



Felix Beilharz



#FAKE-

Warum wir auf Online-Fakes hereinfallen und wie wir uns (und unsere Lieben) davor schützen können

Unser Leben wird immer digitaler. Persönliche Kontakte, der Informationsaustausch, das Versorgen mit Dingen und auch mit Know-how findet zunehmend über die Bildschirme von Smartphones und Computern statt. Geht man in einen Laden, kann man erkennen, dass er echt ist. Spricht man mit einem Menschen von Gesicht zu Gesicht, weiß man ebenso, dass man es mit einer realen, echten Person zu tun hat. Versorgt man sich über Fernsehen oder die Presse mit Informationen, kann man zumindest in Ansätzen sicher sein, dass man dort recherchiert und gegeneinander abwägt, bevor man uns diese Informationen liefert. Dazu mag man sich stellen, wie man mag, aber richtig knallharte Lügen findet man z. B. im Rundfunk wirklich sehr selten. Ganz anderes ist es digital. Heutzutage kann jeder, aber wirklich jeder, für jeden weltweit sichtbar „publizieren“. Jeder mit ein wenig Geschick kann einen Online-Shop aufsetzen, der einer ersten Inaugenscheinnahme standhält. Nicht jeder prüft sofort via Impressum, ob alles mit rechten Dingen zugeht. Nicht jedem fällt auf, dass bei Behauptungen belastbare Quellen fehlen, falsch zitiert sind oder von ebenso dubiosem Hintergrund.

Kurzum: Wir bekommen als Gesellschaft ein Problem durch das Entkoppeln von realer Welt und einem mehr oder weniger großem Teil unseres Lebens. Umso leichter fällt es Betrügern, Bauernfänger und virtuellen Taschenspielern, sich ihre Opfer digital zu suchen. Eine Wahl beeinflussen? Offenbar heute kein Problem mehr. Verschwurbelte „Fakten“ in die Welt zu setzen, dass Milliardäre heimlich Computerchips ins Essen mischen, um uns zu kontrollieren (was sonst sind die schwarzen Punkte im Vanillepudding?), make shit – a hit!

Was können wir dagegen tun? Der renommierte Internet- und Social-Media-Experte Felix Beilharz hat sich dieses Problems großflächig und tiefgängig angenommen und gibt Tipps, auf was man achten sollte und kann, um möglichst wenigen Fakes aufzusitzen.

DER AUTOR



Felix Beilharz ist „einer der führenden Berater für Online- und Social Media Marketing“ (RTL). Sein Profil: 10 Bücher, Seminare und Vorträge in 16 Ländern und über 50 TV-Auftritte.

„Ich? Ich falle doch nicht auf Fakes im Internet rein! Da muss doch ziemlich blöd für sein, mir kann das nicht passieren!“ Genau diese Haltung erlebe ich regelmäßig, wenn es ums Thema „Online-Fakes“ geht.

In meinem eigenen Umfeld habe ich in den letzten Monaten verschiedenste Gegenbeispiele erlebt: Ein Psychologie-Professor teilt eine (eigentlich recht offensichtliche) Fake News, eine promovierte Digitalberaterin fällt auf ein Facebook-Fake-Gewinnspiel rein, ein erfolgreicher Unternehmer in der Nachbarschaft bestellt Luftfilter für sein Haus bei einem Fake-Shop, eine psychologisch und technisch versierte Unternehmensberaterin versenkt 2.000 Euro bei einer Fake-Hotline der Lufthansa – und ich selbst habe in Lockdown-Verzweiflung Kurzhanteln in einem chinesischen Fake-Shop bestellt. Dabei tröstet mich der Gedanke, dass ein recht angesehener Kollege auf den gleichen Shop und sogar das gleiche Produkt hereingefallen ist. All diese Fälle haben eines gemeinsam: Alle Opfer sind überdurchschnittlich medien- und digitalaffin, bestens gebildet und sogar beruflich im Internet tätig. Und trotzdem sind wir Opfer von Fakes geworden.

Ich behaupte: Jede/r ist bereits auf Fakes hereingefallen. Manche haben es nur noch nicht gemerkt. Die Fakes lauern an so vielen Stellen und in so vielen unterschiedlichen Formen, dass niemand verschont bleibt. Und ich glaube sogar, die obige Haltung „Das kann MIR doch nicht passieren“ macht uns besonders anfällig. Denn die Faker und Betrüger machen sich psychologische Trigger zunutze, die in jedem Gehirn greifen – egal ob Akademiker oder Auszubildender, egal ob jung oder alt.

Deswegen: Die Person, die noch keiner Fake News aufgesessen ist, noch nie einer gefakten Bewertung ihr Vertrauen geschenkt, noch nie auf einen Fake-Shop reingefallen ist oder



Abb. 1: Zumindest konnten die vermeintlichen Flüchtlinge ihr Plakat in fehlerfreiem Deutsch verfassen, was für die Kommentatoren eher nicht gilt

die noch nie mit einem Fake-Profil gechattet hat, die möchte ich einmal kennenlernen. Ich vermute, die Auswahl ist sehr rar ...

Doch die gute Nachricht: Wir können etwas dagegen tun. Und vor allem können wir unsere vielleicht weniger digitalaffinen Freunde, Familienmitglieder und Kollegen unterstützen, um sie ebenfalls vor den Gefahren zu schützen.

Warum wir auf Fakes reinfallen

Wenn es stimmt, dass wir alle auf Fakes reinfallen, muss es gute Gründe dafür geben. Und die gibt es tatsächlich. Ich habe im Laufe der Zeit vor allem drei Gründe identifiziert.

1) Wir sind oberflächlich

Ganz ehrlich: Hast du schon mal einen Artikel im Social Web oder auf WhatsApp geteilt, ohne ihn wirklich zu lesen? Einfach, weil dich die Überschrift so getriggert hat? Falls ja, bist du in bester Gesellschaft. Eine Studie der Columbia University hat bereits 2016 ergeben, dass 59 % der Links, die über Twitter geteilt wurden, keinen einzigen Klick erzielen – also nicht mal vom Absender selbst.

Ein interessantes Experiment dazu stammt vom Blog beefing.de (heute frisches-flensburg.de). Die Blogger erstellten einen Artikel mit einem sehr provokanten Open-Graph-Vorschau-Inhalt: Der Title besagt: „Unverschäm! Flensburger Flüchtlinge fordern mehr

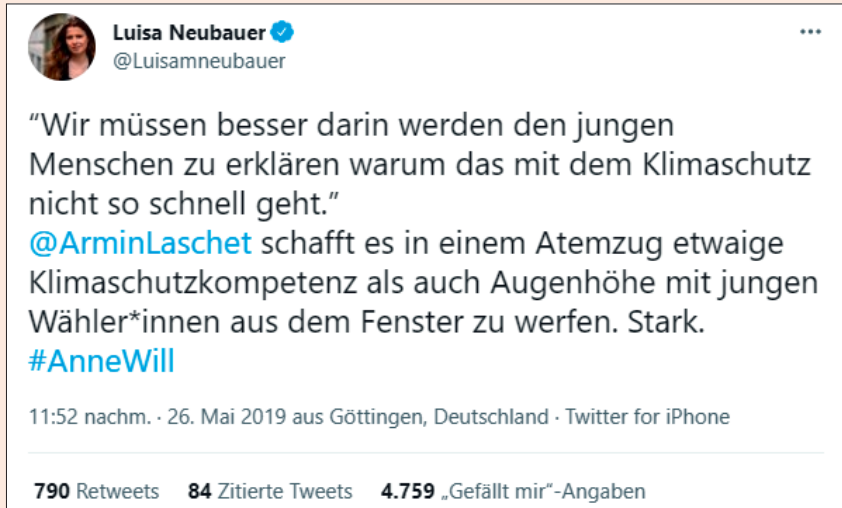


Abb. 2: Ein empörendes Zitat, das so nie gefallen ist

Geld!“ Auf dem Vorschau-Bild waren vier Flüchtlinge vor einem Wohncontainer zu sehen, die ein Plakat mit der Aufschrift „Wir fordern mehr Geld“ in die Höhe hielten.

