So geht's leichter...

Schluss mit all dem Fake im Netz

- Fake-News zuverlässig erkennen
- Fake in Social Media enttarnen
- So erkennt Ihr Fake-Shops
- Fallt nicht auf Fake-Messenges rein
- Nervige Fake-Calls blocken

Jörg Schieb

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion schieb.de
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

schieb.de

Inhalt

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Das Internet ist eine schier unendliche Quelle von Informationen. Wo früher Recherchen Wochen und Monate gedauert haben, findet Ihr hier zu (fast) jedem Thema Unmengen an Informationen und Meinungen.

Es gibt aber auch „dunkle" Seiten – und davon reichlich. Die Rede ist von Fake-News, Fake-Shops, Fake-SMS, Fake-Nachrichten und Fake-Seiten. Alles lässt sich im Netz fälschen – und das ist gefährlich.

Falsche Informationen gab es natürlich schon immer, meist aus Unwissenheit oder falsch verstandener Fachlichkeit. Mehr und mehr aber werden falsche Informationen auch gezielt eingesetzt. Um Menschen zu verwirren, um Unsicherheit zu schaffen, um Meinungen zu beeinflussen und einen Vorteil daraus zu ziehen.

Fake News sind nicht erst seit Donald Trumps Präsidentschaft in den USA zu einem Begriff geworden, der immer wieder durch die Presse geht. Wir zeigen Euch, wie Ihr Nachrichten überprüfen könnt, wie Ihr falsche Nachrichten erkennt und richtig einordnet. Auch beim Kauf im

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Internet und in den sozialen Medien bekommt Ihr immer wieder Angebote, die Ihr besser hinterfragt. Wir zeigen Euch, wie Ihr die erkennt und wie Ihr Euch möglichst gut schützen könnt.

Identifikation von Fake News

Fake News sind nicht nur ärgerlich und störend, sie sind gefährlich. Dadurch, dass Euch Fakten verdreht oder falsch präsentiert werden, bildet Ihr Euch Eure Meinung auf einer falschen Grundlage. Dagegen könnt Ihr Euch schützen, wenn Ihr auf einige Sachen achtet:

Verschiedene Arten und Schweregrade

Das sicherlich bekannteste Beispiel ist der US-amerikanische Wahlkampf im November 2020: Dadurch, dass immer wieder – fälschlicherweise – Nachrichten über Wahlbetrug in den Medien und sozialen Netzwerken platziert wurden, kam es am Ende zu gewalttätigen Unruhen. Das ist sicherlich eine Ausnahme, oft sind die Auswirkungen viel subtiler:

- Nachrichten werden so aufbereitet, dass Euch die Überschrift zum Anklicken animiert, der Inhalt hat später aber wenig bis nichts mehr mit der Überschrift zu tun: Das nennt man auch **Clickbait**.
- **Satirische Meldungen**, die den Anschein einer echten Meldung machen: Der Postillion und die US-amerikanische The Onion sind Beispiele dafür, wobei beide dafür bekannt sind und in ihren Artikeln oft so übertreiben, dass die Satire offensichtlich ist.
- **Phishing und Betrug**: Tolle Angebote, erschreckende Nachrichten und „Neuigkeiten, die Euch überraschen werden". Die dann aber im Gegensatz zu einfachem Clickbait dazu führen

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

sollen, dass Ihr Euch Schadsoftware herunterladet oder persönliche Informationen und Eure echten Anmeldedaten auf falschen Webseiten eingebt.

- **Geplante Falschmeldungen**: Während Meldungen der vorangegangenen Kategorie noch einen gewissen Unterhaltungswert haben können, werden gezielte Falschmeldungen zu einem ernsten Ziel verwendet: Meinung zu machen. Die Leser zu beeinflussen, eine bestimmte Meinung anzunehmen, die er ohne die Falschmeldungen nicht gehabt hätte. Oft werden hier
- **Hetze und Mobbing**: Während geplante Falschmeldungen eher thematisch Unwahrheiten verbreiten, gehen Hetze und Mobbing ganz gezielt gegen einzelne Personen oder Personengruppen vor. Die Auswirkungen sind katastrophal, nicht umsonst ist im Jahr 2021 ein ganzes Gesetzespaket gegen Hass und Hetze in Kraft getreten, das die strafrechtliche Verfolgung deutlich verschärft. Den Opfern hilft dies allerdings meistens wenig, der Schaden ist dann ja schon angerichtet.
- **Deep Fakes**: Diese neue Kategorie ist in den vergangenen Monaten immer ausgeklügelter geworden. Statt geschriebener Meldungen, denen viele Anwender schon kritisch gegenüberstehen, werden mittels künstlicher Intelligenz (KI) Bilder und Videos täuschend echt gefälscht. Selbst Experten haben ihre liebe Mühe, diese Fälschungen von echten Videos unterscheiden zu können.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Fake-Newsseiten erkennen

Im Kern einer jeden Fake-Nachricht steht eine Aussage, die nicht der Wahrheit entspricht. Nun ist der Mensch von Natur aus misstrauisch und würde nicht alles glauben, wenn es dafür keine Belege gäbe. So, wie es auch seriöse Journalisten machen: Sie behaupten nicht nur etwas, sondern sie liefern die Quellen dazu. Diese Quellen können dann natürlich nicht irgendwelche Adressen haben, vielleicht sogar noch aus Russland oder China: Je größer und verlässlicher die Quelle ist, desto glaubwürdiger die (falsche) Meldung. Wie aber kann das funktionieren?

Die echten Webseiten wie spiegel.de, Focus.de, bild.de werden diese Nachrichten natürlich selbst nicht veröffentlichen. Die echten Anbieter können nur nicht jede Ausprägung der Internetadresse registrieren. Fake-Internetadressen haben oft einen kleinen Tippfehler (wie spiergel.de) oder eine andere Domainerweiterung (bild.asia statt

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

bild.de), minimale Änderungen, die Euch auf den ersten Blick nicht auffallen.

Solche ähnlichen Internetadressen registrieren die Fake-Anbieter, und sie gehen noch einen Schritt weiter: Die Webseiten sehen den Originalen täuschend ähnlich. Entweder, weil sie akribisch mit allen Logos und Bereichen nachgebaut wurden. Manchmal werden dazu auch Bots eingesetzt, die die aktuellen Inhalte der echten Seite nachladen und so der Fake-Seite ein aktuelles Aussehen geben.

Inmitten dieser Artikel findet sich dann der Fake-Artikel (oder sogar mehrere). Auf den ersten Blick sieht das alles echt und wahr aus.

Prüfen der Quelle

Eigentlich ist es vergleichbar zum analogen Leben: Wenn Euch jemand etwas erzählt, dann denkt Ihr auch erst einmal über zwei Sachen nach:

- Ist die Quelle vertrauenswürdig? Wenn die Information jemandem kommt, der gerne mal Geschichten erzählt, dann zweifelt Ihr. Ist derjenige bekannt für seine guten Informationen, dann glaubt Ihr ihm.
- Klingt die Nachricht an sich glaubwürdig? Ist das nicht der Fall, dann fragt Ihr vielleicht auch noch einmal andere Menschen, die etwas zu dem Thema wissen könnten.

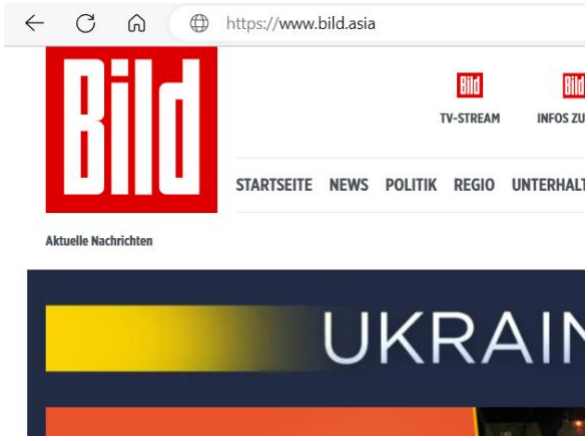
Das Prüfen der Internetadresse

Schaut Euch bei allen Nachrichten, die Ihr im Internet lest, die Internetadresse ganz genau an.

- Ist die Webseite an sich vertrauenswürdig? Ihr kennt die Webseiten, die Ihr regelmäßig konsumiert. Ist die Nachricht von einer dieser Seiten?

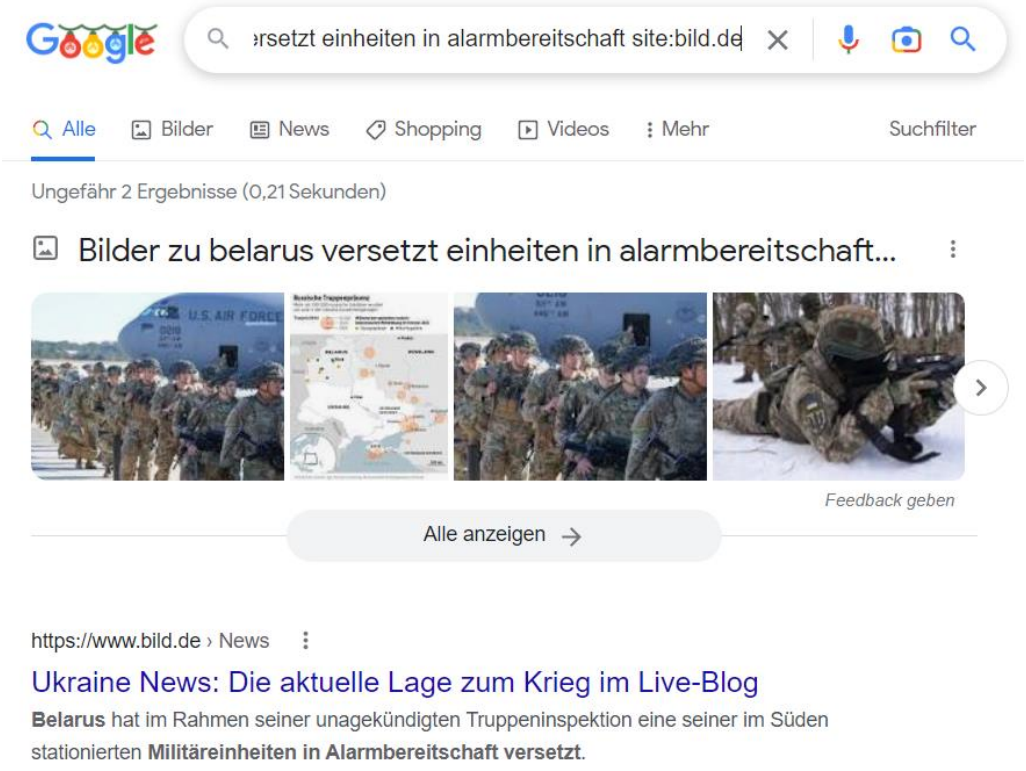
Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Stimmt die Adresse der Webseite genau mit der überein, die Ihr normalerweise aufruft? Auch kleinste Abweichungen wie eine andere Domainendung (wie im Beispiel .asia statt .de) oder ein Tippfehler sollten schon Grund für Euer Misstrauen sein!



- Stammt die Nachricht wirklich von der Seite, die Ihr gerade zu besuchen meint? Dazu könnt Ihr Google zur Hilfe nehmen. Kopiert von der Quellseite einfach die Überschrift in die Zwischenablage und fügt sie auf der Google-Seite ein, gefolgt von einem **site:** und dem Namen der Webseite, beispielsweise **site:bild.de**. Google sucht nun nach der Überschrift auf der angegebenen Seite. Wenn die dort nicht gefunden wird, ist das ein deutliches Zeichen für einen Fake-Artikel.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen



Alter des Artikels prüfen

Mittlerweile lassen sich auch normale Webseiten dazu herab, gerade bei aktuellen Themen auch schon mal Uraltartikel aufzuwärmen. Es macht durchaus einen Unterschied, ob eine Katastrophe aktuell passiert ist, oder ob es sich um eine Meldung von vor zwei Jahren handelt (die Ihr schon lange kanntet).

