziell verseuchte Systeme. Festplatten untersucht es mit Antiviren-Scannern. Mit Profi-Tools kann man unter bestimmten Voraussetzungen sogar verloren geglaubte Daten wie Abschlussarbeiten retten oder ganze Festplatten klonen.

Weitere Infos: ct.de/wj1z

Themenschwerpunkte

- Desinfec't richtig starten
- Desinfec't anpassen und vielseitig nutzen
- Tipps & Tricks für Desinfec't
- Desinfec't via Btrfs erweitern
- Windows-PCs untersuchen und reinigen
- Hardware-Diagnose mit Desinfec't
- Daten auf Festplatten, SSDs und USB-Sticks retten
- Netzwerk-Forensik mit Desinfec't
- Desinfec't im Netzwerk via PXE booten

Know-How statt Hype

Mit KI-Tools effektiv arbeiten

Heft + PDF mit 29 % Rabatt

Die Nachrichten über revolutionäre KI-Lösungen überschlagen sich täglich. Wie soll man da den Überblick behalten? Mit Tests und Praxistipps erklären wir im c't-Sonderheft, was heute schon geht sowie Ihnen bei der Arbeit hilft und wo Sie den Maschinen noch Zeit zum Reifen geben sollten.

- ChatGPT zwischen wirtschaftlicher Effizienz und menschlichem Wunschdenken
- Bilder-KI Stable Diffusion lokal installieren und betreiben
- Textgeneratoren für jeden Zweck
- Sprachmodelle mit Suchmaschinen koppeln
- Vier KI-Komponisten im Test
- ChatGPT als Hacking-Tool

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-chatgpt