Mittelstand-Digital
Zentrum
Handel

Betrug im E-Commerce - Was kann ich tun?

In diesem Infoblatt erfahren Sie, wie relevant das Thema Betrug im Onlinehandel ist und welche Schäden durch betrügerische Aktivitäten entstehen. Dabei zeigen wir, welche unterschiedlichen Betrugsformen es gibt und mit welchen Maßnahmen Sie Ihren Shop vor Betrug schützen können. Zudem beleuchten wir, wie sich eine fälschlich als betrügerisch eingeschätzte Bestellung auf die Kundenbeziehung auswirkt.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Handel

Mit wachsendem Onlinehandel nehmen auch die Risiken zu!

Der Onlinehandel wächst seit Jahren überdurchschnittlich. Auch wenn die Umsatzentwicklung 2023 nicht mehr an die Rekordzahlen aus den Coronajahren anknüpfen konnte, gehen Expert:innen davon aus, dass die Onlineumsätze auch zukünftig weiter wachsen werden. Mit der zunehmenden Bedeutung des Onlinehandels sehen sich Händler:innen und Konsument:innen auch einem zunehmenden Betrugsrisiko ausgesetzt. Einer Umfrage von CRIF aus dem Jahr 2023 unter Onlinehändlern im DACH-Raum zur Folge wurden 94 Prozent der deutschen Onlinehändler bereits Opfer von Bergungsversuchen.[1]

Auf Konsumentenseite ist es laut ECC KÖLN ein Viertel, das bereits Opfer von Betrug beim Onlineshoppen wurde[2] und auch im B2B-Umfeld sind Betrugsversuche keine Seltenheit. 64 Prozent der B2B-Unternehmen waren bereits mit Betrug konfrontiert, durchschnittlich zwei Prozent der Bestelllungen können als Betrug klassifiziert werden und durchschnittlich 14 Prozent des Umsatzes gehen B2B-Händlern durch Betrug im Onlineshop verloren.[3]

[1]CRIF: Betrug im E-Commerce, München, 2023
[2]ECC KÖLN: ECC Payment Update 2024, Köln, 2024
[3]ECC KÖLN: B2BEST-Barometer Vol.15, Köln, 2024

Was euch erwartet:

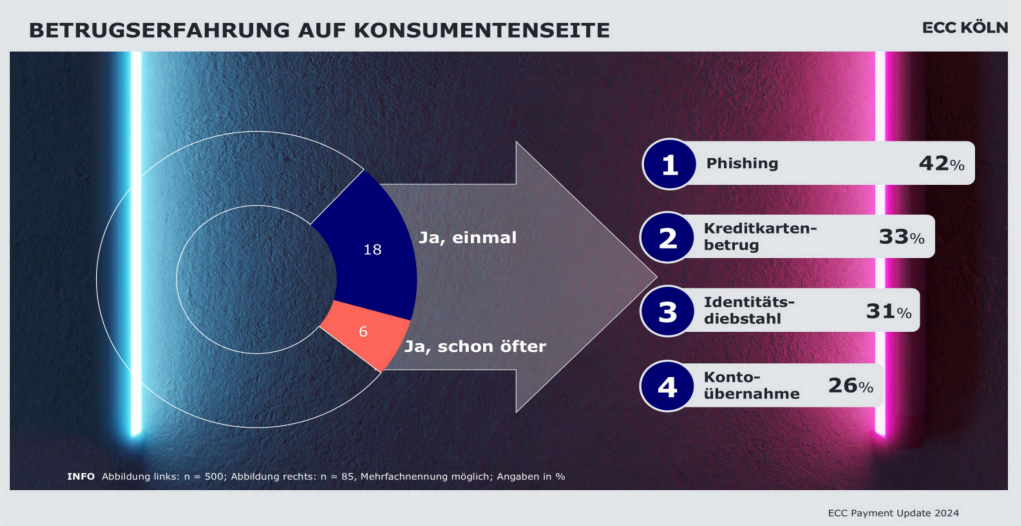
1. **Schäden durch Betrug für deutsche Onlinehänder:innen**
2. **Betrugsvermeidungsstrategien**
3. **Kosten der Betrugsprävention**
4. **False Positives: Eine nicht zu unterschätzende Herausfordeung**