Oft findet Ihr in den Artikeln dann den Hinweis „Dieser Artikel ist bereits in der Vergangenheit erschienen. Er hat viele Leserinnen und Leser besonders interessiert. Deshalb bieten wir ihn erneut an."

Anders formuliert: „Damals haben wir schon viele Klicks und damit Werbeeinnahmen bekommen, dann versuchen wir das jetzt einfach nochmal!"

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Anmerkung der Redaktion: Dieser Text ist bereits in der Vergangenheit erschienen. Er hat viele Leserinnen und Leser besonders interessiert. Deshalb bieten wir ihn erneut an.

Das sei noch immer deutlich günstiger als bei einem Benziner, der bei der gleichen Strecke etwa 532 Dollar an Sprit verbraucht hätte. „Ich hoffe, unser Trip zeigt, wie sehr es finanziell Sinn macht, ein E-Auto zu mieten, zu fahren oder zu kaufen, wenn man es noch nicht gemacht hat“, heißt es im Fazit des Berichts. „Stellt euch nur mal die Zukunft vor, wenn mehr Autos elektrisch und Ladestationen allgegenwärtig sind.“

Andere Quellen prüfen

Eine tatsächlich echte und wichtige Nachricht wird nie nur von einer Internetseite veröffentlicht. Sucht Euch parallel zu der einen Fundstelle über die Suchmaschine Eurer Wahl noch anderen Quellen heraus, denen Ihr vertraut. Findet sich die Nachricht nur auf „komischen“ Webseiten, aber nicht als vertrauenswürdig bekannten, dann ist die Wahrscheinlichkeit hoch, dass es sich um eine Fake-Nachricht (oder schlicht um schlechte Recherche) handelt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

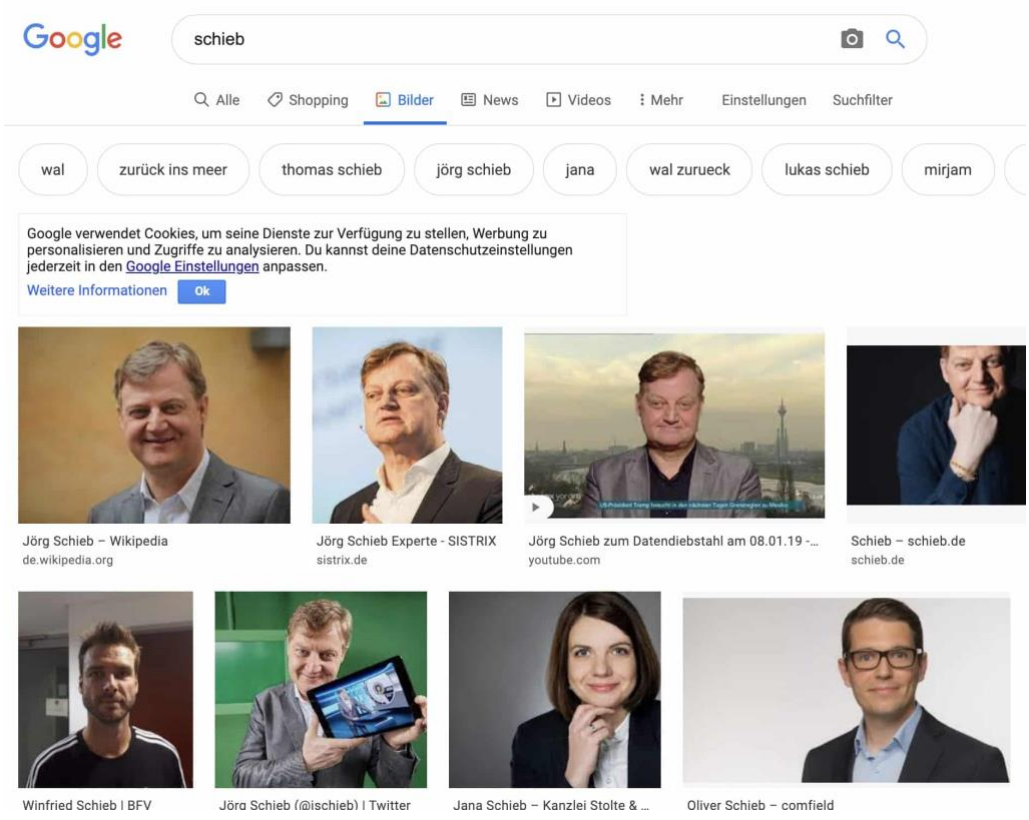
Diese Prüfung ist allerdings manchmal nur ein trügerischer Schutz: Mehr und mehr Webseiten plappern Fake News unbeabsichtigt nach. Frei nach dem Motto: „Klingt gut, bringt Besucher, dann schreiben wir das auch." Das passiert aber bei seriösen Quellen durch ganz, ganz selten.

Bilderquellen bei der Google-Suche identifizieren

Wenn Ihr einen Suchbegriff bei Google eingebt, dann kommen neben den Links zu Internet-Seiten, die diesen enthalten, oft auch Bilder als Ergebnis. Das ist erst mal nichts Besonderes, nur manchmal findet Ihr darin Bilder, die so gar nichts mit der Suche zu tun haben. Oder ein Bild von sich selbst, das Euch erschreckt und von dem Ihr wissen wollt, wo es erscheint. Wichtig vor allem dann, wenn es für einen Fake-Artikel genutzt wird!

- Die Bilder zu Ihrem Suchbegriff seht Ihr, wenn Ihr auf **Bilder** unter der Suchleiste klickt.
- Google zeigt Euch nun alle Bilder an, die zu Eurem Suchbegriff passen. Klickt auf eines der Bilder, dann kommt in den meisten Fällen aber nicht die Webseite, auf der das Bild ist, sondern nur das Bild in größerer Ansicht.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

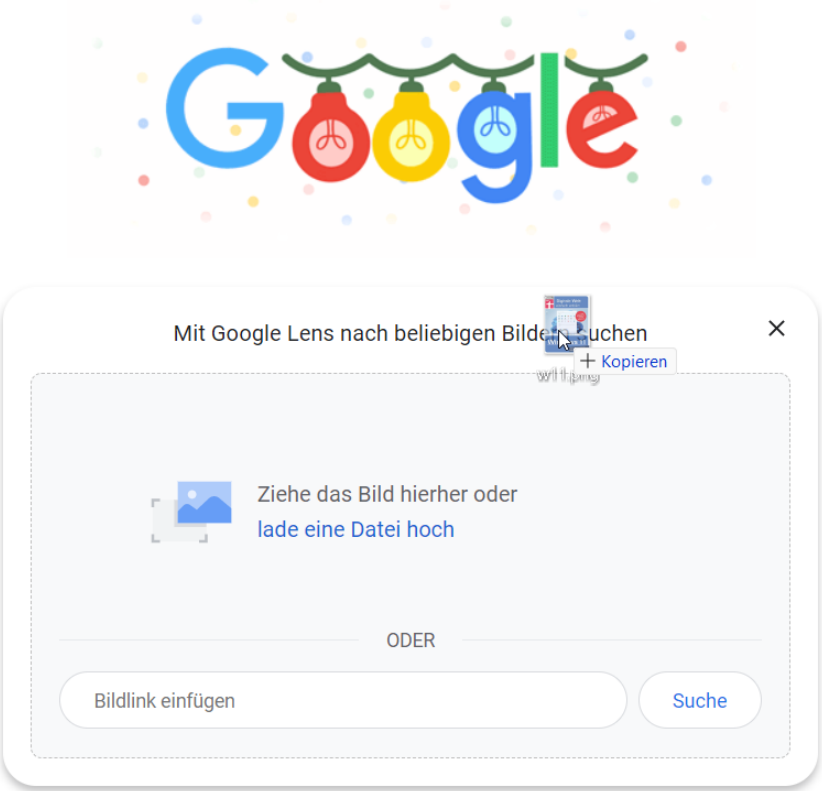


- Unter dem Bild findet Ihr aber eine kleine Schaltfläche, die den Namen der Webseite enthält. Klickt darauf, dann solltet Ihr zur Seite geleitet werden.
- Passiert das nicht, dann habt Ihr noch eine Alternative: Klickt mit der rechten Maustaste auf das Bild und dann auf **Bildlink kopieren**.
- Klickt dann in die Adressleiste des Browsers und drückt gleichzeitig **Strg** + **V**. Ihr seht nun in der Adressleiste des Browsers die Herkunfts-Adresse des Bildes. Mit der könnt Ihr dann direkt auf die Quellseite gelangen.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Fake-Bilder: Invers-Bildersuche bei Google

Oft versuchen sich Fake-Artikel den Anschein der Echtheit zu geben, indem sie passende Bilder verwenden. Die stammen dann aber oft aus ganz anderen Zusammenhängen, aus Artikeln zu einem anderen Thema von einer ganz anderen Quelle. Was wenig bekannt ist: Google bietet neben der Textsuche auch eine Inverssuche für Bilder an, sucht Euch also zu einem Bild weitere Webseiten heraus, auf denen es vorkommt.



- Klickt mit der rechten Maustaste auf ein Bild in einem Beitrag, den Ihr überprüfen wollt, dann auf **Bild speichern unter**.
- Speichert das Bild auf dem Desktop (oder einem anderen Ort auf Eurer Festplatte).

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Ruft im Browser die Google-Suche auf.
- Zieht das Bild von der Festplatte in das Google-Fenster, das Eingabefeld verändert sich zu Google Lens.
- Das Bild wird nun automatisch hochgeladen und das Internet nach Webseiten durchsucht, auf denen es vorkommt.
- Kommt das Bild auf anderen Webseiten zu einem komplett anderen Thema vor, dann ist das ein deutlicher Hinweis auf einen Fake-Artikel!

Fake in Social Media

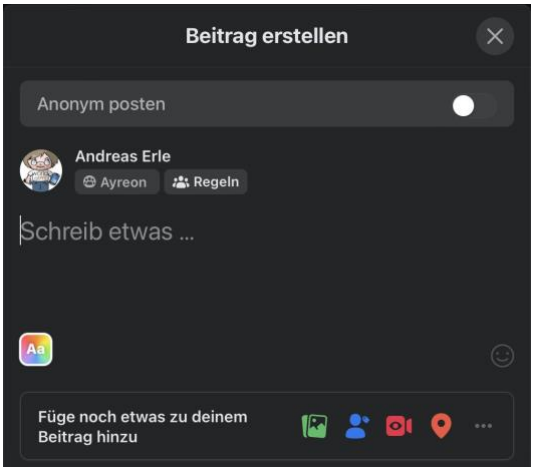
Das Internet ist schon ein Sammelbecken für Falschnachrichten. Allerdings bedarf es hier einigen Aufwands, denn das Erstellen einer echt wirkenden Fake-Webseite ist nicht mal eben erledigt. Ganz anders die sozialen Netzwerke: Facebook, Twitter, WhatsApp, Telegram machen es den Benutzern einfach, Nachrichten zu posten. Die inhaltliche Kontrolle fällt da mehr oder weniger aus. Natürlich gelten für die Netzwerke die schon beschriebenen Vorsichtsmaßnahmen ebenso, allerdings müsst Ihr hier noch einige zusätzliche Sachen beachten:

Anonyme Beiträge auf Facebook

Das Internet soll nicht anonym sein, Personen sollen dazu stehen, was sie schreiben. Das gilt aber nicht immer: Manchmal sind anonyme Beiträge sinnvoll, beispielsweise, wenn über Belastendes berichtet werden soll. Das erlaubt Facebook in Gruppen unter bestimmten Umständen.