Im Artikel selbst wird nach zwei Zeilen aufgeklärt, dass es sich um

ein Experiment handelte. Doch offensichtlich reichte für viele Menschen schon das Vorschau-Bild aus, um den Beitrag wütend zu teilen. Über 94.000 Interaktionen erhielt der Artikel auf Facebook, davon allein 23.500 Shares. Dazu kommt eine unbekannte Anzahl

an WhatsApp- und weiteren Messenger-Shares, die ja leider nicht auswertbar sind.

Ein einziger Klick auf die Website und ein paar Sekunden Verweildauer hätten gereicht, um den Fake zu entlarven.

Und selbst wenn wir eine Website oder einen Shop besuchen, nehmen wir uns kaum Zeit, genau hinzuschauen. Viele Besuche dauern nur wenige Sekunden. Dabei könnte man z. B. Fake-Shops meist recht eindeutig entlarven, wenn man sich ein paar Sekunden mehr Zeit nehmen würde. Und auch so manches Angebot oder News erscheinen recht unglaubwürdig, wenn man mehr als einen Blick darauf verschwendet.

Timme Cloud 2.0

Leistung satt!

Flexibel
skalierbar!
Jederzeit.

Die Timme Cloud ist einfach bedienbar und individuell erweiterbar.

Ohne Vorkenntnisse.

Und wann immer Sie wollen!


TimmeHosting
nginx-Webhosting

SSD

100%
GRÜNE
ENERGIE

HOSTING
MADE IN
GERMANY

Mehr Power.
Einfach zu bedienen.

timmehosting.de/cloud-hosting



Abb. 3: Ein jahrtausendealtes Narrativ, das bis heute kursiert

(2) Wir sind medieninkompetent

Das gilt für die Leserschaft der Website Boosting mit Sicherheit weniger als für die breite Allgemeinheit, aber selbst unter uns: Hast du wirklich eine fundierte Ausbildung im Umgang mit Medien genossen? Oder dir mehr oder weniger alles selbst beigebracht? Dann dürfte die „unbewusste Inkompetenz“ groß sein – Dinge, von denen du gar nicht weißt, dass du sie nicht weißt.

Übrigens schieben sich bei diesem Thema gern Jung und Alt den schwarzen Peter zu. Die Jungen lachen über die Alten und ihre oft unbeholfene Art, mit Medien umzugehen. Und die Alten schimpfen auf die Jungen und ihren viel zu sorglosen Umgang mit digitalen Medien. Dabei nehmen sich beide nicht viel. Medienkompetenz wird weder automatisch mit den Lebensjahren erworben noch in ausreichendem Maße in den Schulen vermittelt. Erfahrungsgemäß können junge Nutzer zum Beispiel Werbung nicht mehr von (redaktionellen) Inhalten unterscheiden, dafür fallen ältere Nutzer eher auf Fake News, Spam-Mails oder sonstige Abzocken herein. Es dürfen sich also getrost alle Generationen an die eigene Nase fassen.

(3) Wir sind psychologisch prädestiniert

Wie schon erwähnt: Die Faker und Abzocker nutzen gezielt psychologische Trigger und Verzerrungen. Da ist zum Beispiel der Confirmation Bias, der besagt, dass wir gezielt nach Informationen suchen, die unsere Meinung bestätigen. Und sie gezielt ignorieren, wenn sie uns widersprechen. Der Believe Bias geht in eine ähnliche Rich-

tung: Wir glauben Informationen eher, die unser Weltbild bestätigen.

Hier liegt der Hase im Pfeffer: Wir WOLLEN oft einfach, dass der Fake wahr ist! Die Playstation 5 ist überall ausverkauft, aber in diesem einen Shop ist sie tatsächlich noch zu haben, und zwar 30 % günstiger als Marktpreis? Sollte suspekt klingen, aber ich WILL einfach, dass es stimmt.

Besonders deutlich werden diese Verzerrungen bei politischen Fake News. In den letzten Monaten und Jahren tauchten von jedem Spitzenkandidaten empörende Zitate auf, die eifrig geteilt wurden. Armin Laschet wird von Luisa Neubauer auf Twitter zum Beispiel das Zitat zugeschrieben: „Wir müssen besser darin werden, den jungen Menschen zu erklären, warum das mit dem Klimaschutz nicht so schnell geht.“

Dieses empörende Zitat wurde tausendfach mit entsprechenden Sharepics verbreitet. Dabei hat Armin Laschet das nie gesagt. Aber es würde einfach so wunderbar in manch ein Weltbild passen und so mancher WILL einfach, dass es wahr ist. Zack, der Believe Bias hat zugeschlagen.



Abb. 4: „Die da oben“ lassen es sich gut gehen, während „wir“ eingesperrt werden

Auch die Aussage von Annalena Baerbock, dass die private Tierhaltung aufgrund der hohen CO2-Emissionen von Haustieren ein Ende haben müsse, wurde tausendfach geteilt, entbehrt aber ebenso jeglicher Grundlage. Aber es passt halt so wunderbar in anti-grüne Weltbilder. Und macht uns daher wieder empfänglich für den Fake.

Und von diesen kognitiven Verzerrungen gibt es noch einige mehr. Alle haben eines gemeinsam: Sie machen uns nicht gerade immun gegen Online-Fakes. Egal, wie jung, alt, erfahren oder gebildet wir sind. Dessen müssen wir uns einfach immer wieder bewusst sein.

Fake News

Manche Fakes im Netz sind zwar ärgerlich, aber nicht unbedingt dramatisch. Fake News sind beides – blöd für den, der drauf reinfällt, und existenziell gefährdend für eine Demokratie.

Ausmaß der Fake News

In unserer „aufgeklärten“ und maximal digitalversierten Website-Boosting-Bubble bekommen wir vermutlich gar nicht so wirklich mit, welches Ausmaß Fake News überhaupt annehmen. So manch ein Newsfeed da draußen wird dagegen fast ausschließlich aus Fakes, Lügen und Manipulationen bestehen. BuzzFeed untersuchte 2017 viele Tausend Artikel auf ihre virale Verbreitung

im Social Web (insbesondere auf Facebook). Das Ergebnis: Die acht meistgeteilten Beiträge waren allesamt Fake News. Kein einziger Artikel der großen Medien wie Spiegel Online, Focus oder t-online.de konnte da mithalten. Auch aus den USA sind ähnliche Ergebnisse

zu haben, die regelmäßig Fake News teilt (<https://felixbeilharz.de/studie-fakes/>).

Arten von Fake News

Dabei gibt es ganz unterschiedliche Klassen von Fake News. Nicht alles lässt sich als glatte Lüge einstufen. Der in der BuzzFeed-Analyse meistgeteilte Artikel (von anonymous-news.ru) bezog sich auf eine Studie, dass ungeimpfte Kinder signifikant weniger krank seien. So eine Studie gab es tatsächlich – allerdings wurde sie bereits lange vorher wegen eklatanter Mängel zurückgezogen.

