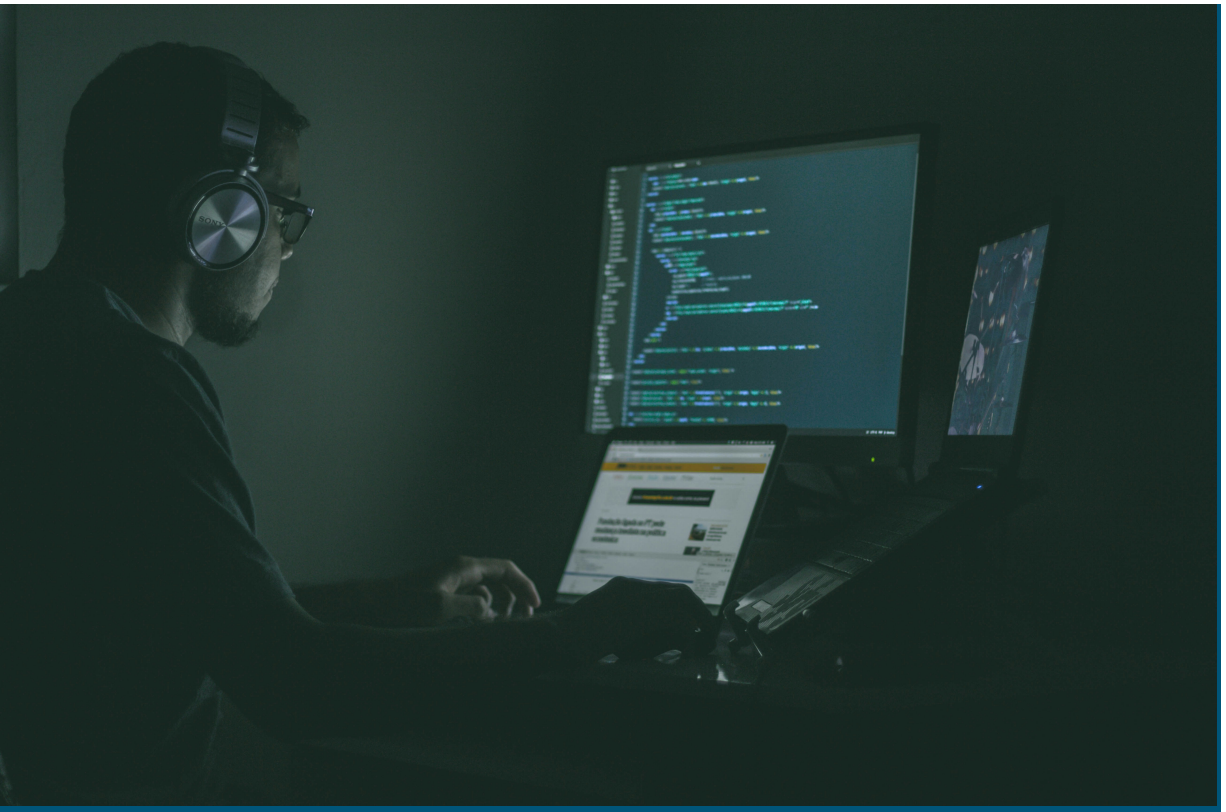
Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie



# Betrugsprävention im E-Commerce

## Strategien und Maßnahmen für sichere Online-Geschäfte

stmwi.bayern.de

# Sicherheit als Wettbewerbsfaktor

Der digitale Handel ist heute ein zentraler Bestandteil der Wirtschaft. Kunden erwarten bequeme, schnelle und vor allem aber auch sichere Online-Einkäufe. Für Händler eröffnen sich dadurch neue Absatzchancen und Märkte, gleichzeitig wächst jedoch das Risiko, Opfer von Betrug zu werden.

Zahlreiche Erhebungen zeigen, dass viele Onlinehändler bereits mit Betrugsversuchen konfrontiert waren. Auch kleine und mittlere Unternehmen sind betroffen, da sie häufig weder spezialisierte IT-Abteilungen noch standardisierte Sicherheitsprozesse besitzen. Hinzu kommt, dass Sicherheitsaufgaben im Tagesgeschäft häufig nachrangig behandelt werden, solange kein akuter Schaden eintritt. Allein im Jahr 2023 entstanden durch Online-Betrug in Europa und Nordamerika Verluste von mehr als 50 Milliarden US-Dollar. Besonders kostenintensiv sind Fälle, bei denen Transaktionen ohne physische Kartenpräsenz durchgeführt werden (sogenannter „Card-Not-Present Fraud“), ebenso wie Rückbuchungen und Identitätsmissbrauch. In der Praxis liegt der tatsächliche Schaden häufig drei- bis viermal über dem unmittelbaren finanziellen Verlust, da zusätzlich Kosten für Reklamationen, Rückabwicklungen und Reputationsschäden entstehen.[1] Betrugsprävention ist daher keine technische Randaufgabe, sondern eine betriebswirtschaftliche Notwendigkeit. Sie schützt den Umsatz und das Vertrauen in ein Unternehmen.