Das Internet besteht nicht nur aus Beleidigungen und Trollereien, sondern oft auch aus Berichten Betroffener, die sich Luft machen wollen.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen



Das Berichten über Erlebtes fällt leichter, wenn man es aus dem Schutz der Anonymität machen kann. Die Voraussetzung bei Facebook: Ein Gruppenadministrator muss dies für die Gruppe aktivieren.

Klickt in der Gruppe in das Feld für einen neuen Beitrag, dann seht Ihr über Eurem Namen einen Schalter **Anonym posten**. Aktiviert diesen, dann wird Euer Beitrag ohne Euren Namen/Euer Profilbild gepostet. Allerdings müsst Ihr dabei die folgenden Dinge beachten:

- Der Beitrag geht vorab zur Prüfung an die Administratoren, wird also nicht wie normal direkt online gesetzt.
- Für die normalen Leser ist der Beitrag anonym, die Administratoren können trotzdem sehen, dass Ihr ihn geschrieben habt.
- Auch Facebook selbst sieht den tatsächlichen Absender des Beitrages. Damit soll sichergestellt werden, dass die Community-Standards eingehalten werden.
- Manche Beiträge/Beitragstypen können von den Administratoren per se als anonym klassifiziert werden.

Ihr müsst hier aber abwägen: Je nach Thema ist ein anonymer Beitrag natürlich viel unglaubwürdiger als einer, der von einer echten, nachverfolgbaren Person geschrieben ist. Wenn es also um Empfehlungen oder gar „wichtige Nachrichten“ geht, dann solltet Ihr bei einem anonymen Beitrag immer hinterfragen!

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Vorsicht bei Facebook-Ratespielchen

Facebook ist unterhaltsam. Neben Neuigkeiten Eurer Freunde und Bekannten findet Ihr alle möglichen Ratespielchen der Art "Mein erstes Auto war ein...". Das lädt ein, eben mal schnell eine Antwort zu schreiben und die andern durchzulesen. Das Risiko ist aber nicht zu unterschätzen!

Alleine genommen fallen Euch die in solchen Aktionen gestellten Fragen oft nicht auf, wenn Ihr sie aber einmal hintereinander anseht, dann erkennen Ihr schnell, dass diese oft eines gemeinsam haben: Diese Fragen werden auch als Sicherheitsfragen für die Passwortwiederherstellung oder als zweiter Schutzfaktor verwendet. Die Wahrscheinlichkeit ist hoch, dass Ihr diese Fragen gleich beantwortet haben.

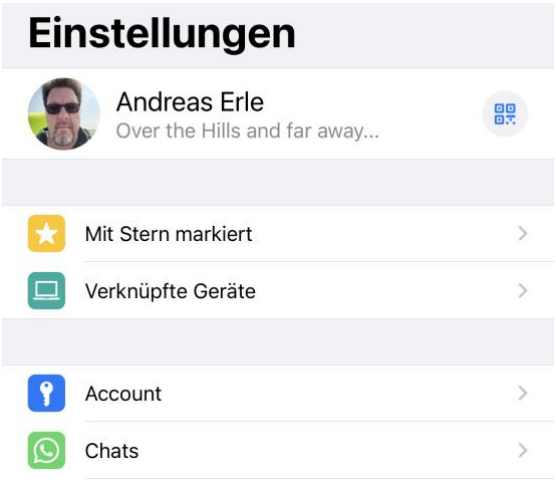
Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- In der Folge hat damit jeder Zugriff auf diese Antworten, denn die "Fragesteller" haben eine öffentliche Timeline, jeder kann die Beiträge lesen.
- Mit wenigen weiteren Informationen haben Übeltäter damit gegebenenfalls die Möglichkeit, durch einen Passwortreset und die richtige Antwort auf eine Sicherheitsfrage eines Eurer Konten zu übernehmen.
- Wenn Ihr diese Antworten als Teil Ihrer Passwörter verwendet, dann ist das Risiko noch höher.
- Zusammengefasst: Solche Frageaktionen im Internet mögen kurzen Spaß bringen, verursachen aber gegebenenfalls länger andauernden Ärger!

WhatsApps mit Anrufaufforderungen

Jedes Kommunikationsmittel bietet Angreifern Möglichkeiten, es zu missbrauchen. Wenn Ihr eine WhatsApp mit einer Telefonnummer mit *-Codes vorne bekommt, ignoriert diese unbedingt!

Das WhatsApp-Konto ist für viele Anwender der Kern ihrer Kommunikation. Der schnelle Chat nebenbei, aber auch die Absprache von Verabredungen oder sogar der Abschluss von Geschäften finden über den Messenger statt. Kommt Euer Konto in falsche Hände, dann kann Euch rechenbarer



Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Schaden entstehen! Gerade geht eine Welle von vermeintlichen Aufforderungen zu einem Rückruf durch die WhatsApp-Welt. Seid vorsichtig, bevor ihr der Aufforderung Folge leistet!

- Die Rufnummern, die Ihr anrufen sollt, fangen mit ****21*** an. Was wie der Teil der Rufnummer aussehen soll, ist in Wirklichkeit ein sogenannter GSM-Code, ein Steuerbefehl für Funktionen des Mobilfunknetzes.
- In diesem Fall wird damit die Rumleitung von Eurer Rufnummer auf die Rufnummer, die sich hinter dem GSM-Code befindet, eingerichtet.
- Alle Anrufe an Eure Nummer gehen dann an die Nummer des Angreifers. Der startet dann eine Registrierung von WhatsApp mit Eurer Nummer mit der Übermittlung des Codes per Anruf. Da der Anruf ja an seine Rufnummer umgeleitet wird, kann er das Konto verifizieren und damit Euer WhatsApp-Konto übernehmen.
- Die Lösung: Ignoriert die Nachricht und blockiert den Absender!

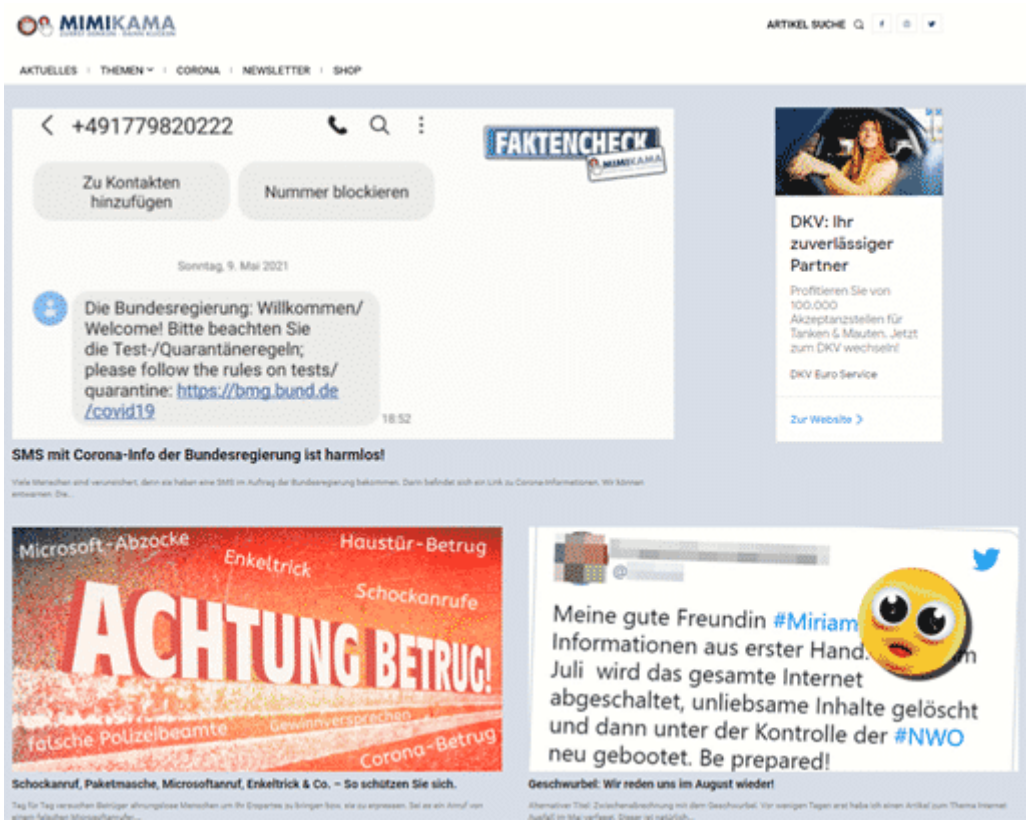
Schwarmintelligenz: Mimikama

Die diversen Fake-Meldungen, Kettenbriefe und Preisausschreiben, die Ihr allüberall in den sozialen Netzwerken findet, sind meist fiese Fallen. Das angebliche Video, in dem Ihr in einer schlüpfrigen Situation zu sehen sein sollt, das E-Bike, dass Ihr einfach durch Kommentieren einer Nachricht kostenlos bekommt, diese haben eines gemeinsam: Sie wollen Euch dazu animieren, zu klicken.

- Im einfachen Fall, damit Eure Daten gesammelt werden können.
- Im schlimmeren Fall, um Euch zur Preisgabe Eurer Kontoinformationen zu animieren und Ihr Konto zu übernehmen.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Eine tolle Anlaufstelle ist die Webseite Mimikama. Deren Motto „Zuerst denken – dann klicken“ fasst gut zusammen, wie Ihr Euch vor solchen Fakes schützen könnt: Viele der verbreiteten Aktionen werden auf Mimikama erklärt und bewertet.



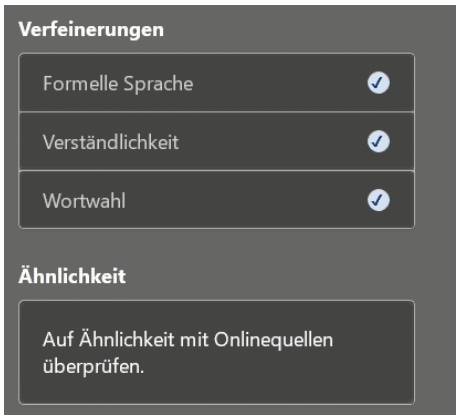
- Das gibt Euch eine größere Sicherheit, nicht auf eine solche Fake-Aktion hereinzufallen.
- Neben den wirtschaftlichen Schäden, die entstehen können, ist es auch für Eure Follower ein schlechtes Zeichen, wenn Ihr eine Nachricht zitiert und postet, die schon lange als Fälschung bekannt ist!

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

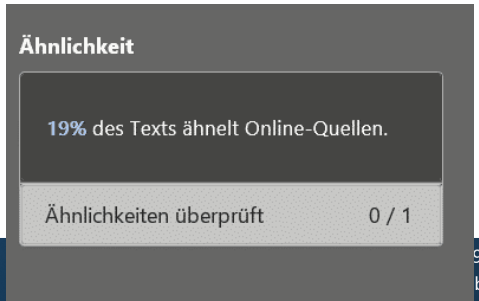
Suche nach Plagiaten

Plagiate, ein Begriff, der in den letzten Monaten immer mehr in die Presse gekommen ist. Dabei ist dieser nicht neu: Kopiert, im Volksmund "abgekupfert" wurde schon immer. Allerdings fällt das dank der Möglichkeiten des Internets deutlich schneller auf. Oft verwenden Anbieter von Fake News einfach Kopien von bestehenden Informationen und Texten. Wenn Ihr sicherstellen möchtet, dass ein Text nicht aus einer anderen Quelle stammt, dann könnt Ihr Word dafür nutzen:

- Kopiert den Text aus dem Internet oder dem Dokument, den Ihr überprüfen möchtet, fügt ihn in Word ein und markiert ihn dort.
- Dann klickt in der Menüleiste auf **Überprüfen** > **Editor**. Der Editor ist die zentrale Instanz in Word, wenn es um die Überprüfung des Textes auf Mängel wie Rechtschreibfehler, Grammatik, formelle Sprache etc. geht.



