

SO BEZAHLEN SIE SICHER BEI ONLINE-EINKÄUFEN



Achtung, Köder im Netz:
Durch diverse Tricks versuchen Betrüger an Ihr Geld und an Ihr Konto zu kommen.

Vorwort



Liebe Anwenderinnen und Anwender,

Die Adventszeit naht, die Geschäfte locken mit festlicher Dekoration und verlockenden Angeboten. Viele von uns nutzen die Gelegenheit, um Weihnachtsgeschenke bequem online zu bestellen. Doch gerade jetzt, wo der Black Friday mit seinen vermeintlichen Schnäppchen lockt, ist Vorsicht geboten! Denn neben seriösen Händlern tummeln sich auch Betrüger im Internet, die mit gefälschten Online-Shops ahnungslose Käufer in die Falle locken wollen.

Um Ihnen einen sicheren und entspannten Online-Einkauf zu ermöglichen, habe ich Ihnen die wichtigsten Tipps zusammengestellt, wie Sie Fake-Shops erkennen und sich vor Betrug schützen können.

Ihr Kaner Etem

Wie Sie nicht auf Fake-Shops hereinfliegen

1. Die Webadresse genau unter die Lupe nehmen:

Misstrauen Sie unvollständigen Adressen, ungewöhnlichen Domainendungen, die Sie nicht zuordnen können, oder Schreibfehlern.

Achtung: Auf das „grüne Schloss“ bei Webadressen zu achten ist ein weitverbreiteter Tipp. **Aber:** Das signalisiert nur, dass die Verbindung zwischen Ihnen und der Webseite verschlüsselt ist. Es hat jedoch keine Aussage darüber, ob ein Online-Shop seriös ist oder böse Absichten hat!

2. Das Impressum auf Herz und Nieren prüfen:

Jeder seriöse Online-Shop verfügt über ein vollständiges Impressum mit folgenden Angaben:

- Name und Anschrift des Unternehmens (idealerweise in Deutschland oder Österreich)
- Telefonnummer und E-Mail-Adresse
- Umsatzsteuer-Identifikationsnummer (USt-IdNr.)

Sollten diese Informationen fehlen oder unvollständig sein, ist Vorsicht geboten!

3. Kundenbewertungen:

- Recherchieren Sie den Shop im Internet, z.B. indem Sie den Namen des Shops zusammen mit dem Begriff „Erfahrungen“ in eine Suchmaschine eingeben.
- Lesen Sie Kundenbewertungen aufmerksam und achten Sie dabei besonders auf kritische Stimmen.
- Vorsicht bei ausschließlich positiven Bewertungen! Diese könnten gefälscht sein.
- Vertrauen Sie nicht blind auf Bewertungen auf der Shop-Seite selbst, da diese vom Shop-Betreiber manipuliert sein könnten.

4. Sichere Zahlungsmethoden wählen:

- Bietet der Shop ausschließlich Vorkasse an? Dann Finger weg! Bei Vorkasse und Betrugsfällen ist Ihr Geld in der Regel verloren.
- Auch bei Kreditkartenzahlung als einziger Option ist Vorsicht geboten. Im Betrugsfall erhalten Sie zwar meist Ihr Geld zurück, dies ist jedoch mit bürokratischem Aufwand, Wartezeiten und möglicherweise einer Kartensperrung verbunden.

Seriöse Shops bieten eine Auswahl an sicheren Zahlungsoptionen. Diese sind:

- PayPal
- Klarna
- oder Kauf auf Rechnung.

PayPal und Klarna sind Drittanbieter, die die Zahlung für Sie abwickeln und überwachen. Sollte es zu Problemen kommen (wie etwa: Ware nicht geliefert) erhalten Sie Ihr Geld zurück. Und beim Kauf auf Rechnung zahlen Sie erst, wenn Sie die Ware erhalten haben.

5. Unrealistische Angebote kritisch prüfen:

Erscheinen Ihnen die Preise unrealistisch niedrig? Vergleichen Sie die Preise mit denen anderer Anbieter, z.B. auf Preisvergleichsportalen wie idealo.de oder geizhals.de.

Denken Sie daran: Wenn ein Angebot zu gut klingt, um wahr zu sein, ist es das wahrscheinlich auch.

Vertrauen Sie Ihrem Bauchgefühl!

Wenn Sie trotz aller Prüfungen ein ungutes Gefühl bei einem Online-Shop haben, kaufen Sie lieber woanders ein. Es gibt eine Vielzahl seriöser Online-Shops, bei denen Sie sicher und bequem einkaufen können. Zahlen Sie im Zweifelsfall lieber etwas mehr und gehen Sie auf Nummer sicher.

Was tun, wenn etwas schiefgeht?

Wenn Sie den Verdacht haben, Opfer eines Cyberbetrugs geworden zu sein, hilft erstmal Ruhe zu bewahren und die richtigen Schritte einzuleiten.

Hier eine Checkliste, die Ihnen hilft, im Ernstfall richtig zu reagieren:

Kontaktieren Sie Ihre Bank:

- Melden Sie den Vorfall Ihrer Bank oder Ihrem Kreditkartenanbieter.
- Lassen Sie gegebenenfalls Ihre Karte sperren, um weiteren Missbrauch zu verhindern.
- Erkundigen Sie sich nach den Möglichkeiten einer Kreditkartenreklamation oder eines Lastschriftwiderspruchs.

Erstatten Sie Anzeige bei der Polizei:

- Stellen Sie Anzeige bei der Polizei, um den Vorfall offiziell zu melden.
- So erhalten Sie eine Fallnummer, die Sie für weitere Schritte, z.B. bei der Versicherung, benötigen.
- Beachten Sie jedoch, dass die Aufklärung von Online-Betrugsfällen oft schwierig ist.

Lohnt sich eine Cyber-Versicherung?

Eine pauschale Antwort auf diese Frage gibt es nicht. Ob sich eine Cyber-Versicherung für Sie lohnt, hängt von verschiedenen Faktoren ab, wie z. B. Ihrer Online-Aktivität, Ihren Sicherheitsvorkehrungen und Ihrem persönlichen Risikoprofil.

Cyber-Versicherungen bieten Schutz bei verschiedenen Online-Risiken, wie z. B.:

- Hackerangriffe
- Kreditkartenmissbrauch
- Identitätsdiebstahl
- Fake-Shop-Betrug
- Cybermobbing

Die Kosten für eine Cyber-Versicherung beginnen bereits ab 5 Euro monatlich. Allerdings sollten Sie beachten, dass die Leistungen der Versicherungen oft begrenzt sind, sowohl in Bezug auf die Höhe der Versicherungssumme als auch auf die Anzahl der versicherten Schäden.

Bevor Sie sich für eine Cyber-Versicherung entscheiden, sollten Sie überprüfen, welche Aspekte der Cybersicherheit bereits durch Ihre bestehenden Versicherungen abgedeckt sind. So können z. B. folgende Versicherungen Leistungen im Zusammenhang mit Cyber-Risiken enthalten:

- Haftpflichtversicherung (z. B. bei der Weiterleitung eines Trojaners)
- Hausratversicherung (z. B. mit einer „Online-Klausel“)
- Rechtsschutzversicherung (z. B. bei Streitigkeiten im Zusammenhang mit Online-Käufen)
- Bankkonto (z. B. Schadensausgleich bei Kreditkartenmissbrauch)

Mein Tipp: Prüfen Sie die Bedingungen Ihrer bestehenden Versicherungen. Eventuell ist eine Cyber-Versicherung dann nicht mehr von Nöten.