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

1. Schäden durch Betrug für deutsche Händler:innen

Angriffe durch Cyberkriminelle zu identifizieren und sich vor diesen zu schützen, stellt viele Händler:innen vor große Herausforderungen. Die Betrugsmaschen von Kriminellen sind vielfältig und schnelllebig. Betrüger:innen erfinden immer neue Vorgehensweisen und Techniken und verursachen so erhebliche finanzielle Verluste, schaden dem Ruf von Unternehmen und untergraben das Vertrauen der Kundschaft.
Im E-Commerce sind zahlreiche Betrugsmaschen verbreitet, von denen einige besonders hervorzuheben sind:

- Identitätsdiebstahl und Kreditkartenbetrug: Betrügende verwenden gestohlene oder gefälschte Kreditkarteninformationen, um Waren zu kaufen, die sie weiterverkaufen können.
- Rückbuchungsbetrug (Chargeback Fraud): Kund:innen behaupten fälschlicherweise, eine Transaktion nicht autorisiert zu haben oder die Ware nicht erhalten zu haben, um eine Rückbuchung zu erwirken.
- Kontoübernahmen (Account Takeover): Betrügende erlangen unerlaubten Zugriff auf Kundenkonten, um Bestellungen aufzugeben oder die Kontodetails zu missbrauchen.
- Phishing und Social Engineering: Durch gefälschte E-Mails oder Nachrichten werden sensible Informationen erschlichen, um Betrug zu begehen.
- Friendly Fraud: Friendly Fraud liegt vor, wenn Kund:innen einen rechtmäßigen Kauf tätigt, dann aber die Abbuchung beim Kreditkartenunternehmen mit der Begründung reklamieren, dass der Kauf betrügerisch war. Dieses Vorgehen dient manchmal dazu, die Bezahlung des Artikels zu vermeiden, den Rückgabevorgang für den Artikel zu unterlaufen oder die Forderung nach einer Erstattung zu umgehen.



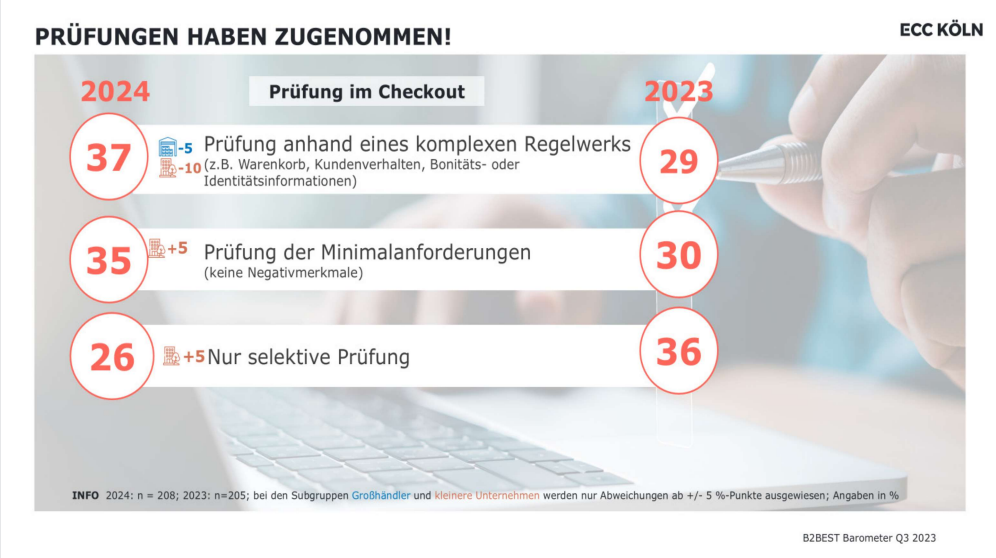
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