Andere Fake News sind schlichtweg frei erfunden. Auf Platz drei der BuzzFeed-Analyse landete die Meldung, in McDonalds Fleischfabrik sei menschliches Fleisch gefunden worden.

Da hätte es den Zusatz „+++++Bitte Teilen+++++“ eigentlich gar nicht gebraucht, um die Meldung als Blödsinn zu erkennen. Trotzdem erreichte sie 67.000 Interaktionen auf Facebook.

Und wie so oft bei Fake News ist die Meldung alt (die älteste Quelle, die ich gefunden habe, stammt von 2014) und kursiert auch 2021 immer noch munter im Netz.

Wieder andere Fake News fallen in die Kategorie „Irreführender Kontext“. Auch hier wird ein wahrer Kern verbreitet, jedoch in einem völlig falschen Zusammenhang, wodurch der Fake entsteht. Gerade Bilder tauchen in dieser Kategorie sehr oft auf.

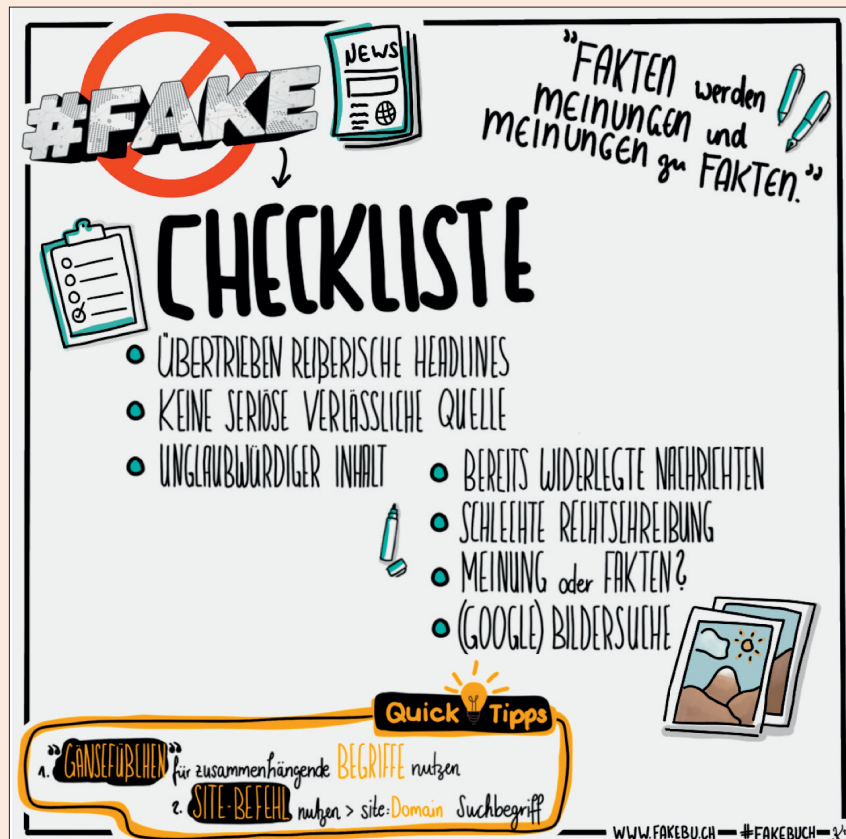


Abb. 5: Checkliste Fake News (Design by Isabel Kulesa)

bekannt: Die meistgeteilten Fake News werden häufiger geshart als die meistgeteilten realen Nachrichten.

In der Studie „Infodemie“ der Vodafone-Stiftung von 2020 gaben 76 % der deutschen Jugendlichen an, mindestens wöchentlich mit Fake News im Netz konfrontiert zu sein, 21 % sogar mehrmals täglich. Beide Prozentzahlen steigen seit Jahren zweistellig pro Jahr.

Eine eigene Umfrage stützt diese Tendenz. 88,7 % der Befragten gaben an, in den letzten sechs Monaten mindestens eine Fake News im Social Web gesehen zu haben. Und 61,1 % berichten sogar, im eigenen Freundes- oder Familienkreis mindestens eine Person











 <p>Amazon Bewertungen ab 19,40 € pro Bewertung Einzelpreis: 22,95 €</p>	 <p>Google Bewertungen ab 9,72 € pro Bewertung Einzelpreis: 12,95 €</p>	 <p>Facebook Bewertungen ab 9,72 € pro Bewertung Einzelpreis: 12,95 €</p>
 <p>App Bewertungen ab 9,72 € pro Bewertung Einzelpreis: 12,95 €</p>	 <p>Tripadvisor Bewertungen ab 12,60 € pro Bewertung Einzelpreis: 14,95 €</p>	 <p>Trustpilot Bewertungen ab 12,60 € pro Bewertung Einzelpreis: 14,95 €</p>
 <p>Arbeitgeber Bewertungen ab 12,60 € pro Bewertung Einzelpreis: 14,95 €</p>	 <p>Jameda Bewertungen ab 15,31 € pro Bewertung Einzelpreis: 16,95 €</p>	 <p>HolidayCheck Bewertungen ab 15,31 € pro Bewertung Einzelpreis: 16,95 €</p>
 <p>Kostenlose Testbewertung für Neukunden gratis</p>		

Abb. 6: Beim vermutlichen Marktführer FIVESTAR MARKETING sind Bewertungen für jede größere Plattform zu haben

Wie so viele Fakes wurden auch irreführende Bilder im Rahmen der Corona-Pandemie massenweise verbreitet. Im Dezember 2020 ging zum Beispiel ein Bild einer illustren Reihe von Politikern viral, die gemütlich bei einem Glühwein zusammenstehen, während das Volk im Shutdown eingesperrt ist. Da kann man sich schon mal aufregen. Das heißt, man könnte, wenn das Bild nicht aus dem Dezember 2019 stammen würde und damit deutlich VOR der Pandemie.

Darüber hinaus gibt es noch zahlreiche weitere Formen der Fake News. Von manipulierten Bildern bis hin zu Deepfake-Videos, die uns in Zukunft noch größere Probleme machen werden, ist alles dabei.

Fake News erkennen

Auch ohne abgeschlossenes Studium der Medienwissenschaften sollte es möglich sein, die meisten Fake News recht schnell als solche zu entlarven. Allein schon eine gewisse Skepsis und das Wissen über den Believe Bias machen uns weniger anfällig. Wenn eine Nachricht einfach ZU gut in das eigene Weltbild passt, sollten wir zumindest mal nachprüfen, ob es sich vielleicht um eine Fake News handeln könnte. Praktisch kann das so aussehen:

- » Stammt die Nachricht von einer anerkannten, verlässlichen Quelle

oder von einer völlig unbekanntem, eher dubios anmutenden Seite?

- » Bezieht sich die Nachricht auf nachprüfbar Primärquellen? Werden solche Quellen verlinkt und sind diese ihrerseits glaubwürdig?
- » Was taucht auf, wenn du mal nach Stichwörtern aus der Nachricht googelst? Wurde die Nachricht bereits widerlegt? Gibt es andere Fundstellen, die die Nachricht stützen?
- » Entspricht die Gestaltung der Nachricht insgesamt journalistischen Maßstäben (Rechtschreibung, gemäßigter Tonfall, Trennung von Fakten und Meinung)?

Diese kleinen Tipps, verbunden mit der angesprochenen Selbstkritik und Skepsis, dienen uns schon als recht gutes Werkzeug, um nicht mehr auf Fake News hereinzufallen.