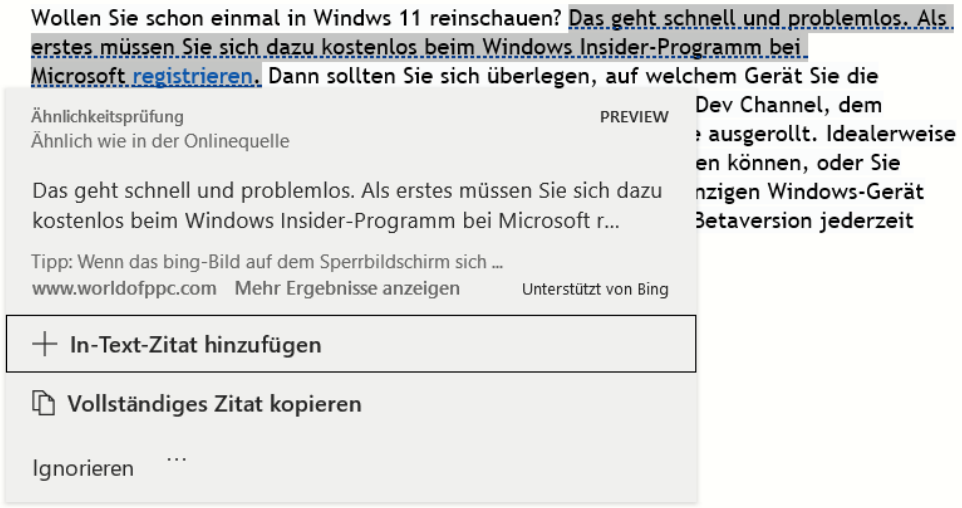
- Ganz unten in den Optionen findet Ihr **Ähnlichkeit**. Klickt darauf, dann vergleicht Word den Text mit Online-Quellen.
- Am Ende dieses Vorgangs bekommt Ihr eine Einschätzung, wie viel Anteil Ihres Textes sich in Online-Quellen findet beziehungsweise diesem ähnelt.
- Das kann durchaus richtig sein, wenn der Autor ein Zitat verwendet hat oder aus einer



Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

eigenen Quelle im Internet zitiert.

- Klickt auf das Ergebnis, dann zeigt Euch Word die Bereiche des Textes direkt im Dokument.
- Damit aber nicht genug: Wenn Ihr die Funktion nutzt, um einen eigenen Text zu überprüfen, dann könnt Ihr das gefundene Zitat durch einen Klick auf **In-Text-Zitat hinzufügen** direkt in das Dokument aufnehmen und so korrekt zitieren!



Bestimmte Begriffe in Twitter stummschalten

Das Internet hat viele Schattierungen, und neben den vielen schönen natürlich auch unschöne. Dazu gehört die schier unendliche Vielzahl an Themen und der Umgang damit, der nicht immer jedem Benutzer gefällt. Gerade unmoderierte Dienste wie Twitter, in denen quasi jeder schreiben kann, was er möchte, sind hier für den ein oder anderen Anwender ein Problem. Und das nicht erst, seit Elon Musk die Standards noch einmal gesenkt hat!

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Wenn Euch Fake News zu bestimmten Themen auf den Nerv gehen, Ihr aber trotzdem Twitter weiter nutzen wollt, dann habt Ihr dazu eine Funktion zur Verfügung: Ihr könnt beliebige Themen und Wörter auswählen und in der Timeline ausblenden.

- Geht in Eure Twitter-App auf dem Smartphone, tippt auf Euer Kontobild und dann auf **Einstellungen und Datenschutz**.
- Twitter selbst fragt in regelmäßigen Abständen bei bestimmten Beitragsthemen nach, ob Ihr eine solche Stummschaltung ausführen wollen, dann könnt Ihr natürlich auch direkt auf das Banner klicken.
- Aktiviert den **Qualitätsfilter**, um Twitter eine Vorauswahl von unangemessenen Posts machen zu lassen. Diese werden dann automatisch ausgeblendet. Das Risiko hierbei: Ihr habt wenig Kontrolle, ob nicht vielleicht doch ein Post dabei ist, der vielleicht interessant wäre. Besser ist hier die manuelle Nutzung von Filtern:

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Tippt auf **Stummgeschaltet** > **Stummgeschaltete Wörter**. Ihr könnt nun unter **Hinzufügen** neue Wörter hinzufügen, die zu einer Ausblendung führen sollen.
- Wählt durch die Schalter aus, ob der Filter auf die **Home-Timeline** und/oder die **Mitteilungen** wirken soll.
- Ab der Aktivierung verwendet Twitter die eingegebenen Begriffe automatisch, um Beiträge auszublenden und Euch nicht mehr zu belästigen.

Fake-Shops und Angebote

Der Einzelhandel ist unter Druck: Mehr und mehr Anwender kaufen ihre Waren im Internet. Dank Zahlungsdienstleistern wie PayPal und anderen nicht nur in Deutschland oder Europa, sondern weltweit. Zahlung und Versand sind so einfach, und die Preise im Ausland oft verlockend günstig. Viele Angebote sind Fake: Gefälscht, von der Beschreibung abweichend, manchmal nicht vorhanden, das Geld soll es aber nicht zurück geben.

Fake-Shops erkennen

Ein immer größer werdendes Übel sind die sogenannten Fake-Shops. Wie die gleich genannten Nachrichten versuchen diese, Euch etwas vorzugaukeln. Tolle Angebote, günstige, meist zeitlich limitierte Preise und schneller Versand sollen Euch zum Kauf animieren. Habt Ihr erst mal bezahlt, dann wartet Ihr oft ewig auf die Lieferung. Wenn Ihr überhaupt kommt, dann entspricht die Ware oft nicht dem, was Ihr bestellt und erwartet habt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Noch schlimmer: Legt Ihr ein Benutzerkonto an und verwendet schon mal woanders benutzte Zugangsdaten, dann landen die schnell in Datenbanken, die im Internet verkauft werden und Übertätern dazu dienen, einfach mal bei allen möglichen Seiten zu versuchen, sich damit in Eurem Namen anzumelden!

Absolute Sicherheit bei der Erkennung der schwarzen Schafe gibt es nicht. Wir zeigen Euch aber Merkmale, die Euch stutzig machen sollten.

Der Preis

Bei vielen Fake-Shops ist es eine Kombination aus dem vollkommen unrealistisch niedrigen Preis und der Aussage, dass der ja nur noch ganz kurz gilt. Oder die Zahl der verfügbaren Geräte schon fast ausgeschöpft ist.

Vergesst einfach die Hoffnung, dass es Händler gibt, die Euch teure Hardware nahezu schenken. Das ist eine Illusion, die Euch nur unnötig Geld kostet und Frust bringt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Tipp Diese Warnungen gelten natürlich nicht für die Angebotsschlachten der großen Anbieter wie Amazon und anderen: Black Friday, Cyber Monday und wie sie alle heißen beinhalten tatsächlich in den meisten Fällen stark reduzierte und von der Anzahl her limitierte Waren!

Die Zahlweise

Die meisten Internetshops bieten sichere Zahlweisen über bekannte Zahlungsanbieter wie PayPal, Klarna oder andere an. Wenn eine Webseite entweder nur „sonderbare" Zahlungsanbieter verwendet oder aber die ganzen üblichen bei der Bezahlung nicht funktionieren und nur die Vorabüberweisung übrigbleibt: Finger weg! Ist das Geld erst einmal auf der Reise, dann habt Ihr wenig Handhabe, wenn die Ware nicht kommt. Käuferschutz gibt es nun mal bei Überweisungen nicht.

Die Millionen zufriedener Kunden

Wer kann besser Auskunft über die Vertrauenswürdigkeit eines Shops geben als andere Kunden? Prinzipiell richtig, bei Fake-Seiten aber ein zweischneidiges Schwert: Nichts einfacher, als automatisiert positive Bewertungen auf eine Seite zu stellen, wenn man sie selber programmiert hat.

Wenn die Bewertungen größtenteils positiv sind, dann schaut Euch diese genauer an: Bei Fake-Shops habt Ihr regelmäßig dieselben Wortlaute und Formulierungen, die immer und immer wieder verwendet werden. Auch sonderbarer Satzbau und Wortwahl sollten skeptisch machen: Fake-Bewertungen werden meist per automatischem Übersetzer erstellt und ungeprüft hochgeladen.

Mittlerweile lassen sich Bewertungen gar im Hunderterpack online kaufen. Das ist vom Münchner Landgericht Ende 2019 als rechtswidrig

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

erklärt worden. Doch auch unabhängig von der Rechtslage: Wenn ein Shop es nötig hat, sich Bewertungen zu kaufen, dann kann es mit der Qualität nicht weit her sein!

Besonders tolle Siegel

Der Käufer an sich ist ja schon kritisch: Wenn er schon im Internet kauft, dann muss es zumindest ein geprüfter Händler sein. Zumindest sind wir Europäer so aufgestellt. Und bei „echten" Online-Shops sind die Siegel tatsächlich ein Zeichen für Kontrollinstanzen. Ob die nun besonders aussagekräftig sind, darüber kann man streiten. Zumindest führt Euch ein Klick auf ein solches Siegel zu der Zertifizierungsstelle.

Bei den meisten Fake-Shops bekommt Ihr unzählige bunte Bildchen angezeigt, teilweise auch von namhaften Anbietern. Wenn Ihr darauf klickt, dann passiert entweder gar nichts, oder Ihr werdet auf eine echte Seite geleitet, die aber keinen Bezug zu der Shop-Seite hat. Auch das ist ein Warnsignal!

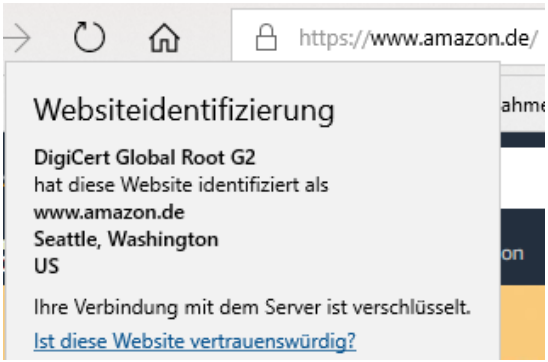
Sichere Webseiten

Eine Webseite schafft Euch eine leicht andere Einkaufsumgebung als ein echter Laden. Beim Shopping in der Stadt könnt Ihr Euch vor dem Kauf

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

anhand des Angebots, der Lage des Ladens, der Mitarbeiter zumindest einen visuellen Eindruck verschaffen. Und vor allem könnt Ihr die Produkte anfassen und deren Qualität vorher beurteilen. Im Internet ist vieles Vertrauenssache. Wenn Ihr kauft, dann könnt Ihr nur hoffen, auch die bestellte und meist vorbezahlte Ware zu bekommen.

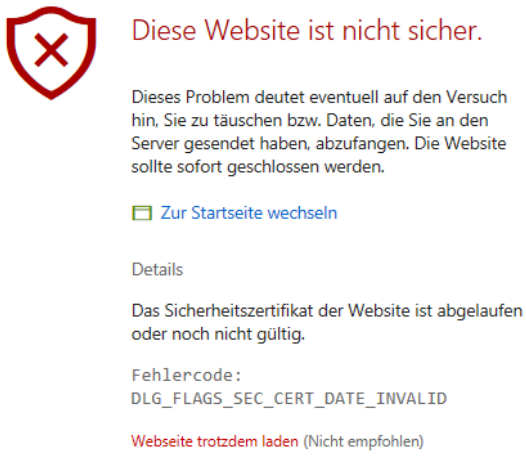
Einen Hinweis wenig bietet hier das Zertifikat der Webseite. Ein SSL-Zertifikat ist quasi ein Siegel, das die Organisation, der die Webseite gehört, und die Webseitenadresse miteinander in Verbindung bringen. Das Zertifikat ermöglicht es dann, die Kommunikation zwischen Eurem Rechner und dem Shop zu verschlüsseln.



