Betrugsprävention im E-Commerce

Schwarze Schafe müssen draußen bleiben

Bettina Vier
Digitalisierung + E-Commerce

©Bettina Vier, Digitalisierung + E-Commerce

Betrüger verursachen im E-Commerce Millionen- bis Milliardenschäden

Laut CRIF-Umfrage verursachen betrügerische Kunden in Online-Shops Millionen- bis Milliardenschäden. Betroffen ist fast jeder Online-Shop. 42% erleiden Verluste von weniger als 10.000 € im Jahr. 32 % müssen Verluste von 10.000 bis 100.000 € verbuchen und 25% sogar mehr als 100.000 €. Neben den Zahlungsausfällen und Warenverlusten muss der Händler zusätzliche Kosten für juristische Dienstleistungen oder Rücksendekosten tragen.

Quelle: IT-ZOOM, 95 Prozent der Online-Shops von Betrug betroffen, https://www.it-zoom.de/mobile-business/e/95-prozent-der-online-shops-von-betrug-betroffen-35074/, abgerufen: 5.12.2025

© generiert von ChatGPT, 6.12.2025

Die häufigsten Betrugsformen in Online-Shops

- In 76% der Fälle liegt Identitätsdiebstahl vor. Kriminelle gelangen an Informationen wie Namen, Adressen, Zugangsdaten oder Kreditkartendaten, und nutzen diese beispielsweise für Bestellungen, Kontoeröffnungen oder zur Verbreitung von Falschinformationen.

- 53% der Online-Händler sind durch Eingehungsbetrug betroffen In diesen Fällen wissen die Kunden bereits bei Vertragsabschluss, dass sie nicht in der Lage sind, ihren Vertragsteil leisten zu können, z.B. weil sie zahlungsunfähig sind.

Quelle: IT-ZOOM, 95 Prozent der Online-Shops von Betrug betroffen, https://www.it-zoom.de/mobile-business/e/95-prozent-der-online-shops-von-betrug-betroffen-35074/, abgerufen: 5.12.2025

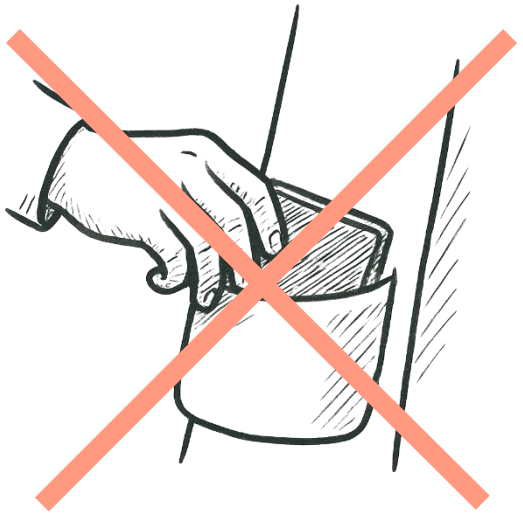
© generiert von ChatGPT, 6.12.2025

Betrugspräventionen

Im folgendem werden mögliche Präventionsmaßnahmen vorgestellt, die sowohl im B2C- als auch im B2B-Umfeld eingesetzt werden können.

Generell spielen Kundenumfeld, Branche und Verkaufsregionen eine wichtige Rolle, welchem Risiko der Shop ausgesetzt ist. Dem gegenüber stehen die Kosten der Maßnahmen und müssen daher entsprechend abgewägt werden.

Daher ist die nachfolgende Liste nur als Anregung aber nicht als Standardlösung zu werten.



© generiert von ChatGPT, 6.12.2025

Schutz vor Fake-Bestellungen, Zahlungsausfall und Identitätsdiebstahl

Aktivität	Beispiele für technische Lösungen
Bonitätsprüfung	Online Live-Abfragen an Online-Dienste (z.B. Schufa, Boniversum)
Adressvalidierung & Plausibilitätschecks	Online Dienste für Adressvalidierungen; diese Dienste können häufig auch für die Datenpflege in CRM-Systemen eingesetzt werden (z.B. adress-Validierung, byteplant, Loqate, Deutsche Post)
„Know Your Customer" (Kenne deinen Kunden) KYC	Services einbinden, die eine Kundenprüfung vornehmen (z.B. WebID Solutions, IDnow, AUTHADA, Sumsub, Veriff, Regis24); mit Paymentprovider abstimmen
Sanktionsprüfungen (Verhindert Verstöße gegen Außenwirtschaftsgesetze, Embargos und Finanzsanktionen)	Online-Prüfungen (z.B. ELEX, SOLID) oder im ERP integriert (ID.prove, Mercoline)
Muster von Betrugsversuche erkennen	Fraud-Prevention-Tools (KI, Machine-Learning; wird u.a. von Payment-Providern angeboten)

Schutz vor Missbrauch des Rechnungskaufs und Stornierung von Rücklastschriften

Aktivität	Beispiele für technische Lösungen
Kunden klassifizieren und nach Kundenkategorie Zahlungsarten zuteilen. Z.B. ▪ Neukunden nie Rechnungsstellung anbieten ▪ vertrauenswürdigen Bestandskunden immer Rechnungstellung und Ratenzahlung anbieten	Direkt im Shop-System die Kunden nach Kundengruppen (Kategorien) gruppieren und den Checkout entsprechend einstellen lassen.
	Kundengruppen im CRM anlegen und an das Shopsystem übergeben; Checkout entsprechend einstellen lassen.