Fakes im E-Commerce

Für die Website-Boosting-Leser wird diese Fake-Kategorie sicherlich die geläufigste sein. Der Online-Handel boomt und mit ihm natürlich auch Betrug, Abzocke und Schindluder aller Art. Hier werden die Folgen der Fakes auch konkret im eigenen Geldbeutel spürbar. Während Fake News eher die Gesellschaft und Demokratie im Ganzen aushöhlen, langsam und schleichend, leidet der Einzelne unter den folgenden Fakes direkt und unmittelbar.

Fake-Bewertungen

Ganz ehrlich: Bevor ich für die Buch-Recherche richtig tief in das Thema eingestiegen bin, habe ich Bewertungen doch recht stark vertraut. Klar weiß man irgendwo im Hinterkopf, dass ein Teil der Bewertungen gekauft oder manipuliert ist, aber so insgesamt wird sich das doch in der Summe egalisieren.

Heute weiß ich: Nein, tut es nicht. Es ist äußerst einfach, Fake-Bewertungen zu erstellen (oder zu erhalten). Und das Ausmaß ist erschreckend. Experten schätzen, dass zwischen 30 und 42 % der Amazon-Bewertungen gefälscht sind. Allerdings sind die Fake-Bewertungen nicht gleich verteilt. Dazu später mehr.

Der Grund, warum gerade hier so viel gefakt wird, ist einfach: Kaufentscheidungen hängen ganz entscheidend von Bewertungen ab. 65 % der Befragten gaben in einer Bitkom-Studie an, dass Online-Bewertungen für sie das wichtigste Entscheidungskriterium im Online-Shopping überhaupt seien. Andere Studien bescheinigen den Bewertungen einen höheren Einfluss als der Unternehmenswebsite oder gar dem direkten Kontakt zum Unternehmen.

Bei den gefakten Bewertungen lassen sich grob zwei Kategorien unterscheiden: Bewertungen von Bots und solche von echten Menschen, die aber für ihre Bewertung eine Gegenleistung erhalten haben. Mit der ersten Kategorie

brauchen wir uns nicht allzu sehr zu beschäftigen. Hier geben sich die Plattformen größte Mühe, solche Bewertungen zu erkennen und zu löschen.

Schwieriger wird das bei menschlich erstellten Reviews. Auch hier gibt es im Prinzip zwei Methoden: das direkte Generieren von Bewertungen (vor allem für Amazon-Produkte) und den Bewertungskauf über Dienstleister, die Pakete verschiedener Größen anbieten.

Letztere beschränken sich nicht nur auf Amazon. Für nahezu jede Plattform, die Bewertungen integriert, lassen sich Pakete kaufen: Google, die App-Stores, Kununu, Jameda, Tripadvisor, HolidayCheck, Lieferando, OTTO und viele mehr. Je nach Anbieter gehen die Bewertungen bei wenigen Euro Einkaufspreis los, je größer das Paket, desto günstiger. 100 Fünf-Sterne-Bewertungen für Google sind bereits für 699 Euro zu haben.

Der Markt für solche Bewertungshändler ist undurchschaubar. Viele der Dienstleister gehören zum gleichen Anbieter und viele weitere treten nur als Reseller unter eigener Marke auf. Ja, es stimmt: Es gibt auch im Bewertungshandel eine Art Dropshipping und Reseller-Markt.

Diese Bewertungen werden letztlich von freiberuflichen Autorinnen und Autoren verfasst, die sich für ein paar Euro pro Bewertung etwas Schönes ausdenken. Also eine Art Textbroker für Fake-Bewertungen.

Zumindest bei Amazon entsteht dabei aber ein Problem: Hier will man ja die vertrauenswürdigen „verifizierten Käufe“ für die Bewertungen (übrigens schreibt sogar die Bundesregierung auf ihrer Website: „Verifizierter Kauf steht für Seriosität ...“). Und auch dafür gibt es natürlich eine Menge Agenturen, die das sogenannte „Cash Back“-Verfahren anbieten. Soll heißen: Du kaufst das Produkt bei Amazon, schreibst deine Rezension und bekommst dann dein Geld zurück. Das Produkt darfst du behalten.

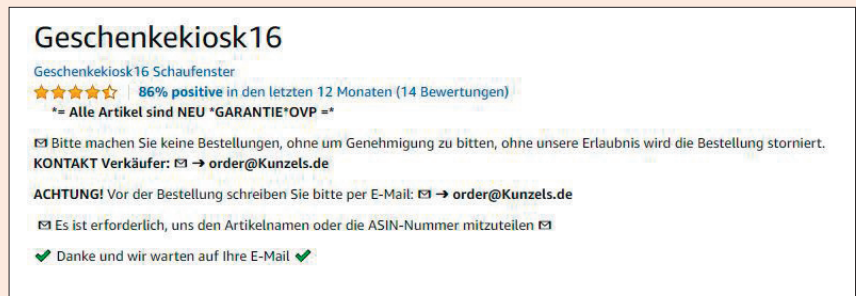


Abb. 7: Echter Amazon-Händler, allerdings übernommen von einem Betrüger

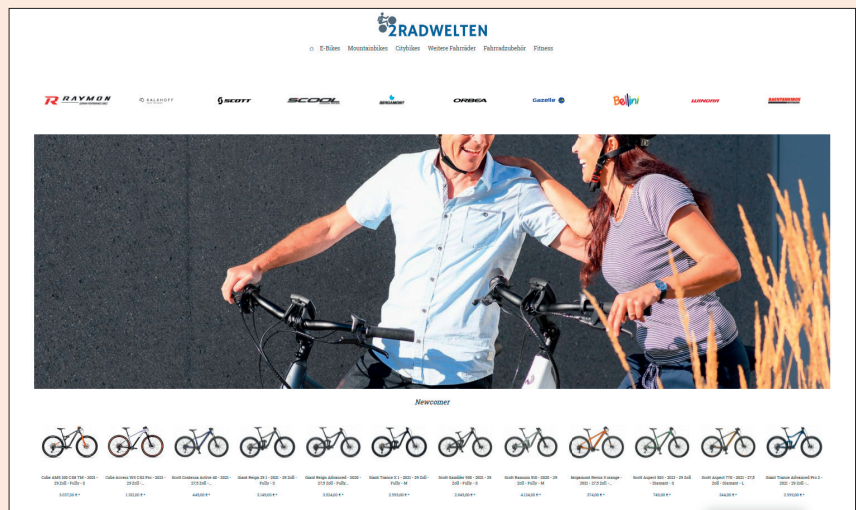


Abb. 8: 2RadWelten.de sieht aus wie echt – ist aber einfach ein gut gemachter Fake-Shop

Kann das wirklich so einfach sein? Das wollte ich ausprobieren. Wer nicht auf einen Dienstleister oder eine Agentur setzen will, findet bei Facebook und Telegram genug Angebote. Die Gruppen heißen „Deutschland Produkttester Amazon“ oder „Produkttester Deutschland AMAZON EBAY“ und haben alle das gleiche Prinzip: Händler oder sogenannte „Agenten“ stellen dort ihre Produkte ein, entweder direkt mit Link oder mit der Aufforderung, selbigen per DM zu erfragen. Der Rest läuft dann nach dem obigen Schema. Kauf, Review, Geld zurück.

Und in diesen Gruppen ist ganz schön was los. Teilweise werden über tausend Produkte pro Tag in diesen Gruppen gepostet, aus denen die Bewerter auswählen können. Dabei muss man gar nicht unbedingt selbst aktiv werden – als ich in einige dieser Gruppen eintrat, hatte ich unmittelbar einige Dutzend DM in meinem Postfach

von „Agenten“, die mir freundlich in mittelmäßigem Englisch oder Deutsch ihre Produkte anboten. Einige der Anbieter schickten mir über 100 Bilder ihrer Produkte, aus denen ich auswählen konnte.