Das ist wichtig, damit beispielsweise Kreditkarten- oder Kontoinformationen für die Bezahlung nicht auf dem Weg abgefangen und missbraucht werden können. Erkennen können Ihr den Einsatz eines SSL-Zertifikats daran, dass links (oder rechts, je nach Browser) der Internetadresse ein Schloss angezeigt wird. Klickt darauf, dann seht Ihr die sogenannte Webseitenidentifizierung. Die zeigt an, auf welchen Händler die Seite registriert ist. Keine Fake-Seite könnte sich also hier als Apple oder Amazon ausgeben, weil sie gar nicht erst durch den Prüfprozess zur Erteilung des SSL-Zertifikats kommen würde.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Vorsicht ist geboten, wenn eine Webseite nicht verschlüsselt ist oder gar das Zertifikat nicht zu Seite passt oder abgelaufen ist. Letzteres kann immer mal passieren, ist aber bei einem Online-Händler kein gutes Zeichen. Ihr könnt die Webseite dann trotzdem besuchen, empfehlenswert (gerade bei Shopping- oder Online-Banking-Seiten) ist das nicht!



Gütesiegel als Qualitätsmerkmal

Wenn eine Webseite nicht schon bekannt ist und sich einen gewissen Ruf erarbeitet hat, dann ist es recht schwer, Vertrauen zu schaffen. Da hilft es, sich von einem unabhängigen Zertifizierer die Aussage zu besorgen, dass man als Händler vertrauenswürdig ist. Wenn Ihr auf ein solches Siegel klickt, dann gelangt Ihr im Normalfall auf die Webseite des Zertifizierers und bekommt angezeigt, welche Eigenschaften des Shops dieser mit dem Siegel bestätigt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Nun ist Papier geduldig, und nicht jedes Siegel ist gleich wertvoll. Trusted Shops (https://www.trustedshops.de/) beispielsweise vergibt sein Siegel nur an Shops mit besonders hohen Standards. Als Zeichen der Überzeugung bietet Trusted Shops dann gleich noch einen eigenen Käuferschutz an: Habt Ihr Probleme beim Kauf, dann findet Ihr dort Unterstützung. Andere bekannte und renommierte Siegel sind das **EHI geprüfter Online-Shop** und das **Safer Shopping** vom TÜV Süd.

Es gibt noch viele andere Zertifikate, aber manche sind nicht das virtuelle Papier wert, auf dem sie stehen.

Impressum, Kontakt und Datenschutz

Vertrauensbildend, aber auch eine rechtliche Notwendigkeit: Ein Impressum und eine Datenschutzerklärung muss eine jede Webseite haben. Auch hierauf solltet Ihr einen genauen Blick werfen. Aus mehreren Gründen:

Impressum und Unternehmenssitz

Das Impressum, alternative auch „Anbieterkennzeichnung" genannt, gibt Euch vor allem Auskunft über den Betreiber der Webseite. Das zeigt Euch vor allem, ob es sich um einen Betreiber in Deutschland oder dem Ausland handelt. Dazu übrigens später noch ein paar weitere Anmerkungen. Wenn eine Webseite aber kein Impressum hat, dann solltet Ihr skeptisch sein: Euch fehlt der


impressum

Verantwortlich für die auf dieser Website publizierten Artikel und Inhalte (mit Ausnahme der Kommentare), sofern keine anderen Angaben gemacht werden:

Jörg Schieb
Humboldtstr. 10
D-40667 Meerbusch

FON: 02132-6733305
FAX: 02132-67333059

MAIL: fragen@schieb.de

Bitte verwenden Sie mein Kontaktformular.

Autoren auf schieb.de
Das Infoportal schieb.de enthält Artikel von verschiedenen Autoren/Redakteuren.

Chefredakteur:
Jörg Schieb

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Ansprechpartner, wenn es einmal hart auf hart geht und Ihr einen Anwalt einschalten müsst. Zum Beispiel, weil die Ware nicht kommt oder eine Rücksendung nicht funktioniert oder Ihr sicher seid, dass aus diesem Shop Eure Benutzerdaten entwendet oder missbraucht wurden. Und da in Deutschland Impressumspflicht herrscht und jeder Händler eine Abmahnung scheut, ist der Shop entweder schludrig oder schert sich nicht darum. Keine gute Voraussetzung für einen Einkauf!

Allgemein gilt: Das Impressum sollte nicht mehr als einen Klick von der Startseite entfernt sein. Meist findet Ihr es am oberen oder unteren Bildschirmrand.

Kontaktmöglichkeiten

Neben den rechtlichen Kontaktdaten, wie sie im Impressum zu finden sein sollten, ist auch die Beratungsmöglichkeit ein Thema. Ein Online-Händler, der etwas auf Kundenservice hält, bietet Euch Hilfestellung. Ob per Telefon, Chat oder Ticketsystem, zumindest aber per E-Mail. Auch bei einem Umtausch oder einer Reklamation solltet Ihr wissen, wie Ihr jemanden erreicht.

Oft wird das Impressum kombiniert mit den allgemeinen Geschäftsbedingungen (AGB). In diesen sollte sich auch die Abwicklung bei der Rückgabe gekaufter Ware finden.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Das Rückgaberecht

Als Verbraucher, der eine Ware online bei einem Händler kauft, hat Ihr innerhalb von 14 Tagen ein Recht auf den Umtausch gegen Erstattung des Kaufpreises. Man liest oft immer noch vom Fernabsatzgesetz (FernAbsG), auch wenn das schon lange nicht mehr existiert: In Deutschland finden sich die entsprechenden Regelungen seit einigen Jahren im Bürgerlichen Gesetzbuch (BGB). Genaueres findet Ihr hier: https://www.e-recht24.de/artikel/ecommerce/12.html Dieses Rückgaberecht gilt natürlich auch in Fällen, in denen die Ware im Rahmen eines Fake-Angebots nicht kommt oder ganz anders als beschrieben ist!

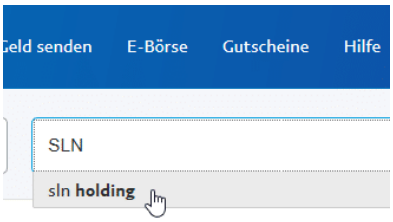
- Grob gesprochen könnt Ihr innerhalb von 14 Tagen nach Erhalt der Ware den Kauf widerrufen.
- Dann könnt Ihr die Ware zurückschicken und bekommt das Geld zurück.
- Wie genau die Abwicklung ist, solltet Ihr in den AGBs des Händlers finden.
- Auch Händler außerhalb von Deutschland bieten so etwas oft an, das heißt dann „30 Day Money Back Guarantee“ oder so. Denkt dabei nur daran, dass Ihr das – meist nicht unerhebliche – Porto zahlen müsst und die eventuell angefallenen Zollauslagen auch nicht zurückbekommt. Oft lohnt sich das dann nicht mehr.

Käuferschutz bei PayPal

Klappt der Kauf nicht wie gewollt und der Verkäufer reagiert nicht auf Eure Reklamation, dann ist erst einmal guter Rat teuer, vor allem, wenn der im Ausland sitzt. Wenn Ihr als Zahlungsmittel PayPal einsetzt, dann könnt Ihr mit wenig Aufwand Käuferschutz beantragen.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Meldet Euch dazu an Eurem PayPal-Konto an und klickt auf **Letzte Aktivitäten**.



- Wenn Ihr den betroffenen Einkauf nicht direkt seht, dann klickt in das Suchfeld und gebt den Namen des Händlers ein. Damit könnt Ihr die Liste der Transaktionen filtern.

- Öffnet die Transaktion, dann findet Ihr unten den Link zu **Problem melden**. Gebet die angeforderten Informationen an, dann wird automatisch ein Fall bei PayPal geöffnet. Das ist allerdings noch kein Antrag auf Käuferschutz, der zu einer Gutschrift führt!

Rechnungsnummer
WC-36674

Kaufdetails

Memorable Stan Statue	39,99 USD
Versand	4,95 USD
Summe	**44,94 USD**

⚠ **Problem melden**

- PayPal empfiehlt nun, einige Tage auf eine Reaktion des Verkäufers zu warten. Wenn Ihr das schon getan habt (oder

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

ungeduldig seid): Klickt in der PayPal-Übersicht auf **Konflikte**, dann öffnet den gerade geöffneten Fall.

- Klickt ganz unten auf **Paypal zur Klärung einschalten**. Ihr müsst dann noch einige Informationen eingeben, dann wird PayPal offiziell mit der Lösung des Konflikts beauftragt.
- Wenn der Händler eine Zustellung der Bestellung nicht nachweisen kann, dann habt Ihr gute Chancen, eine Gutschrift zu bekommen. Wenn es sich um eine Ware handelt, die nicht im beschriebenen Zustand war, dann könnt Ihr als Nachweis beispielsweise auch Bilder an den Fall anhängen.

eBay ist anders

Lange Zeit gab es unterschiedliche Auffassungen zu eBay und dem Rückgaberecht. Für Versteigerungen gilt das Rückgaberecht nicht. Nur: ist eBay ein Auktionshaus im klassischen Sinne? Die meisten Entscheidungen von Gerichten gehen mittlerweile davon aus, dass das nicht der Fall ist und damit eine eBay-Auktion auch dem Rückgaberecht unterliegt.

Allerdings sind viele eBay-Auktionen ja Angebote von Privatleuten, die ihren virtuellen Dachboden entrümpeln. Bei Privatgeschäften gilt das Rückgaberecht per se nicht.

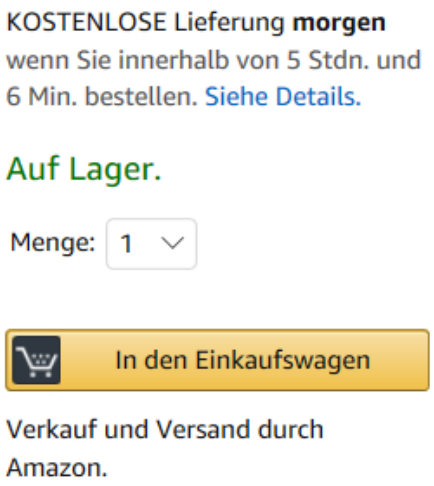
Wenn Ihr unsicher seid, ob ein Verkäufer eine Rückgabe anbietet, dann schaut in den Daten des Angebots nach.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Amazon ist nicht gleich Amazon

Wenn Ihr bei Amazon kauft, dann wähnt Ihr Euch bei einem Händler, der in Deutschland Lager hat und von dort aus auch verschickt. Und Ihr seid überzeugt davon, dass Ihr den Kundenservice von Amazon im Rücken habt.

Was der ein oder andere Käufer nicht weiß: Bei Amazon findet Ihr drei Welten:



- Amazon selbst
- Amazon Warehouse Deals
- Amazon Marketplace.

Amazon ist der normale Handelsplatz, auf dem Ihr direkt bei Amazon Ware kauft. Amazon Warehouse Deals ist ähnlich, nur, dass Ihr hier von Amazon gebrauchte, von anderen Kunden zurückgegebene und wieder aufbereitete Ware kauft.