Schutz vor Reselling-Betrug und Mehrfachbestellungen unter falschen Identitäten

In diesen Fall nutzen Betrüger Preisaktionen, um mehrere Artikel zu kaufen und diese teurer weiterzuverkaufen. Auch Online-Seminare werden gebucht und teurer weiterverkauft.

Aktivität	Beispiele für technische Lösungen
Identitätsnachweise einfordern	Dienste wie Post-Ident anbinden.
Bonitätsprüfungen	Online Live-Abfragen an Online-Dienste (z.B. Schufa, Boniversum)
Einkaufslimits	Je Kunde nur eine limitierte Menge (generell, pro Einkauf, pro Woche etc.); direkt im Shop-System (ggf. Plug-in) oder im CRM-System hinterlegen
Ausschluss auffälligen PLZ-Gebieten / Branchen	▪ KI-Analyse der eigenen CRM-Daten ▪ Online-Dienste nutzen, mit denen Zielgruppen nach regionalen und soziografischen Merkmalen geclustert werden können
Kunden gruppieren (Neukunden, vertrauenswürdige Bestandskunden, etc.)	direkt im Shop-System oder im CRM-System hinterlegen

Schutz vor „Nicht erhalten“ und Rücksendebetrug

Rücksendebetrug liegt vor, wenn Kunden leere Pakete zurückschicken, das Produkt austauschen oder benutzte Produkte (z.B. getragene Kleidung) zurückschicken.

Aktivität	Beispiele für technische Lösungen
Versandtracking	Dienste, die in der Regel vom Logistikunternehmen angeboten werden
Seriennummern bei Retouren Prüfen	Lesegeräte (Strichcode, QR-Codes)
Retourendokumentation	z.B. Retourenprüfung mit Kameraüberwachung
Beschädigungserkennung	Mit Hilfe von KI
Kunden mit hoher Retourenquote markieren	Direkt im Shop oder im CRM; Maßnahmen ableiten: z.B. Anzahl Kleidungsstücke je Bestellung limitieren, Produktgruppen für den Kunden ausschließen

Muster der Nutzer / Kunden erkennen

Wenn Nutzer plötzlich ihr Kaufverhalten ändern könnte das ein Indiz für Identitätenklau sein. Bestellt ein Kunde z.B. unerwartet viel, dann kann man die Auslieferung der Ware blockieren, bis der Kunden per Post-Ident seine Identität bestätigen lässt.

Aktivität	Beispiele für technische Lösungen
Ungewöhnliche IP-Adressen	▪ Nutzertracking im Shop (mit Trackingtools) ▪ Kundenanalysen mit KI (im CRM oder angebundenen Analysetools) ▪ Analysen der Reklamationen mit KI ggf. kombiniert mit Kunden / Bestelldaten (BI Analysetools)
Bestellhäufigkeit vs. Bestellgewohnheit der Kunden	
Retourenverhalten	
Reklamationen (Inhalte)	
Abweichende Rechnungs- und Lieferadressen	
Nutzung von VPN / Proxy (können als Tarnversuche gewertet werden)	

Besonderheit: Sanktionslisten

Verhindern Sie, dass Sie mit Kunden Geschäften betreiben, die auf Sanktionslisten stehen. Damit sind Kunden aus Ländern gemeint, mit denen aufgrund der Außenwirtschaftsgesetze, aufgrund von Embargos oder Finanzsanktionen keine Geschäfte betrieben werden dürfen.

Aktivität	Beispiele für technische Lösungen
Sanktionsprüfungen	Online-Prüfungen: ELEX, SOLID oder Integrationen ins ERP: ID.prove, Mercoline

Ergänzende operative Maßnahmen

Die bisher genannten Präventionsmaßnahmen sind technische Maßnahmen. Darüber hinaus gibt es auch nicht-technische Maßnahmen:

- Schulung der Mitarbeiter in der Retourenannahme und am Service-Telefon bzw. im Live-Chat
- Rechtssichere AGB, in der Widerruf und Rücksendung geregelt sind. Dazu gehört z.B. auch der Ausschluss von Waren von der Retoure wie Hygieneartikel oder digitale Downloadprodukte wie E-Books.
- Schulung in der Nutzung von Tracking- und Analysetools
- Meetings / Workshops, in denen sich Mitarbeiter aus verschiedenen Bereichen Beobachtungen und Wissen über Betrugsverhalten austauschen und Maßnahmen ableiten.

Disclaimer

Bitte beachten Sie, dass dieser Artikel keine Rechtsbelehrung beinhaltet und nach besten Wissen und Gewissen erstellt wurde. Bei Fragen wenden Sie sich bitte an einen Juristen mit entsprechenden Kenntnissen.

Ich unterstütze Unternehmen als freiberufliche Interim-Managerin in Leadpositionen von E-Commerce-Teams und bei der digitalen Transformation hin zum datengetriebenen Vertrieb.

Bettina Vier

Digitalisierung + E-Commerce

Diplom-Volkswirtin / IHK-Change-Managerin

E-Mail: ecommerce-management@gmx.de
Mobile: 0152-3397 4054

E-Commerce-Managerin mit tiefem digitalem Hintergrund. Begleitung von Unternehmen in Wachstums-, Krisen- und Veränderungsphasen. Erfahren in Produktdatenprozesse, E-Commerce & teamübergreifende Zusammenarbeit sowie Projektmanagement und Leitungsfunktion.

© Bettina Vier – Digitalisierung + E-Commerce

Lesetipps:

zum Blogbeitrag mit Download

zum Blogbeitrag mit Download

Blog „Digitaler Wandel“

© Bettina Vier – Digitalisierung + E-Commerce