Das genaue Ausmaß der Fake-Bewertungen lässt sich nur erahnen. Analysen verschiedener Hochschulen und Medien zeigen aber: Betroffen sind weit überwiegend chinesische Billig- und No-Name-Produkte, kaum bekannte Marken. Von daher scheinen sich Marken doch wieder als Qualitätsanker zu etablieren – bei mir haben die Recherchen zum Buch jedenfalls diesen Effekt gehabt.

Wenn also die No-Name-Küchenschere über 3.000, der Billig-MP3-Player fast 4.000 und das markenlose Küchen-Schneidebrettchen über 1.500 Bewertungen hat (alles reale Beispiele von Produkten mit gefakten Bewertungen) – bleib skeptisch. Und gib im Zweifel lieber drei Euro mehr aus.

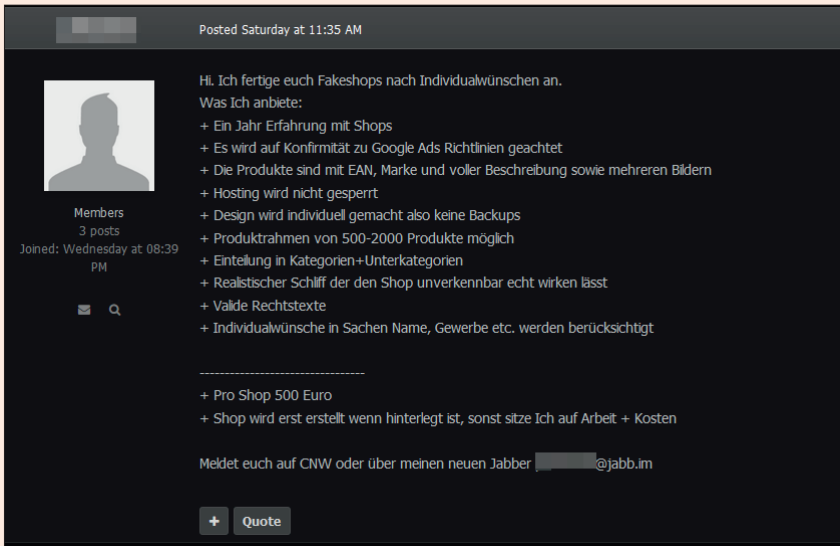


Abb. 9: Fake-Shop-Angebot im Darknet – fix und fertig für 500 Euro

Tool-Tipp: www.reviewmeta.com rechnet die Fake-Bewertungen soweit möglich aus der Gesamtzahl raus und gibt eine realistische Gesamtbewertung von Amazon-Produkten an.

„Gehackte“ Amazon-Shops

Eine andere Kategorie der Fakes findet überwiegend bei Amazon statt. Auch auf diesen Fake bin ich um ein Haar hereingefallen. Und auch hier war wieder Corona schuld. Beim ersten Lockdown wollte ich, wie so viele, mein kleines Homegym aufrüsten und suchte nach einem passenden Crosstrainer. Klappbar sollte er sein und eine hohe Schwungmasse aufweisen. Im dreistelligen Preisbereich gibt es da genau ein Produkt: den MAXXUS CX 4.3F. Kostet allerdings 899 Euro. Also machte ich mich auf die Suche nach Schnäppchen. Nach ein paar Stunden Recherche war klar: Fehlanzeige. Das Ding gibt es nirgendwo billiger.

Huch, außer bei Amazon. Von einem Händler, neu und für starke 450 Euro. Da musste ich einfach zuschlagen. Leider währte die Freude nur wenige Minuten, da die Bestellung vom Händler storniert wurde. Also direkt noch mal bestellt – und wieder storniert. Was war da los? Ein Blick auf das Händlerprofil schaffte schnell Klarheit – der Account wurde offenbar von

Betrü gern gehijackt, also übernommen.

Die Masche ist dabei recht simpel: Die Faker verschaffen sich Zugang zu einem seriösen, aktiven Händleraccount, zum Beispiel durch eine Phishing-E-Mail oder ein leicht zu erratendes Passwort. Schon haben Sie Zugriff auf einen echten Account mit vielleicht schon Dutzenden oder Hunderten positiver (echter) Bewertungen.

Nun laden sie massenweise Produkte hoch. Das können schnell mal mehrere Tausend neue Produkte in wenigen Stunden sein. Dabei orientieren sich clevere Betrüger natürlich an Produkten und Kategorien, die stark nachgefragt sind – Bastelbedarf, Haushaltstechnik oder eben Sportgeräte zum Lockdown. Die Preise sind dabei so attraktiv, dass Otto Normalonlineshopper nicht lange nachdenkt, sondern zuschlägt.

Und jetzt kommt der Clou: Die Bestellungen werden storniert, verbunden mit dem Hinweis, dass man bitte die Verfügbarkeit erst per Mail abklären solle. In dieser Mail werden dann Kontaktdaten abseits Amazon genannt, auf die das Geld überwiesen werden solle.

Ich hatte im Rahmen der Buchrecherche die Gelegenheit, mit einem Amazon-Händler zu sprechen, dessen Konto ebenfalls auf diese Art missbraucht wurde. Innerhalb von nur einer Stunde gingen 3.500 Bestellungen bei

ihm ein! Wenn nur 1 % der Besteller letztlich auch bezahlt, macht das bei Produktpreisen von durchschnittlich 300–500 Euro einen schönen Stundenlohn ...

Fake-Shops

Eine der größten Gefahren für Otto und Olga Normalonlineshopper/in dürfte in den Fake-Shops liegen, die an jeder Ecke aufploppen. Und leider sind die Faker auch hier in den letzten Jahren immer besser geworden. Während der beste Ratschlag vor wenigen Jahren noch lautete: „Prüfe, ob der Shop ein Impressum hat“, oder: „Werde misstrauisch, wenn zu viele Rechtschreibfehler in den Texten enthalten sind“, muss man heute schon SEHR genau hinschauen, um einen Fake-Shop als solchen zu erkennen.

Die gut gemachten Fake-Shops haben nicht nur einen gut klingenden Domainnamen, SSL-Verschlüsselung und ein seriöses Layout, sondern auch sonst alles, was zu einem regulären Online-Shop gehört: Impressum, Datenschutzhinweise, Cookie Consent, AGB und Widerrufsbelehrung, teilweise sogar Newsletter, Partnerprogramm und Sendungsverfolgung. Wer also nach solchen Signalen sucht, wiegt sich schnell in falscher Sicherheit.

Wie kann man also einen Fake-Shop erkennen, wenn die so gut gemacht sind? Ein paar Hinweise gibt es dann doch, an denen man die Fakes meistens erkennt:

- » Wenn eine Service-Telefonnummer angegeben ist, einfach mal anrufen. Bei Fake-Shops führt die in der Regel ins Leere oder zu einem falschen Anschluss.
- » Oft bauen die Fake-Shops Social-Media-Icons in den Footer oder Header ein, wie es ein regulärer Shop auch tun würde. Die Links führen dann aber nicht zum jeweiligen Auftritt im Social Web, sondern ins Leere.