Amazon Marketplace aber ist etwas ganz anderes: Amazon bietet anderen Händlern eine Handelsplattform. Die können nach Freischaltung dort Waren anbieten, Amazon selbst übernimmt nur die Abwicklung des Kaufs. In wenigen Fällen auch des Versandes. Meist aber ist der Händler selbst dafür verantwortlich. Wenn Ihr nicht genau darauf achtet, dann kommt es schnell vor, dass Ihr Ware bei einem anderen Händler mit weniger Service bestellt.

- Amazon sortiert Händler, die schlechte Beurteilungen bekommen, rigoros aus und entzieht ihnen die Verkaufsberechtigung.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Ebenso schnell sind aber neue Händler angemeldet, die dieselben Produkte verkaufen.
- Wenn Ihr hier ein Problem habt, dann könnt Ihr über Amazon einen sogenannten **A-Z Garantieantrag** starten, direkt aus der Bestellung.
- Amazon übernimmt dann die weitere Abwicklung und schreibt Euch meist das Geld gut.

Bestellungen aus dem Ausland/Zoll/Plagiate

Ob nun bei Amazon Marketplace, eBay oder einem Onlinehändler mit nicht so klarer Kennzeichnung: Wenn Ihr Ware aus dem Ausland bestellt, dann bringt das nicht nur längere Versandzeiten mit sich, sondern auch das Risiko der Zollerhebung.

Ware, die nicht aus dem EU-Wirtschaftsraum kommt, muss verzollt werden. Entweder müsst Ihr bestellte und schon bezahlte Ware dann beim Zollamt gegen eine Zahlung auslösen, oder der Paketdienst kassiert die Abgaben bei der Auslieferung ein.

- Prüft sorgfältig die Angebote (beziehungsweise das Impressum der Webseite, von der Ihr kauft), um Euch über die Herkunft der Ware klar zu sein.
- Das kann durchaus Sinn machen: Ware von verlässlichen Händlern aus dem Ausland kann durchaus deutlich günstiger sein als von einem heimischen Händler.
- Ihr solltet Euch nur bewusst darüber sein, dass Lieferzeit, Zusatzkosten und gegebenenfalls problematischere Rückgabe oder Garantieabwicklung damit einhergehen können. Kalkuliert das einfach in die Preisabwägung ein!

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Bitter wird es, wenn Ihr übergünstig Markenware kauft: Die ist oft nicht echt, sogenannte Plagiate. Viele Hersteller haben beim Zoll Zurückhalteverfügungen hinterlegt: Der Zoll kassiert die Ware ein, sendet sie an den Hersteller, und Ihr schaut in die Röhre. Die Hersteller geben die Ware nur frei, wenn sie eineindeutig echt ist. Oft erst nach Wochen, wenn überhaupt.

Wenn ausländische Sendungen sich nicht mehr bewegen

Dank des Internets bestellen wir immer mehr auch im Ausland. Auch wenn Ihr beim Versand eine Trackingnummer bekommen habt, bewegen sich Pakete manchmal nicht mehr. Das hat Gründe! Bevor Ihr also von einem Fake-Kauf ausgeht und reklamiert, solltet Ihr erst einmal genauer hinschauen.

Immer auf einem verfolgbaren Versand bestehen

Manchmal steht es im Kleingedruckten: Wenn Ihr bei der Bestellung den Standardversand wählt - der meist erfreulich günstig ist - dann habt Ihr keine Versicherung und auch keine Nachverfolgbarkeit. Das ist zum einen unangenehm, weil Ihr keinerlei Übersicht habt, ob und wann das Paket ankommt Noch schlimmer aber: Wenn es verloren geht, dann verweigert der Versender meist einen Ersatz. Ihr hättet für die Versicherung ja schließlich mehr zahlen können. Auch PayPal verweigert in solchen Fällen oft den Käuferschutz.

Darum: Wenn Ihr eine Sendung mit einem gewissen ideellen oder monetären Wert habt, investiert besser ein wenig mehr in die Versandoption!

Tracken einer Sendung

Einfach ist es, wenn der Versender internationale Unternehmen wie DHL, UPS, FedEx, TNT oder andere verwendet: Diese haben jeweils ein

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Tracking-Portal, in dem Ihr die Sendung vom Versand bis zur Zustellung verfolgen könnt, unabhängig von der Zahl der Länder, die diese durchreist.

- Wenn in der Versandnachricht kein expliziter Trackinglink vorhanden ist, dann ruft manuell die Webseite des Versenders auf.
- Wählt Eure Sprachversion aus, diese hat nichts mit dem Land des Versenders zu tun. Auf der Seite von UPS Deutschland könnt Ihr eine US-amerikanische Sendung genauso verfolgen wie auf der US-Seite!
- Alternativ nutzt Dienste wie Aftertrack, die das Tracking von Sendungen der unterschiedlichsten Paketdienste und Transporteure weltweit übernehmen.

Lokal versendet, international verloren?

Richtig ärgerlich wird es aber, wenn Ihr eine Sendung habt, die über einen lokalen Versender, etwa der Australischen Post oder dem amerikanischen USPS, aufgegeben wurde. Da könnt Ihr wie oben beschrieben das Tracking des Versenders nutzen, nur scheint sich das

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Paket ab einem gewissen Zeitpunkt nicht mehr zu bewegen. Dann nämlich, wenn es das Ursprungsland verlassen hat und im Zielland angekommen ist. Dann findet Ihr nur den Status "Wurde an die Zustellorganisation im Zielland übergeben", aber keine weitere Bewegung mehr.

- In einem solchen Fall ruft einfach mal die Seite von DHL oder Hermes (die meist die Zustellung solcher Sendungen übernahmen) auf
- Gebt dort die Paketnummer ein und schaut, ob die Sendung dort verfolgbar ist, die Wahrscheinlichkeit ist hoch!
- Dieses Tracking funktioniert nur erst nach der Übergabe an den deutschen Paketdienst. Vorher bekommt Ihr eine Fehlermeldung.
- Oft findet Ihr nur hier die Information, dass die Sendung bereits in einer Filiale liegt und darauf wartet, dass Ihr sie durch Zahlung der Einfuhrabgaben befreit!

Ihr seht also: Es gibt unterschiedliche Möglichkeiten, eine Sendung aufzuspüren. Die Wahrscheinlichkeit, dass sie wirklich verloren ist, ist sehr gering!

Crowdfunding – Schnäppchen mit Risiko

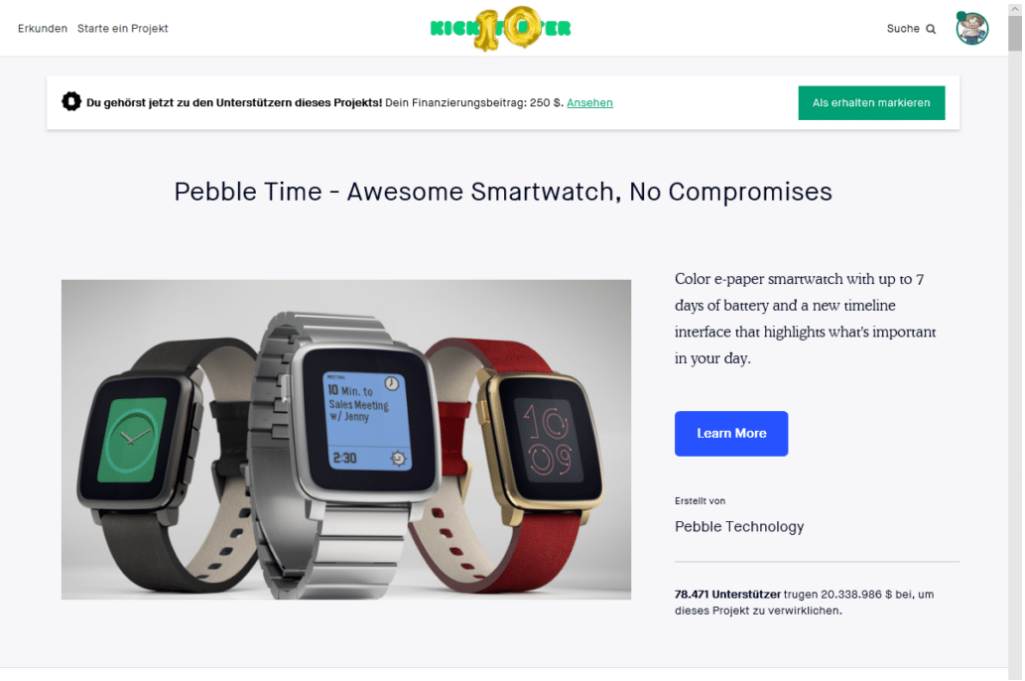
Crowdfunding ist ein Modebegriff, der nach Schnäppchen und Innovation klingt. Seiten wie Kickstarter und Indiegogo versprechen Innovationen zu einem Bruchteil des späteren Marktpreises. Ihr seid als Käufer quasi früher Investor und Käufer zum Sonderpreis. Das kann funktionieren, ist aber nicht ohne Risiko: Die "verkauften" Produkte sind in der Regel weder produziert noch vollständig getestet. In den meisten Fällen geht es darum, den Unternehmen eine Anschubfinanzierung

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

zukommen zu lassen. Als Belohnung winkt früher Zugriff auf das Produkt und ein günstigerer Preis. Verlockend, aber auch risikobehaftet!

- Über eines solltet Ihr Euch auf jeden Fall klar sein: Crowdfunding, übersetzt "Finanzierung durch die Masse", ist etwas komplett anderes als ein Kauf bei einem Online-Händler oder ein Einzelhandel.
- Es gibt viele Kampagnen, die erfolgreich und für die Teilnehmer sehr zufriedenstellend gelaufen sind. Ein Beispiel ist hier sicherlich die Pebble-Smartwatch. So erfolgreich, dass die Marke mittlerweile vom Konkurrenten Fitbit übernommen wurde.
- Viele Kampagnen aber laufen ganz anders. Zum Zeitpunkt der Beteiligung der Käufer ist oft nur ein Prototyp vorhanden. Der Kampagnenführer weiß also gerade mal, dass das Produkt funktionieren kann. Nicht aber, wie eine Massenfertigung funktioniert, welche Probleme bei mehr Nutzern auftreten etc. Und so kommt es nicht selten vor, dass das Produkt verspätet, mit anderem (oft geringerem) Leistungsumfang oder sogar gar nicht bei den Käufern ankommt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen



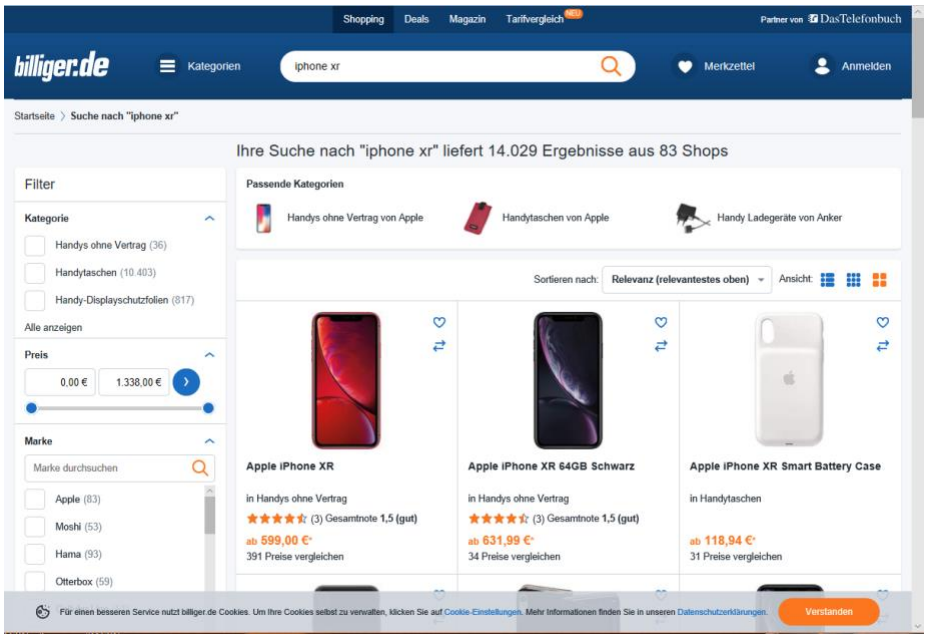
- Kickstarter wie auch Instagram weisen in ihren AGB darauf hin. Eine Haftung oder gar Rückabwicklung ist nicht möglich.
- So reizvoll ein tolles neues Smartphone mit bisher noch nicht gesehenen Features für kleines Geld auch sein mag: Seid Euch bewusst, dass Crowdfunding etwas komplett anderes ist als der Kauf eines bereits im Handel befindlichen Produkts!