2. Betrugsvermeidungsstrategien

Um sich gegen Betrug zu schützen, können Händler:innen verschiedene Strategien und Technologien einsetzen:

- Verifizierung von Transaktionen: Einsatz von Tools zur Überprüfung der Authentizität von Transaktionen, z.B. durch 3D-Secure-Verfahren.
- Maschinelles Lernen und KI: Analysieren von Transaktionsdaten, um betrügerische Muster zu erkennen und in Echtzeit zu reagieren.
- Multi-Faktor-Authentifizierung: Zusätzliche Sicherheitsebenen für die Anmeldung und Transaktionsbestätigung bieten einen besseren Schutz.
- Adress- und Zahlungsvalidierung: Überprüfung der Adress- und Zahlungsinformationen auf ihre Richtigkeit und Konsistenz.

Generell hat die Betrugsprävention bei Unternehmen einen hohen Stellenwert und auch die Prüfungen anhand komplexer Regelwerke nehmen weiter zu. Dennoch werden viele Unternehmen erst nach dem ersten Betrugsfall wirklich aktiv.[4] Hier gilt es aufzurüsten und sich ggf. externe Unterstützung durch einen Dienstleister zu holen.



3. Kosten der Betrugsprävention

Die Implementierung von Betrugspräventionsmaßnahmen verursacht Kosten, die von der Größe des Unternehmens und dem Umfang der Maßnahmen abhängen. Investitionen in fortschrittliche Sicherheitstechnologien können erheblich sein, bieten jedoch im Vergleich zu den potenziellen Verlusten durch Betrug einen deutlichen Mehrwert. Es gilt eine Balance zwischen den Kosten für Sicherheitsmaßnahmen und dem Risiko von Betrugsfällen zu finden. Zur sog. Fraud Prevention können Händler:innen auf verschiedene Bonitäts- und Plausibilitätschecks zurückgreifen, wie beispielsweise ein automatisier-

[4]ECC KÖLN: B2BEST-Barometer Vol.15, Köln, 2024

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

ter Adressabgleich, Prüfung der IBAN und des angegebenen Namens oder eine SCHUFA-Auskunft in Echtzeit. Häufig empfiehlt sich hier die Zusammenarbeit mit spezialisierten Partnern. Händler:innen, die bereits mit einem Payment Service Provider zusammenarbeiten, können die Betrugsprävention in der Regel auch über diesen abwickeln – zumindest für die Zahlungsverfahren, die über den Payment Service Provider angebunden sind.

4. False Positives: Eine nicht zu unterschätzende Herausfordeung

Ein wichtiger Aspekt der Betrugsprävention ist das Management von False Positives, also legitimen Transaktionen, die fälschlicherweise als betrügerisch eingestuft werden. Dies kann zu entgangenen Verkäufen führen und das Kundenerlebnis negativ beeinflussen. Die Optimierung von Betrugspräventionsalgorithmen zur Minimierung von False Positives ist daher essenziell. Im B2B-Bereich geben 46 Prozent der Unternehmen an, Kund:innen schon einmal fälschlicherweise als Betrug eingestuft zu haben.[5]

Auf Konsumentenseite hat bereits jeder 7. Erfahrung mit einer zu Unrecht abgelehnten Zahlung.[6] Ob eine solche Erfahrung die Kundenbeziehung langfristig schädigt, hängt stark von der Reaktion der Händler:innen, beziehungsweise dessen/deren Zahlungsanbieters ab. Wird das Problem hier nicht schnell und zuvorkom mend gelöst, kann das Vertrauen der Kundschaft nachhaltigen Schaden nehmen.