- » Sind Siegel wie Trusted Shops oder eKomi angegeben? Dann mal draufklicken und prüfen, ob die Siegel mit den Profilen auf der Plattform verlinkt sind. Faker bauen nur die Bilder ein, legen normalerweise aber kein Profil bei dem jeweiligen Dienst an.
- » Ein wichtiges Warnsignal sind auch die Zahlungsmethoden. Fake-Shops bieten meist nur die Möglichkeit der Vorkasse an. Mittlerweile auch auf deutsche Konten, also fällt das Warnsignal „Konto im Ausland“ weg. Trotzdem sollte man bei Shops, die ausschließlich per Vorabüberweisung bezahlt werden wollen, vorsichtig sein. Es muss natürlich kein Fake sein, die Gefahr ist aber größer. Aber auch das alleine ist kein sicherer Weg mehr: Ich habe Fake-Shops gesehen, die neben Vorkasse auch Zahlung per Kreditkarte anbieten. Die Kreditkartenzahlung funktioniert dann zwar nicht und die meisten Besteller werden auf Vorkasse umswitchen, aber schon das Angebot der zweiten Zahlungsmethode „legitimiert“ den Shop. Also auch hier: Augen auf.

Alle diese Signale sind wichtig, aber nicht 100%ig sicher. Deshalb rate ich immer dazu: Wenn man bei einem unbekanntem Shop bestellen will, erst einmal kurz googeln. Den Shop-Namen, die Domain, die Angaben im Impressum. Bei Fake-Shops findet sich sehr oft bereits ein Hinweis auf einer Liste der Verbraucherschutzeinrichtungen oder ein Eintrag in einem Forum, in dem sich Geschädigte austauschen. Das ist momentan die wohl sicherste Methode, Fake-Shops zu erkennen (zumindest, wenn sie bereits als solche aufgeflogen sind).

Wer sich fragt, wo solche Fake-Shops eigentlich herkommen: Wie so oft lautet die Antwort „Darknet“. Hier gibt es Foren, in denen Fake-Shops fix und fertig zum Kauf angeboten werden.

Es gibt kaum einen besseren Ort für Fakes als das Social Web, wo sich jeder Deutsche fast 1,5 h pro Tag aufhält. Dement-

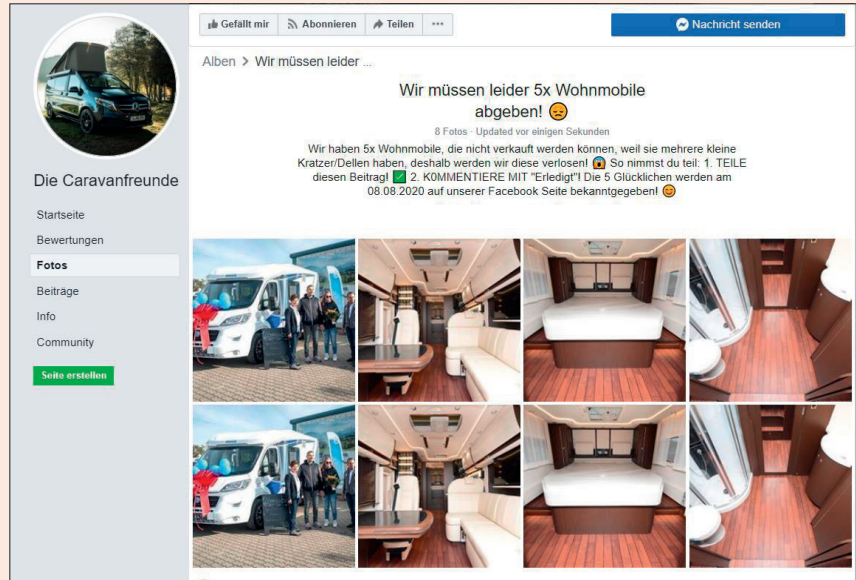


Abb. 10: 259.282 Shares dürfte in eine hohe Millionen-Reichweite münden

Laut Beschreibung der Anbieter sind diese Shops in weniger als 60 Minuten völlig ohne Programmierkenntnisse fertig eingerichtet und umfassen bis zu 20.000 Produkten – auf Kundenwunsch gibt es sogar „Spezialanfertigungen“ mit bis zu einer Million Produkten. Das ist dreimal so viel, wie *AboutYou.de* gelistet hat ... Kostenmäßig geht ein Fake-Shop mit einigen Hundert Produkten schlüsselfertig eingerichtet schon bei 500 Euro los. Das teuerste Angebot, was ich gesehen habe, war ein Shop mit vier Millionen Produkten, da lagen die Kosten dann bei 10.000 Euro in der Erstellung und 2.000 Euro monatlicher Shop-Miete. Dafür hat man dann aber auch einen Fake-Shop, der etwa viermal so groß wie *Mediamarkt.de* ist.

Fakes im Social Web

Es gibt kaum einen besseren Ort für Fakes als das Social Web, wo sich jeder Deutsche fast 1,5 h pro Tag aufhält. Dement-

sprechend groß ist hier die Bandbreite und Anzahl an Betrügereien, Lügen und Falschhalten. Fake News werden überwiegend über das Social Web verbreitet. Und auch die bereits angesprochenen Fake-Shops finden ihre Opfer häufig über Facebook und Co. Teilweise schalten die Fake-Shops sogar

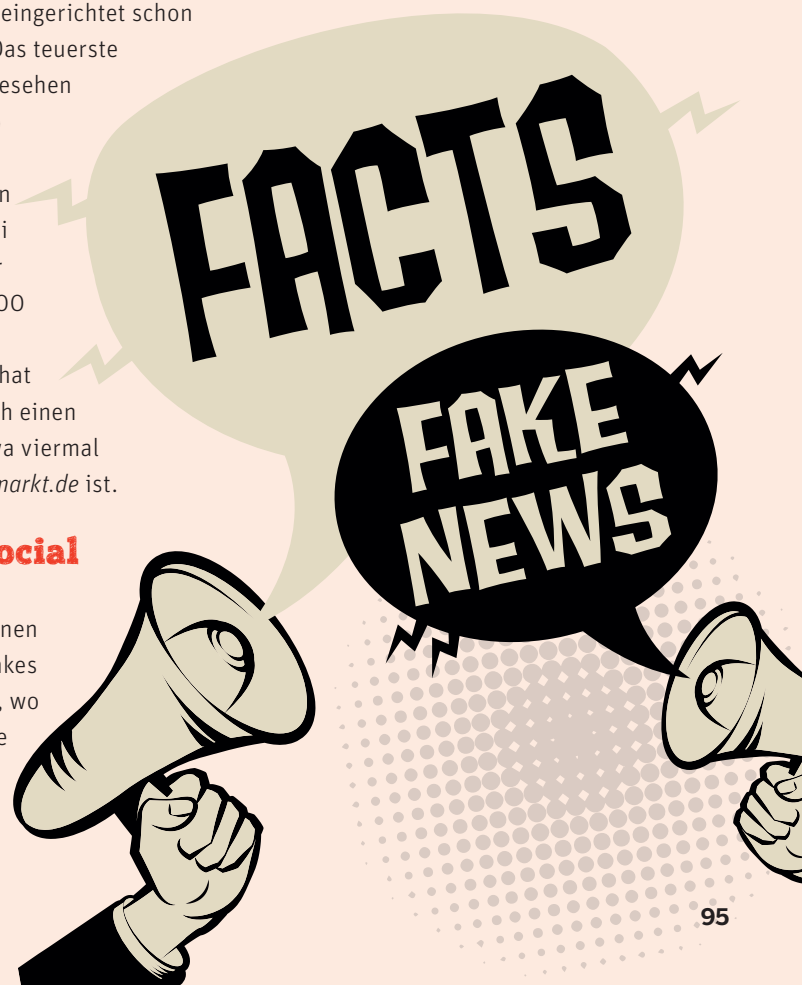




Abb. 11: Eine verifizierte Seite macht Werbung für Abnehm-Spam?