Immer beste Preise? Schnäppchenportale

Ob Ihr nun online einkauft oder in die Stadt geht und dort bummelt: Die Preise der Waren, die Ihr kaufen wollt, sind entscheidend, genauso deren Verfügbarkeit. Wo früher Schnäppchenjäger durch die Läden gehuscht sind und Preise verglichen haben, machen das heute ausgeklügelte Algorithmen. Die Angebote verschiedenster Online-Shops werden automatisch abgefragt und einander gegenübergestellt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Bekannte Vertreter dieser Services sind idealo.de (http://www.idealo.de), CHECK24 (http://preisvergleich.check24.de) und billiger.de (http://www.billiger.de).
- Ruft eine der Seiten auf, gebt in das Suchfeld die gesuchte Ware ein, und Ihr bekommt eine Preisübersicht zurück.
- Gegebenenfalls müsst Ihr noch ein wenig weiter eingrenzen (ein iPhone beispielsweise gibt es in verschiedenen Modellen, die in verschiedenen Farben und Speichergrößen), dann bekommt Ihr die Angebote aller durchsuchten Shops für das gewünschte Produkt.



- Der Vorteil: Neben den Suchergebnissen findet Ihr noch Angaben zu dem jeweiligen Online-Shop. Dort könnt Ihr auf einen Blick sowohl die Reputation (aus der durchschnittlichen Kundenbewertung) als auch die Lieferbarkeit erkennen.

Der Kauf findet dann tatsächlich im Shop des Anbieters statt. Wundert Euch nicht: Lieferbarkeit wie auch Preis können von den

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Suchergebnissen abweichen: Preise ändern sich gerade online sehr schnell und sind bei den Suchmaschinen immer nur so aktuell wie die verwendete Datenbasis.

Nicht jede Preis-Suchmaschine durchsucht dieselben Shops, es macht also Sinn, bei einem größeren Kauf gleich mehrere der Anbieter zu verwenden, um den tatsächlich günstigsten Preis zu finden. Auch kleinere Anbieter wie beispielsweise Dealbunny (https://www.dealbunny.de) haben hier Vorteile!

Ebay Kleinanzeigen: Chance und Risiko

Ebay ist als Marktplatz kaum noch wegzudenken: Kaum ist das neue Gerät da, wandert das andere

Sicherheitswarnungen bei eBay Kleinanzeigen

eBay Kleinanzeigen erfreut sich immer größerer Beliebtheit. Was aber, wenn plötzlich eine Sicherheitswarnung in den Posteingang flattert? Reagieren solltet Ihr in jedem Fall!

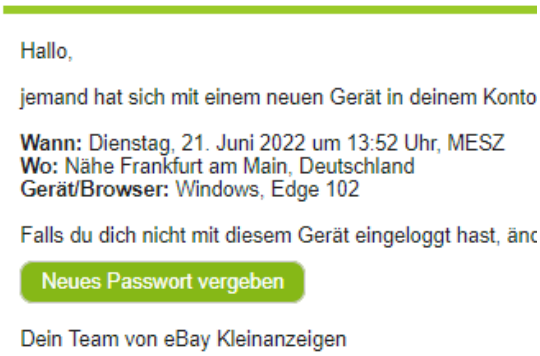
Lange Zeit war eBay Kleinanzeigen der kleine, schmuddelige Bruder der großen eBay-Seite für den lokalen Einkauf vor Ort. Steigende Gebühren bei eBay für Verkäufer und auf der einen und die Möglichkeit des Versands über Kleinanzeigen auf der anderen Seite haben das geändert. Viele Anwender empfinden den Umgang und die Abwicklung hier deutlich angenehmer. Was aber zu beachten ist: Es findet auch viel Betrug über die Plattform statt! Übernommene Accounts, Zahlungsaufforderungen ohne Absicherung und mehr sind nicht selten.

Da sorgt eine Sicherheitswarnung per E-Mail schnell für Unruhe. Damit teilt eBay Kleinanzeigen Euch mit, dass eine Anmeldung an Euren Account erkannt wurde, die nicht dem üblichen Muster entspricht.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Ignoriert diese E-Mail nicht, sondern schaut genau in den Inhalt.

- Habt Ihr Euch gar nicht zum angegebenen Zeitpunkt angemeldet? Dann solltet Ihr umgehend Euer Kennwort ändern, denn diese E-Mail kommt immer nur nach einer erfolgreichen Anmeldung, Benutzername und Kennwort waren bei der Anmeldung korrekt.



- Habt Ihr Euch zu dem Zeitpunkt angemeldet, aber der Ort scheint falsch? Der Ort der Anmeldung wird automatisch aus der IP-Adresse bestimmt. Die kann durchaus eine gewisse geografische Streuung haben. Seiten wie dein-ip-check.de zeigen Euch an, welcher Ort für Euch gerade erkannt wird. Wenn das mit der Angabe der E-Mail übereinstimmt, ist alles gut. Wenn nicht: Ändert vorsichtshalber das Kennwort.

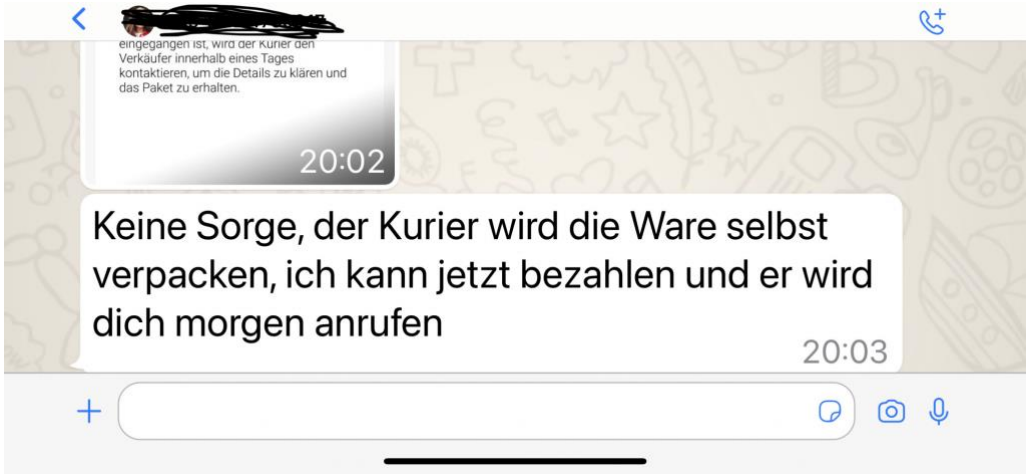
Angebote bei eBay Kleinanzeigen per Spedition

Es klingt so gut: Kaum ist das alte Fahrrad zum Verkauf online, da meldet sich ein Interessent: Sofortige Zahlung, Abholung per Spedition bietet er an. Vorsicht: Meist ist das ein Betrugsversuch!

eBay selbst hat lange auf ein eigenes Zahlungssystem umgestellt. Die Käufer zahlen an eBay, eBay leitet die Zahlung an den Verkäufer weiter. Das mag auf der einen Seite an einem gewissen Kontrollzwang von eBay selbst liegen, schützt aber auch Käufer und Verkäufer gleichermaßen.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

eBay steht als Zwischenstation auch für die Echtheit der Zahlungsvorgänge ein.



Anders sieht es bei eBay Kleinanzeigen aus: Käufer und Verkäufer kommunizieren direkt miteinander, unkontrolliert und offen für Betrugsmaschen. So sind Account-Übernahmen nicht selten, und auch der Zahlungsvorgang wird angegriffen. Fake-Käufer sind hier ein echtes Problem!

- Käufer - in den meisten bekannten Fällen vom Profilbild her junge, gut aussehende Frauen - melden sich per WhatsApp und bieten an, die sperrige Ware sofort zu bezahlen und dann von einer Spedition abholen zu lassen.
- Weil sie weiter weg wohnen, keine Transportmöglichkeit haben. Danach gibt es verschiedene Vorgehensmodelle:
- Ihr sollt die IBAN schicken, damit die Überweisung erfolgen kann. Kurze Zeit später kommt dann eine Bestätigung "Deiner Bank", dass der Betrag eingegangen sei.
- Diese Bestätigung ist gefaked, aus der IBAN lässt sich ja die Bank auslesen und einfach eine vermeintlich echte E-Mail fälschen. Die so erbeuteten IBAN werden verkauft oder missbräuchlich

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

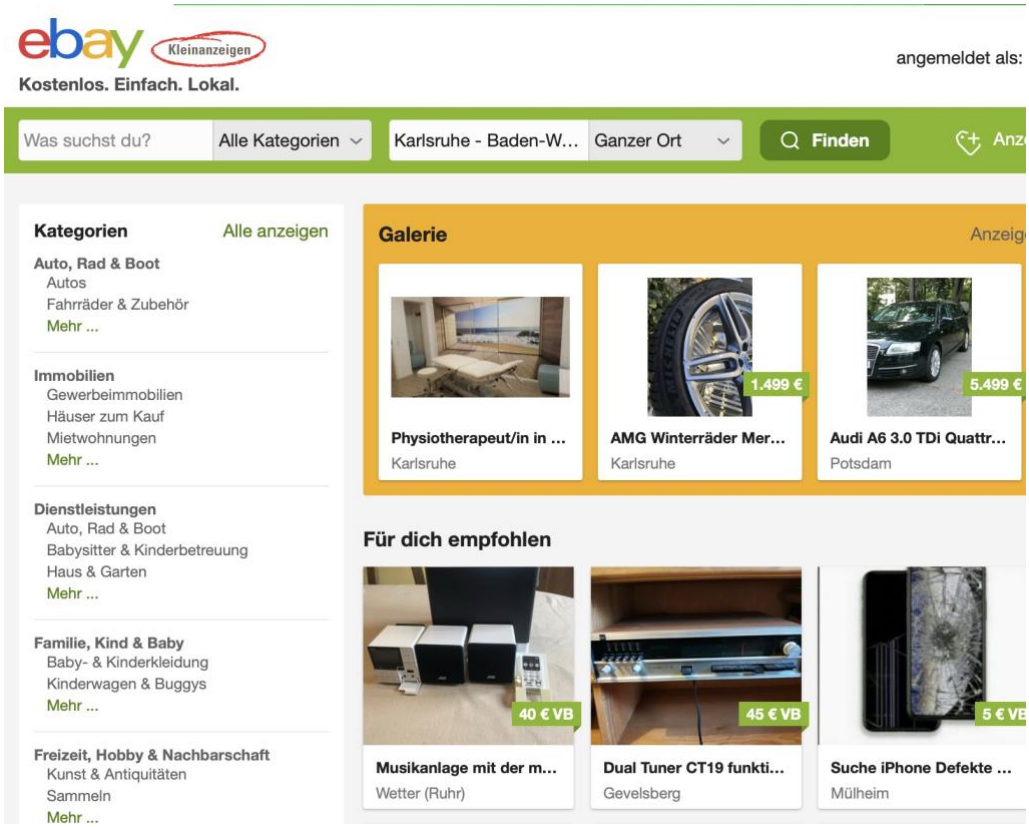
genutzt, die Ware schnell von einer vermeintlichen Spedition abgeholt. Eine weitere Vorgehensweise: Die Bestätigung enthält einen so hohen Betrag, der Käufer bittet um Rücküberweisung der Differenz.

