

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 Preisvergleichen 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 zufriedenes „Halali“ für die Schnäppchenjagd und nachhaltige Freude an Ihren On- und Offlinekäufen!

Markus Montz

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.

- 6 Digital einkaufen, aber sicher!
- 10 Onlinekauf-Checkliste Preisvergleich
- 12 Onlinekauf-Checkliste Schnäppchenportale
- 14 Onlinekauf-Checkliste Shop-Auswahl
- 18 Kundenkarten via App digitalisieren

DIGITAL BEZAHLEN

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

- 24 Onlinekauf-Checkliste Bezahlmethoden
- 28 Girocard versus Debitkarten
- 34 FAQ Debitkarten
- 39 Glossar
- 40 Sicher mit dem Smartphone bezahlen
- 46 Zahlen mit dem neuen Giroipay
- 54 FAQ Giroipay
- 58 Sicher bezahlen im 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.

- 62 Womit Kunden immer wieder Ärger haben
- 66 Onlinekauf-Checkliste Reklamation
- 70 Onlinekauf-Checkliste Rückabwicklung
- 72 Kartenabbuchungen rückabwickeln
- 76 PayPal-Schutz bei Privatgeschäften
- 78 Kostenfallen beim „Später zahlen“
- 84 Wie die Schufa Ihre Bonität berechnet





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.

- 92 Fake Shops erkennen und Ärger vermeiden
- 95 Neue Masche beim Kartenbetrug
- 96 Theaterspiel mit Betrugsabsicht
- 102 „Sicher bezahlen“ bei Kleinanzeigen
- 108 PayPal-Betrug auf Kleinanzeigenportalen
- 112 FAQ „Sicheres Bezahlen“ auf Kleinanzeigen
- 116 Telefonbetrug trotz zweitem Faktor

ZUM HEFT

- 3 Editorial
- 53 Impressum
- 122 Vorschau: c't Desinfec't 2023/24

c't SICHER EINKAUFEN
Online-Shopping ohne Probleme

Schützen Sie sich vor Betrug

- 95 Bankkonten und Kreditkarten schützen
- 102 Sicheres Bezahlen auf Kleinanzeigenportalen

Digital bezahlen

- 28, 34, 54 PayPal, Giropay, Karte: Womit bezahlen?
- 58 Probleme im Ausland vermeiden

Kaufprobleme lösen

- 66 Erfolgreich reklamieren
- 76 Käuferschutz richtig einsetzen

Frustfrei shoppen

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

€14,90
CR 047 27-08
ISS 124-08
LSE 1 12-18



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 schief läuft.

Von **Ulrike Kuhlmann**



Bild: Andreas Martini

| | |
|--|----|
| Digital einkaufen, aber sicher! | 6 |
| Onlinekauf-Checkliste Preisvergleich | 10 |
| Onlinekauf-Checkliste Schnäppchenportale | 12 |
| Onlinekauf-Checkliste Shop-Auswahl | 14 |
| Kundenkarten via App digitalisieren | 18 |

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,

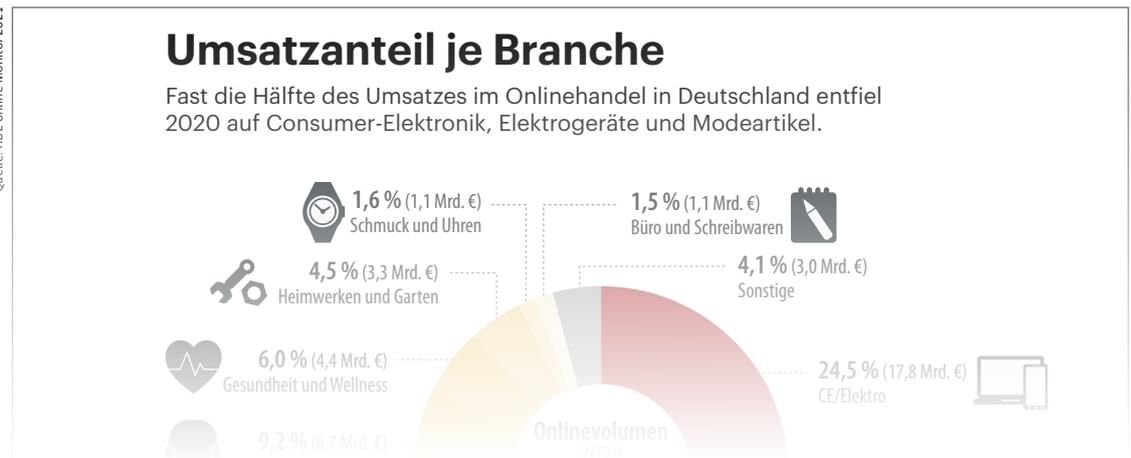
bei wem Sie gerade supergünstig einkaufen wollten. Es gibt betrügerische Shops, die beliebte Ware zum Schnäppchenpreis anbieten, aber nicht beabsichtigen, diese zu liefern. Bei extrem günstigen Angeboten sollten Sie hellhörig werden. Wie Sie gefährliche Fake Shops erkennen und worauf Sie bei der Händlerwahl 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: HfDE online-Monitor 2021