Facebook Ads – das Geschäft scheint sich also zu lohnen.

Im Folgenden gehe ich auf eine kleine Auswahl der Social-Media-Fakes ein – im Buch sind natürlich noch deutlich mehr erklärt.

Fake-Gewinnspiele

Dieses Phänomen tritt, wie die anderen auch, überwiegend auf Facebook auf, mittlerweile jedoch auch bei Instagram und sogar TikTok. Das Schema ist meistens gleich: Es wird ein tolles Produkt verlost, das viele Menschen unbedingt haben wollen. Paradebeispiele dafür sind das Traumauto mit der roten Schleife auf der Motorhaube, das Tiny House, der Traumurlaub, aber auch technische Geräte oder einfach eine tolle Kaffeemaschine.

Die Faker legen eine neue Facebook-Seite an, die meistens eine bekannte Marke nachahmt. Bei genauerem Hinsehen wäre der Fake schnell zu durchschauen, aber wie wir bereits festgestellt haben – so ticken wir einfach nicht. Oft wird das Gewinnspiel auch durch einen nachvollziehbaren Grund legitimiert, zum Beispiel ein Jubiläum, beschädigte Verpackungen oder unverkäufliche Rücksendungen.

Die Teilnehmenden müssen nun in der Regel das Gewinnspiel teilen und kommentieren. Das eigentliche Ziel (neben der durch die Shares erzeugten Reichweite) liegt meist aber im Gewinnen von verifizierten Leads. Das passierte früher einfach durch einen Link im Gewinnspiel-Text, den man anklicken und das dortige Formular ausfüllen sollte. Heute gehen die Faker

etwas cleverer vor: Oft wird man aufgefordert, mit einem bestimmten Wort zu kommentieren, zum Beispiel die Wunschfarbe des Traumaautos. Durch den Kommentar wird dann ein Chatbot getriggert, der jedem Teilnehmenden automatisch eine Direktnachricht mit dem Link zuschickt. So ist „von außen“ kaum zu erkennen, welches Ziel hinter der Aktion steckt.

Da fällt doch niemand drauf rein, oder? Leider falsch gedacht – ich habe in den letzten Jahren ziemlich viele Beispiele gesammelt, die hohe fünf- oder gar sechsstelligen Shares erhalten haben.

Die so generierten Leads können dann gewinnbringend verkauft werden. Je nach Branche, Menge und Qualität lässt sich ein solcher Datensatz für 0,2 €–2 € verkaufen. Gehen wir mal davon aus, dass nur 10 % der Leute, die das Gewinnspiel in Abbildung 10 geteilt haben, auch den Datensatz ausgefüllt haben, dann haben die Betrüger auf jeden Fall einige Tausend Euro, vielleicht sogar gut fünfstellig, damit verdient.

Solche Fake-Gewinnspiele sind sehr einfach zu durchschauen:

- » Sie finden meist auf einer frisch angelegten Seite ohne Historie statt; oft ist das Gewinnspiel der erste Post überhaupt.
- » Viele der Seiten täuschen eine Markenseite vor (REWE, Aldi, BMW etc.) – es handelt sich aber nie um die echte Seite mit blauem Haken.
- » Das Versprechen ist oft sehr unrealistisch. Entgegen der Behauptung in Abbildung 10 werden teure Wohnmobile nicht einfach verschenkt, wenn sie „kleine Kratzer/Dellen“ haben.
- » Es fehlen meist alle relevanten Teilnahmebedingungen, Impressum etc. Allerdings haben manche Faker hier bereits nachgebessert und liefern diese Informationen, um das Gewinnspiel echt aussehen zu lassen.

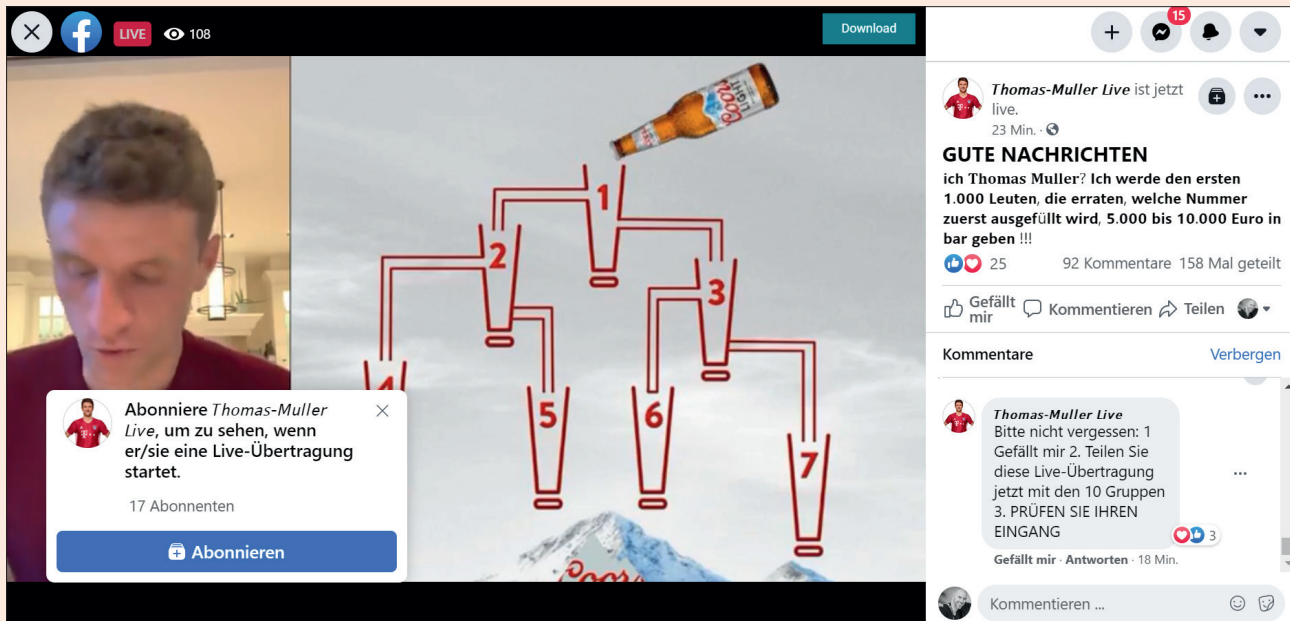


Abb. 12: Thomas-Muller Live – seems legit

- » Oft zeigt der Bearbeitungsverlauf des Beitrags, dass mehrfach Änderungen vorgenommen wurden, z. B. geänderte Bedingungen oder ein verschobenes Enddatum.
- » Der Link, unter dem man das Formular ausfüllen soll, hat nichts mehr mit dem angeblichen Unternehmen zu tun.

Fake-Anzeigen

Die meisten Online-Nutzerinnen und -Nutzer kennen dubiose Werbeanzeigen vor allem aus den Native-Advertising-Sektionen unter Artikeln diverser Portale. Da wird dann gern „dieses eine Lebensmittel“ angekündigt, das „deinen Bauch schmelzen lässt“. Ähnliches passiert auch im Social Web, aber mit einem anderen Hintergrund, der für uns Marketer wiederum sehr interessant ist.