Befolgt immer die einfache Regel: Erst das Geld (in der Hand oder selbst überprüft auf dem Konto), dann die Ware!

eBay Kleinanzeigen: PayPal und Fake Käufer

Der Kauf im Internet ist immer auch Vertrauenssache. Die reine Sicherheit der Plattform ist dabei nur eine Facette: Einer der großen Einflussfaktoren auf die Sicherheit ist der Benutzer. Wenn der seine Konten nicht absichert, dann ist die Übernahme durch Fake-Käufer ein Leichtes. In der Folge laufen über Euren Account plötzlich Verkäufe, mit denen Ihr nichts zu tun habt und bei denen dem Käufer natürlich nicht die gekaufte Ware geliefert wird. Reklamationen und weitere Schritte richten sich dann aber an Euch!

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen



- Leider bietet eBay Kleinanzeigen keine Zwei-Faktor-Authentifizierung an. Es bleibt Euch also nicht viel anderes, als das Passwort regelmäßig zu wechseln.
- Aufgrund der vielen Datenlecks ist die Wahrscheinlichkeit hoch, dass Ihre Standardkombination von E-Mail-Adresse und Kennwort schon weithin bekannt ist: Nutzt für Dienste, die keine zusätzlichen Sicherheitsmechanismen bieten, ein eigenes, komplexes Kennwort.
- Als Käufer könnt Ihr Euch zwar nicht vollständig gegen Betrug schützen, aber zumindest im Falle eines Betrugs absichern: Zahlt per PayPal, aber nicht per PayPal Freunde. Nur beim Standard-PayPal ("Zahlung für Ware oder Dienstleistungen") habet Ihr den

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Käuferschutz, der das vermeintlich verlorene Geld zurückbringen kann.

Richtig auf Fake-Anrufe reagieren

Tag für Tag, Stunde für Stunde rufen fremde Rufnummern an und melden sich nicht oder wollen Euch etwas verkaufen. Wir zeigen Euch, was Ihr dagegen machen könnt!

Werbeanrufe, Cold Calls, der Telefonanbieter oder der angebliche Microsoft-Service: Sie haben alle eines gemeinsam: Sie nutzen Eure Rufnummer und wollen Euch etwas verkaufen. Von Versicherungen über den vermeintlich optimierten Telefontarif bis hin zu einem Sicherheitsproblem auf Eurem Rechner, in den allermeisten Fällen handelt es sich um unerwünschte Anrufe. Die könnt Ihr nicht immer verhindern, aber zumindest weniger nervig machen.

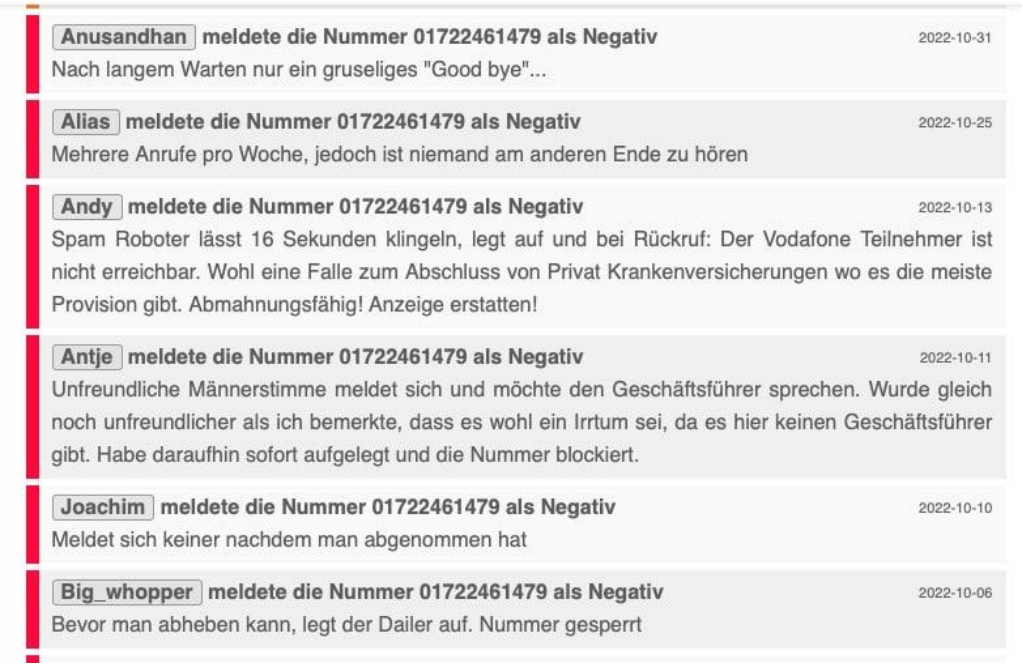
Unbekannte Nummer? Vorsicht!

Es ist natürlich nicht pauschal richtig, eine unbekannte Rufnummer gleich als verdächtig zu klassifizieren, aber achtet einmal darauf: Wie oft rufen Euch Rufnummern an, die nicht in Euren Kontakten sind. Und wie viele davon sind unerwünscht? In Zeiten der Smartphones und Kontaktverzeichnisse kommen bei vielen Anwendern die Anrufe meist von Personen, die in den Kontakten sind. Da seht Ihr statt der Nummer den Namen. Wie könnt Ihr hier ohne Risiko das Gespräch annehmen?

- Kontrolliert bei einem Anruf, ob Ihr die Nummer erkennt.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Wenn Ihr nicht auf einen Anruf wartet, der von einer unbekannten Nummer kommen könnte, dann hebt ab, sagt aber nichts.
- In 80% der Fake-Anrufe wird aufgelegt. Das liegt daran, dass das automatische Wahlprogramm keinen Teilnehmer erkennt. Oft wird die Nummer dann aus der Rufroutine gelöscht und Ihr habt Ruhe.
- Wenn ein echter Anrufer dran ist, fragt der nach einigen Sekunden nach, ob jemand dran ist. Das ist immer noch keine Garantie, dass es sich nicht um SPAM handelt, hat aber schon einmal eine Menge an SPAM aussortiert.



Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Anruferkennungen nachsehen

Wenn eine Rufnummer Euch mehrfach nervt, dann googelt sie einfach oder gebt sie direkt bei Webseiten wie werruft.info oder tellows.de ein.

- Wenn Ihr nicht über die meist werbeüberladenen Startseiten gehen wollt, dann könnt Ihr die Rufnummernidentifikation auch direkt über die Adressleiste des Browsers machen.
- Bei werruft.info gebt als Adresse *https://www.werruft.info/telefonnummer/<rufnummer>* ein.
- Bei Tellows gebt als Adresse *https://www.tellows.de/num/<rufnummer>* ein.
- Wenn Ihr schon eine Vielzahl von Negativmeldungen findet, dann handelt es sich mit hoher Wahrscheinlichkeit um eine SPAM-Nummer.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

Rufnummern sperren

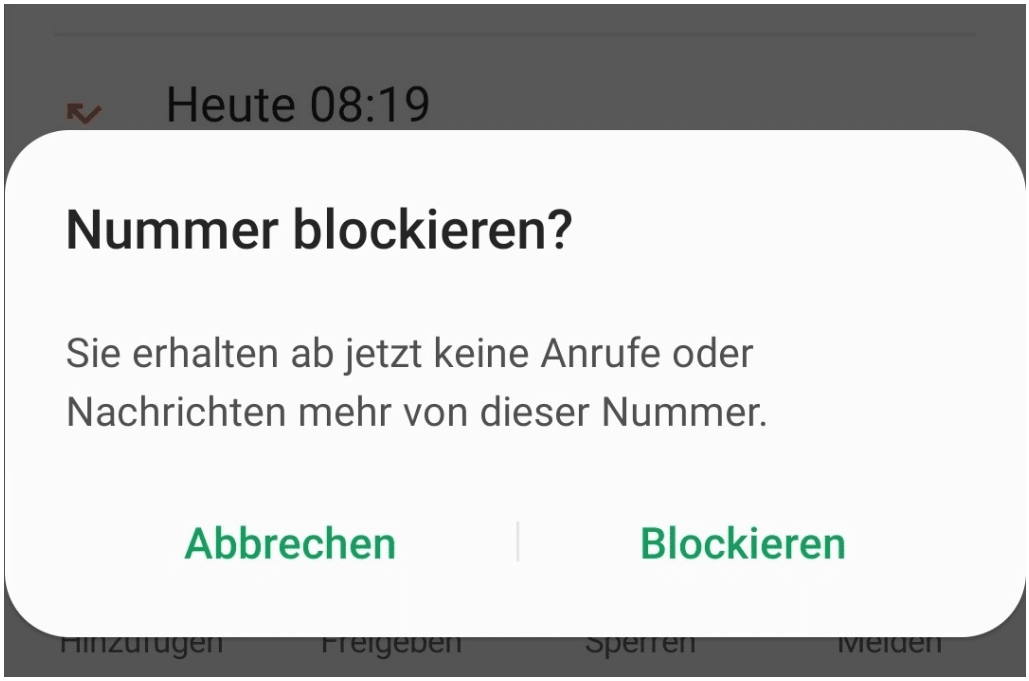
Damit aber nicht genug: Warum eine nervende Rufnummer immer wieder durchkommen lassen? Sperrt sie doch einfach!

- Jeder Router hat eine sogenannte Sperrliste, in die Ihr Rufnummern einsortieren könnt, die gar nicht erst an die Handapparate weitergehen, sondern im Router ausgesondert werden. Das funktioniert mit wenig Aufwand und ist sehr effektiv.

Smartphones bieten ebenfalls einen solchen Filter:

- Zum Blockieren der Rufnummer tippt diese Nummer in der Rufliste an.
- Dann tippt auf das kleine **i** neben den Symbolen unter der Rufnummer.
- Rollt ganz nach unten auf der Seite. Dort tippt bei einem Android-Smartphone auf **Blockieren**. Bei iOS tippt auf **Anrufer blockieren**.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen



- Zur Sicherheit müsst Ihr die Blockierung jetzt noch einmal bestätigen, dann ist sie aktiv.
- Wenn Ihr feststellt, dass die Rufnummer doch wichtig war, dann könnt Ihr sie natürlich auch wieder entsperren. Dazu wählt statt **Blockieren** dann **Entsperren**.

Rufnummernsperren am Router

Der Router fungiert neben vielen anderen Aufgaben auch als Telefonzentrale. Damit laufen die Anrufe auch zuerst am Router auf und werden dann an die Endgeräte weitergegeben. Bei einer Fritz!Box könnt Ihr diese Weiterleitung beeinflussen, auch wenn das nicht ganz intuitiv möglich ist, bei anderen Routerherstellern geht das meist auf ähnlichem Weg.

Schluss mit all dem Fake: So erkennt Ihr die Fälschungen

- Klickt auf **Telefonie** > **Anrufe**, dann sucht die zu sperrende Rufnummer aus der Anrufliste heraus.
- Klickt dann auf das Symbol mit dem **Adressbuch** ganz rechts neben der Rufnummer.
- Achtet dann darauf, dass Ihr statt auf **Telefonbuch** auf **Rufsperren** klickt. Anrufe von den dort aufgenommenen Rufnummern werden gar nicht mehr an die Telefone weitergeleitet, sondern direkt verworfen. Solange die Anrufer ihre Rufnummer nicht variieren, habt Ihr Ruhe.