Fazit

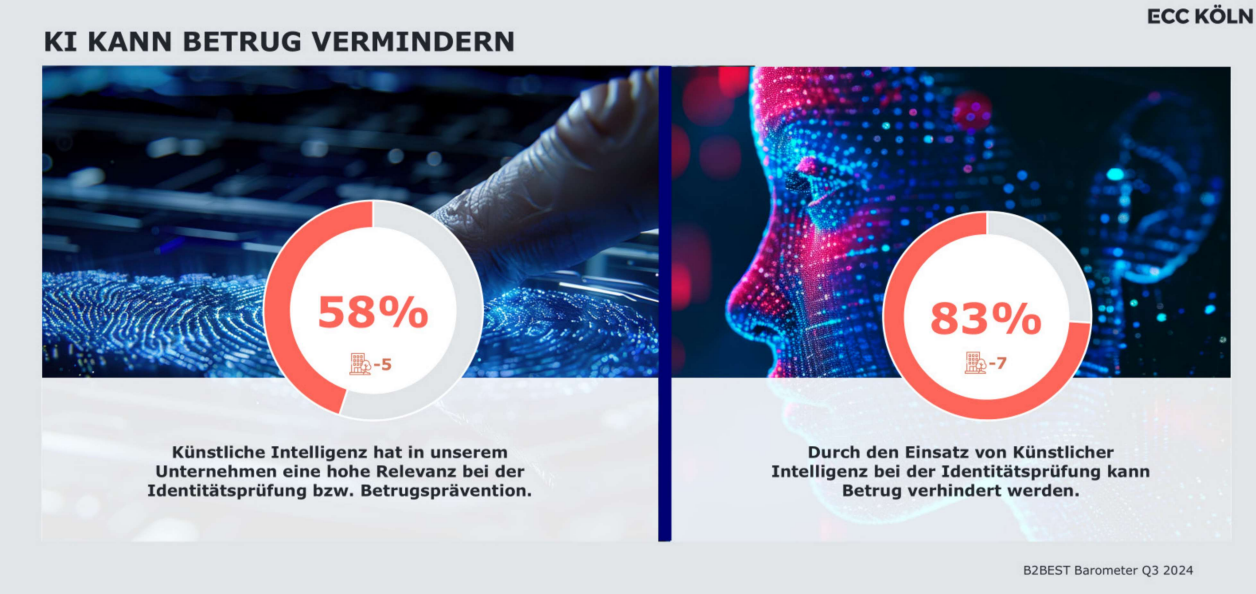
Betrugsprävention im E-Commerce ist für deutsche Händler:innen unerlässlich, um finanzielle Verluste zu vermeiden und das Vertrauen der Kund:innen zu wahren. Durch den Einsatz gezielter Strategien und Technologien können Betrugsrisiken minimiert werden. Neueste Technologien wie Künstliche Intelligenz (KI) und maschinelles Lernen werden zunehmend eingesetzt, um Betrugsmuster zu erkennen und potenzielle Bedrohungen in Echtzeit zu identifizieren. Zudem gewinnen Verfahren wie die Zwei-Faktor-Authentifizierung und biometrische Sicherheitsmaßnahmen an Bedeutung, um die Sicherheit bei Transaktionen zu erhöhen.

Neben den oben genannten Maßnahmen zur Betrugsprävention und der engen Zusam-

[5]ECC KÖLN: B2BEST-Barometer Vol.15, Köln, 2024
[6]ECC KÖLN: ECC Payment Update 2024, Köln, 2024

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

menarbeit mit Experten empfiehlt es sich, darüberhinaus auch die eigenen Mitarbeitenden fortaufend zum Thema Betrug zu sensibilisieren und über aktuelle Trends im Betrugsschutz zu schulen. Auch der Schutz von Kundendaten ist essentiell.
Durch die Implementierung dieser Maßnahmen können Händler:innen nicht nur ihre eigenen Geschäfte schützen, sondern auch das Vertrauen ihrer Kundschaft stärken. Gleichzeitig ist es wichtig, das Gleichgewicht zwischen Sicherheitsmaßnahmen und Kundenerlebnis zu wahren, um nicht durch Unannehmlichkeiten im Check-out oder False Positiv potenzielle Kund:innen zu verlieren.



Das Mittelstand-Digital Zentrum Handel gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Infoblatt: Betrug im E-Commerce - Was kann ich tun? – Oktober 2024
Mittelstand-Digital Zentrum Handel
IFH Köln GmbH
Dürener Str. 401 b, 50858 Köln

digitalzentrumhandel.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital