Geldbewusst durchs Leben.

Leitfaden: Digitale Geldfallen erkennen

Dich mit den häufigsten Geldfallen im Internet auszukennen, hilft dir dabei, dein Geld besser unter Kontrolle zu behalten und nicht auf Betrüger*innen reinzufallen. Wie du die Warnsignale erkennst, *bevor* dir im Internet das Geld aus der Tasche gezogen wird, erfährst diesem Leitfaden.

Abo-Fallen

Im Internet werden viele Dienstleistungen und Informationen gratis angeboten. Manchmal sind sie aber nur auf den ersten Blick wirklich kostenlos. Bei vielen Websites muss man sich anmelden, um an die Information zu kommen, die man haben möchte. Du kennst das vielleicht von Online-Zeitungen: Du kannst einen Artikel nur bis zur Hälfte lesen, bevor du aufgefordert wirst, ein kostenpflichtiges Abo abzuschließen.

Bei vielen Plattformen, die mit „gratis" Mitgliedschaften werben, ist das allerdings nicht klar: Sie verstecken die Kostenhinweise oft **irgendwo im Kleingedruckten**. So übersiehst du, dass du mit der Anmeldung ein Abo abschließt und bekommst plötzlich eine Rechnung. Auch kostenlose Testphasen mit automatischer Verlängerung können schnell zu ungewollten Abonnements führen.

Klassische Beispiele für Abo-Fallen sind:

- Streaming-Plattformen, die kostenlose Filme oder Serien anbieten.
- Wissenstests, Persönlichkeitstests, etc., bei denen man sich anmelden muss.
- Gratis Mitgliedschaften, die nach einem Probemonat automatisch in eine kostenpflichtige Mitgliedschaft übergehen.

Was tun?

- Achte auf **versteckte Kostenhinweise** im Kleingedruckten.
- Gib **keine Kreditkartendaten** an, wenn du nichts bezahlen möchtest.
- Hinterfrage, wofür diese Website/diese Plattform deine persönlichen Daten braucht, wenn doch **angeblich alles gratis** ist.
- Wenn du *wirklich* nur die gratis Testphase nutzen möchtest, stell dir im Kalender eine Erinnerung ein, damit du das Abo auch **rechtzeitig kündigst.** Achte besonders auf die Kündigungsbedingungen.
- Wenn du in eine Abo-Falle getappt bist, wende dich an die Internet Ombudsstelle.

Billigprodukte aus China

Temu, SHEIN, AliExpress, Wish – das ist nur ein kleiner Teil der bekannten Online-Shops mit auffallend günstigen Preisen und einer riesigen Auswahl an Produkten von Elektronik über Kleidung und Haushaltsware bis zu Schmuck. Leider warten hier gleich mehrere Geldfallen auf Nutzer*innen:

Die Produkte sind oft schlecht verarbeitet, die **Qualität** mehr als mangelhaft. Die Fotos auf den Websites entsprechen häufig nicht dem, was tatsächlich bei dir ankommt. Gerade bei Mode ist der Einkauf in diesen Shops wie eine Lotterie: Abgesehen von Qualität, Material und Aussehen sind auch die Größen anders als in Europa. Du kannst dich also nicht darauf verlassen, dass du bekommst, was du bestellt hast. Im schlimmsten Fall sind die Produkte sogar **gefährlich oder gesundheitsschädigend**, weil sie nicht den europäischen Sicherheitsstandards entsprechen.

Auch sind die **Lieferzeiten** unberechenbar und können von Wochen bis hin zu Monaten reichen. Der Lieferweg ist schließlich lang – dies ist auch mit negativen Konsequenzen für die **Umwelt** verbunden. Manchmal bleiben Produkte beim **Zoll** hängen und es kommen zusätzliche Kosten auf dich zu, die ebenfalls schwierig im Vorhinein abzuschätzen sind.

Rücksendungen sind nur manchmal möglich. Es kann sein, dass du die Kosten dafür selbst tragen musst – das zahlt sich meistens nicht aus, da die Produkte günstiger sind als die Rücksendekosten nach China. Und so behalten viele Kund*innen ihre Bestellungen, mit denen sie eigentlich unzufrieden sind.

Was tun?

- Frage dich, unter welchen **Arbeitsbedingungen** solche Produkte hergestellt werden. Wie viel können die Angestellten noch verdienen, wenn du ein T-Shirt um 2€ kaufst?
- Rechne die Einfuhrumsatzsteuer und eventuelle Zollgebühren mit in den Preis hinein.
- Lies dir **Bewertungen** durch, aber behalte im Hinterkopf, dass diese auch häufig gefälscht werden, um das Produkt besser wirken zu lassen.
- Kaufe auf keinen Fall **Produkte, bei denen es um deine Sicherheit** geht (Rauchmelder, Helme, Schutzkleidung etc.) billig über Chinashops ein.
- Rechne immer damit, dass dein Produkt entweder **gar nicht oder mit starken Mängeln** bei dir ankommt.

Scheingewinne & Fake-Gewinnspiele

Besonders auf Facebook und WhatsApp kursieren immer wieder gefälschte Gewinnspiele. Oft geht es um ein Tiny House oder einen topmodernen Camper. Manchmal geben sich die Fake-Firmen auch als bekannte Unternehmen aus und verlosen zum Beispiel einen vermeintlichen 250€ Gutschein oder eine tolle Reise. Die Unternehmen fordern dich häufig dazu auf, auf einen Link zu klicken, ein paar Fragen zu beantworten, das Gewinnspiel zu teilen und zu kommentieren. So kommen die Betrüger*innen zu deinen Daten.

Was tun?

- Suche nach einem **Impressum** oder einer Kontaktmöglichkeit.
- Achte auf **Rechtschreib- und Grammatikfehler.**
- Checke die **echten Social-Media-Seiten des Unternehmens** und schaue nach, ob das Gewinnspiel auch dort aufscheint.
- Gib niemals deine **Kreditkartendaten** bekannt.
- Klicke auf keine dubiosen **Links.**

Künstliche Verknappung

Du hast es sicher schon einmal gesehen: Bei einem Kleidungsstück, Produkt oder Hotelzimmer erscheint im Onlineshop die Nachricht:

> "Nur noch zwei Stück/Zimmer/Plätze verfügbar!"

Um das gewünschte Produkt noch schnell zu ergattern, schlägst du sofort zu, bevor es jemand anderer tut – auch, wenn du es dir eigentlich noch überlegen wolltest. Doch Achtung: **Manchmal wird diese Knappheit bewusst erzeugt und stimmt eigentlich gar nicht.** Aber warum? Onlineshops wollen, dass du eine schnelle (und damit oft unüberlegte) Kaufentscheidung triffst.

Was tun?

- Kaufe im besten Fall nicht unter Zeitdruck, sondern mache dir eine Liste und erfülle dir einen Wunsch, wenn du das Budget dazu hast.
- Lasse dich nicht von künstlichen Verknappungen unter Druck setzen. Mache dir bewusst, dass diese Info in vielen Fällen falsch ist.

Weitere digitale Geldfallen

- **Fakeshops** täuschen Konsument*innen mit einer gefälschten, oft trügerisch echt aussehenden Verkaufsplattform. Auf den ersten Blick sind Fakeshops nicht von anderen Online-Shops zu unterscheiden, denn Produktfotos und Beschreibungen sind in der Regel von diesen geklaut. Produkte, die über einen Fakeshop gekauft werden, werden vorab bezahlt, allerdings nie geliefert.
- Bei **Phishing** handelt es sich um betrügerische E-Mails, SMS oder Websites. Dabei versuchen Betrüger*innen entweder direkt an dein Geld zu kommen, indem sie dich auf emotionaler Ebene überzeugen, ihnen Geld zu überweisen oder sie versuchen, dir sensible Daten wie Kreditkartenummern oder PINs zu entlocken. Ein häufiges Beispiel ist eine gefälschte Nachricht einer Bank, in der du aufgefordert wirst, den Online-Banking-Zugang einzugeben. Es gibt auch SMS, die vortäuschen, dass ein Paket nur nach Angabe persönlicher Daten zugestellt werden kann. Diese Daten werden dann geklaut.

- Hinter **Freemium**-Angeboten steckt ein Geschäftsmodell, das darauf aufgebaut ist, grundlegende Funktionen einer App, eines Spiels oder einer Plattform zunächst kostenlos anzubieten. Hat man sich diese aber erst einmal heruntergeladen, wird man schnell dazu verleitet, Mikro-Transaktionen in der App zu tätigen (sogenannte In-App-Käufe).
- Zu **Influencer*innen** haben wir oft ein größeres Vertrauen, da wir sie vermeintlich besser kennen als eine beliebige Person in der Fernsehwerbung. Sie teilen ihr Leben mit uns und würden uns daher auch nur Produkte empfehlen, die wirklich gut sind, oder? **Leider nicht immer.** Zum Beispiel machen bekannte Influencer*innen mitunter Werbung für SHEIN, ein Ultra-Fast-Fashion-Konzern mit unter ausbeuterischen Bedingungen produzierter Massenware in schlechter Qualität.

- **Cookies** speichern persönliche Nutzer*innendaten, wie zum Beispiel das Surfverhalten (also welche Websites besucht, welche Videos geschaut und welche Links geklickt werden). Mithilfe dieser Informationen kann Werbung noch gezielter auf Nutzer*innen und deren persönliche Interessen abgestimmt werden. Das merkst du z. B. daran, dass genau jene Produkte in Werbebannern etc. angezeigt werden, die du vor Kurzem im Internet gesucht hast. Teilweise werden auch höhere Preise angezeigt, wenn du dir eine Seite oder ein Produkt häufiger ansiehst.