Lesen Sie mehr in c't Sicher einkaufen 2023

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

| | |
|--------------------------------------|----|
| Onlinekauf-Checkliste Bezahlmethoden | 24 |
| Girocard versus Debitkarten | 28 |
| FAQ: Debitkarten | 34 |
| Glossar | 39 |
| Sicher mit dem Smartphone bezahlen | 40 |
| Zahlen mit dem neuen Giropay | 46 |
| FAQ: Giropay | 54 |
| Sicher bezahlen im Ausland | 58 |

Sichere Bezahlfverfahren

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 unsichtbar. 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 Online-

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

Lesen Sie mehr in c't Sicher einkaufen 2023

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**



| | |
|---------------------------------------|----|
| Womit Kunden immer wieder Ärger haben | 62 |
| Onlinekauf-Checkliste Reklamation | 66 |
| Onlinekauf-Checkliste Rückabwicklung | 70 |
| Kartenabbuchungen rückabwickeln | 72 |
| PayPal-Schutz bei Privatgeschäften | 76 |
| Kostenfällen beim „Später zahlen“ | 78 |
| Wie die Schufa Ihre Bonität berechnet | 84 |

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 tau-

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 verteilen, 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

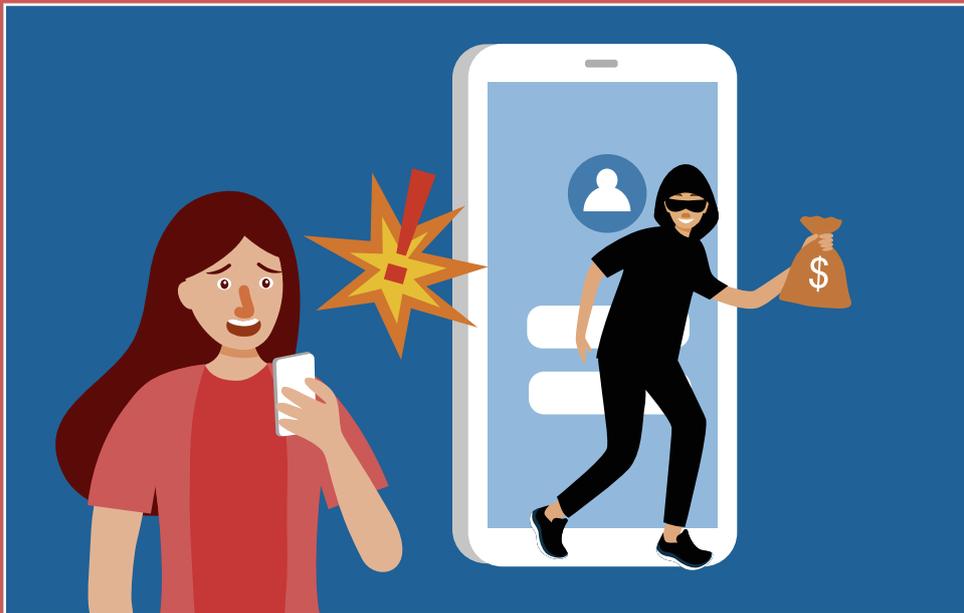
Ein Dauerbrenner sind hingegen scheiternde oder schlecht ausgeführte Garantiereparaturen. Für Ver-

Lesen Sie mehr in c't Sicher einkaufen 2023

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**



| | |
|--|-----|
| Fake Shops erkennen und Ärger vermeiden | 92 |
| Neue Masche beim Kartenbetrug | 95 |
| Theaterspiel mit Betrugsabsichten | 96 |
| „Sicher bezahlen“ bei Kleinanzeigen | 102 |
| PayPal-Betrug auf Kleinanzeigenportalen | 108 |
| FAQ: „Sicheres Bezahlen“ auf Kleinanzeigen | 112 |
| Telefonbetrug trotz zweitem Faktor | 116 |

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 ande-

ständige 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 Widerspruchsbelehrungen 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).

Zahlungsmethoden

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“).

Lesen Sie mehr in c't Sicher einkaufen 2023