Dieser Fake tritt überwiegend in zwei Arten auf: in Form von Abnehmtropfen und in Form von dubiosen Krypto-Investments. Eines haben beide gemeinsam: Sie werden von den Stars aus „Die Höhle der Löwen“ promotet. In der Abnehm-Anzeige hält Judith Williams ein Fläschchen „K2“-Tropfen oder ähnliche Abnehmwunder hoch, in der anderen Anzeige empfiehlt Frank Thelen eindringlich, sich die Investment-Revolution genauer anzuschauen. Oder

jede andere beliebige Kombination.

Das Kuriose dabei ist, dass die Ads (wieder meist auf Facebook) von eigentlich seriösen Seiten verbreitet werden, teilweise sogar mit blauem Haken verifiziert. Wie kann das sein?

Hier passiert Ähnliches wie bei den Fake-Produkten auf Amazon. Betrüger übernehmen Facebook-Seiten seriöser Unternehmen. Meist passiert das über Phishing-Links, die zum Beispiel in Direktnachrichten verschickt werden. Der Vorwand ist zum Beispiel ein angeblicher Urheberrechtsverstoß, der geprüft werden sollte, oder – noch cleverer – die Behauptung, dass man für den blauen Haken berechtigt sei und diesen nun beanspruchen könne. Klickt das Opfer auf den Link, landet es auf einer nachgemachten Facebook- oder Instagram-Log-in-Seite. Auch diese könnte man mit etwas genauerem Hinschauen schnell entlarven, aber das hatten wir ja schon. Gibt man nun dort seine Zugangsdaten ein (und hat keine 2-Faktor-Authentifizierung aktiviert), ist das Profil futsch – und damit auch die Seite und vielleicht sogar der Werbeanzeigenmanager.

Nun schalten die Betrüger ihre Werbung „auf deinen Nacken“, so lange, bis der Schwindel auffällt. Ich habe im Rahmen der Buchrecherche Dutzende

solcher Fälle gesehen – von kleinen lokalen Unternehmen bis hin zu einem Bundesliga-Profi, dessen Konto ebenfalls für diese Masche missbraucht wurde. In Abbildung 11 ist es übrigens ein verifiziertes peruanisches Immobilienunternehmen, die mir das Abnehmwunder anpreist.

Der Vollständigkeit halber: Klickt man auf den Link in der Ad, landet man auf einer Landingpage, die einen Newsartikel nachahmt, z. B. von CNN, USA Today oder MSN. Dort wird dann eine ausführliche Story erzählt, im Falle der Abnehmtropfen zum Beispiel über die angeblichen Erfinderinnen und ihre Erfolgsstory bei „Die Höhle der Löwen“, die alle Löwen so dermaßen begeistert hat, dass es kaum zu glauben war. Untermauert mit zahlreichen Testimonials berühmter Persönlichkeiten, die mit diesen Tropfen rank und schlank geworden sind. Bestellt man die Tropfen dann, erhält man irgendwas zwischen nichts und Fläschchen mit undeklariertem Inhalt unbekannter Herkunft, die ICH mir jedenfalls nicht einverleiben würde.

Im Falle der Krypto-Investments läuft es ganz ähnlich, nur dass eben auf die enormen Gewinnmöglichkeiten mit der geheimen Blockchain-Methode hingewiesen wird. Dahinter stecken dann

meist Investment Scams oder Pyramidensysteme – ebenfalls nichts, wo ich mein Geld hineinpacken würde ...

Wie kann man sich als Unternehmen vor solchen Fakes schützen? Generell gilt: Für alle Dienste wie Facebook, Instagram, Google und Co. die 2-Faktor-Authentifizierung aktivieren (die direkten Links aller relevanten Dienste habe ich auf <https://fakebu.ch> zusammengestellt). Und zweitens: Genau prüfen, wo man seine Zugangsdaten eingibt. Handelt es sich WIRKLICH um die Domain instagram.com? Oder taucht instagram.com vielleicht in der Domain auf, aber nur als Subdomain oder Tippfehler-Variante? Hier können zehn Sekunden genaues Hinschauen eine Menge Ärger ersparen.

Fake-Livestreams

Den letzten Fake aus dem großen Sammelsurium der Online-Fakes habe ich für diesen Artikel ausgewählt, weil er erstens recht neu ist und zweitens eine clevere Weiterentwicklung und Zusammenführung verschiedener bewährter Online-Marketing-Methoden.

Die Rede ist von Fake-Livestreams. Hier mischen die Faker wirklich alles zusammen. Aber der Reihe nach.

Primär scheint dieses Phänomen auf Facebook



TIPP



Wer tiefer in das Thema einsteigen möchte, dem sei das Buch **#FAKE** von Felix Beilharz (ISBN: 978-3969668108) empfohlen. Es ist seit Juli gebunden für 20,- € im Fachhandel erhältlich (Kindle-Version 16,90 €).

und TikTok aufzutreten. Ähnlich wie bei den Fake-Gewinnspielen legen die Betrüger eine Seite an, die vorgibt, eine berühmte Persönlichkeit zu sein, zum Beispiel ein Sportler oder eine Musikerin.

Dann startet die Seite einen Livestream (bei Facebook geht das ja direkt, bei TikTok müsste man 1.000 Follower haben, weshalb etwas Vorarbeit nötig ist oder einfach das Übernehmen eines Accounts nach dem gerade beschriebenen Muster). Der Livestream besteht

aus dem Abspielen eines Videos, das der/die Prominente selbst einmal gepostet hat. In Abbildung 12 ist das Beispiel einer gefakten

Thomas-Müller-Seite zu sehen. Und hier wird auch gleich der nächste Mechanismus klar: Neben den Livestream wird eines der von Facebook bekannten Rätsel präsentiert.

Das Lösen des Rätsels ist dann Voraussetzung für die Teilnahme am Gewinnspiel.

Der Rest läuft analog zu den Fake-Gewinnspielen: Kommentar abgeben, Chatbot springt an, Link zur Leadgen-Seite kommt. Interessant sind hier aber die Bedingungen, die laut erstem Kommentar über den üblichen Like hinaus noch gestellt werden: „Teilen Sie diese Live-Übertragung jetzt mit den 10 Gruppen.“ Das ist schon dreist.

Das Prinzip funktioniert aber: Der Livestream läuft seit 23 Minuten, die Seite hat nur 17 Abonnenten – es schauen aber 108 Menschen zu und der Stream wurde bereits 158-mal geteilt.

Dass das Rätsel mit dem Inhalt des Videos überhaupt nichts zu tun hat und Thomas Müller auch überhaupt keinen Bezug zum Gewinnspiel oder Rätsel nimmt, fällt offenbar ebenso wenig auf wie der kursiv geschriebene Name der Fanpage (wegen Unicode-Sonderzeichen), die seltsame Grammatik oder der falsch geschriebene Nachname (der entsteht, weil das ü im verwendeten Zeichensatz nicht existiert).

Fazit

In diesem Artikel habe ich eine kleine Auswahl an Online-Fakes gezeigt, die deutlich machen soll, wie verbreitet und „bunt“ diese Betrügereien mittlerweile sind. Und wir alle sind potenzielle Opfer, egal wie medienaffin oder digitalversiert wir sind. Deshalb lohnt es sich, die Augen offen zu halten. Ich bin überzeugt, die allermeisten Fakes lassen sich leicht entschärfen, wenn wir genau hinschauen, uns selbst hinterfragen und kurz innehalten, damit das kritische Denkvermögen wieder übernehmen und dem Reptilienhirn Einhalt gebieten kann. So lässt sich nicht nur Schaden von uns selbst und unseren Lieben abhalten, sondern sogar von unserer Demokratie und Gesellschaft. Und das ist so dringend nötig wie nie zuvor. ¶