Ausführlichere Informationen und Tipps für den Umgang mit diesen Geldfallen findest du in der Broschüre „Externe Einflüsse erkennen".

SCAN ME

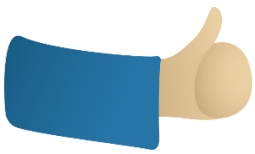
Sicheres Online-Shopping – so geht's!

Nachdem du jetzt die wichtigsten Geldfallen im Internet kennengelernt hast, möchten wir dir noch einige Tipps fürs Online-Shopping mitgeben. Wie immer gilt: Überlege dir gut, was du wirklich brauchst, denn die Verführungen im Internet sind groß.

1. **Prüfe das SSL-Zertifikat.**

SSL steht für "Secure Sockets Layer" und ist ein Hinweis darauf, dass eine Website für den Einkauf sicher ist. Diese Verschlüsselungsmethode sollte eigentlich jede Website nutzen, auf der sensible oder persönliche Daten wie z. B. Kreditkartendaten abgefragt werden. Ob eine Online-Shopping-Website über ein aktuelles SSL-Zertifikat verfügt, erkennst du am Schlosssymbol in der URL-Leiste deines Webbrowsers bzw. daran, ob die URL mit *https* und nicht mit *http* beginnt (das S steht für "sicher").

2. **Suche nach einer Datenschutzerklärung.**



In der Datenschutzrichtlinie wird erklärt, wie das Unternehmen sensible Daten erfasst, verwendet und speichert. Auch wenn es hierzu weltweit unterschiedliche Gesetze und Vorschriften gibt, sollten seriöse Online-Händler eine eindeutige Datenschutzerklärung haben.

3. **Suche nach einer Adresse und Telefonnummer.**

Bei seriösen Online-Shops befindet sich in der Regel eine Telefonnummer und eine Kontaktadresse in der Kopf- oder Fußzeile bzw. im Impressum. Wenn du Zweifel hast, ob ein Online-Shop echt ist, gib die Adressdaten in eine Suchmaschine ein, um zu sehen, ob es die Adresse wirklich gibt. Unseriöse Händler*innen geben entweder gar keine oder eine gefälschte Adresse an.

4. **Achte auf Rechtschreibung und Grammatik.**

Schlecht geschriebene Websites mit zahlreichen Rechtschreib- und Grammatikfehlern sollten dich stutzig machen. Auch Bilder von schlechter Qualität sind ein Warnhinweis.

5. **Prüfe, ob es verschiedene Zahlungsoptionen gibt.**

Kreditkarten gelten als eine der sichersten Methoden für Online-Transaktionen. Gibt es nur Sofortüberweisung als Zahlungsmethode, solltest du vorsichtig sein. Gute Online-Shops bieten ihren Kund*innen verschiedene Zahlungsmöglichkeiten an.

6. **Nutze sichere Passwörter und schütze sie.**

Sichere und unterschiedliche Passwörter für die einzelnen Online-Konten sind zwei der wichtigsten Maßnahmen, die du für sicheres Online-Shopping ergreifen kannst. Sich viele verschiedene Passwörter zu merken, vor allem, wenn sie aus vielen Buchstaben, Zahlen und Sonderzeichen bestehen, ist natürlich nicht ganz einfach. Aber dafür gibt es Passwortmanager. Ein guter Passwortmanager verschlüsselt außerdem die Passwörter, die sonst im Klartext vorliegen.

7. **Nutze beim Online-Shopping kein öffentliches WLAN.**

Cafés, Hotels, Restaurants und andere öffentliche Einrichtungen bieten oft einen kostenlosen WLAN-Zugang an. Du solltest beim Online-Shopping außerhalb von zuhause aber besser deine mobile Internetverbindung nutzen, da öffentliches WLAN nicht gut gesichert ist und Cyberkriminelle leichter deine Daten abfangen können.

8. **Achte darauf, dass dein Computer ein Anti-Viren-Programm verwendet.**

Diese Programme können dich auf gefährliche Websites hinweisen oder nicht vertrauenswürdige Links blockieren.

Weitere Informationen und hilfreiche Links

- Online-Geldfallen im Überblick: watchlist-internet.at
- Fakeshop Detector: fakeshop.at/shopcheck
- Internet Ombudsstelle: ombudsstelle.at
- Informationen zu Einfuhrumsatzsteuer und Zoll: post.at/p/c/import
- Kritik an SHEIN: greenpeace.de/engagieren/nachhaltiger-leben/shein
- SHEIN-Influencer*innen: zdf.de/funk/simplicissimus-12075/funk-exposed-wie-influencer-sich-an-shein-verkaufen-102