Dieses Infoblatt gibt einen Überblick zu den aktuellen Entwicklungen und Betrugsformen im E-Commerce, erläutert ihre Auswirkungen auf den Handel und zeigt praxisnahe Maßnahmen auf, wie Händler verschiedene Schutzmechanismen wirksam miteinander verbinden können.

# Was E-Commerce-Sicherheit bedeutet

Unter E-Commerce-Sicherheit versteht man das Zusammenspiel aus technischen, organisatorischen und rechtlichen Maßnahmen, die darauf abzielen, digitale Transaktionen zuverlässig abzusichern. Im Kern stützt sich die E-Commerce-Sicherheit auf vier Prinzipien:

- Authentizität stellt sicher, dass beide Seiten einer Transaktion, d. h. Händler und Kunde, tatsächlich die sind, die sie vorgeben zu sein.
- Vertraulichkeit bedeutet, dass sensible Daten wie Adress- oder Zahlungsinformationen nur berechtigten Personen zugänglich sind.
- Integrität sorgt dafür, dass übermittelte Daten unverändert bleiben und nicht manipuliert werden können.
- Nachvollziehbarkeit gewährleistet, dass jede Transaktion dokumentiert und im Streitfall rechtssicher nachgewiesen werden kann.

E-Commerce-Sicherheit ist somit ein fortlaufender Prozess. Sie entwickelt sich mit neuen Technologien, rechtlichen Vorgaben und Betrugsmethoden weiter. Was heute als sicher gilt, kann morgen schon eine

[1] https://www.haendlerbund.de/de/ratgeber/recht/schutz-vor-betrug-im-e-commerce

Schwachstelle darstellen. Umso wichtiger ist ein Verständnis von Sicherheit als dynamischem Bestandteil des Geschäftsbetriebs und nicht als technische Zusatzfunktion.

# Neue Dimensionen des Onlinebetrugs

Die Methoden im Onlinebetrug reichen von technischen Manipulationen über Identitätsmissbrauch bis hin zu psychologisch aufgeladenen Täuschungsversuchen. Viele Angriffe kombinieren mehrere Elemente, um Kontrollen zu umgehen und Unklarheit zu stiften. Im Folgenden sind die bekanntesten Arten aufgelistet:

Phishing bleibt eine der häufigsten Angriffsformen: Betrüger versenden hier täuschend echte E-Mails, die scheinbar von Zahlungsdienstleistern, Plattformen oder Behörden stammen. Ziel ist es, Zugangsdaten, Kontoinformationen oder Login-Credentials (z. B. Benutzernamen, PINs oder Passwörter) zu erlangen. Moderne Phishing-Kampagnen sind auf den ersten Blick oft kaum noch von legitimer Kommunikation zu unterscheiden und nutzen häufig KI-generierte Texte, Logos oder Absenderadressen.

E-Skimming beschreibt hingegen den digitalen Diebstahl von Zahlungsinformationen direkt im Bestellprozess. Schadcode wird in den Checkout eines Shops eingeschleust und zeichnet Kartendaten im Moment der Eingabe auf. Besonders gefährlich ist, dass diese Angriffe über Monate unentdeckt bleiben können. Oftmals fällt der Betrug erst auf, wenn Kunden unberechtigte Abbuchungen melden.

Besonders häufig tritt der sogenannte Dreiecksbetrug, auch „Triangulation Fraud“ genannt, auf. Dabei bestellt ein Täter mit gestohlenen Zahlungsdaten bei einem seriösen Händler (häufig kleine, leicht versendbare Artikel wie Elektronikzubehör oder Spielwaren) und nutzt dafür die Daten eines ahnungslosen Dritten. Die Ware wird an eine vom Betrüger kontrollierte Adresse geliefert, während die Zahlung ausbleibt. So entsteht ein undurchsichtiges Dreiecksverhältnis zwischen Opfer, Händler und Täter. Der Aufwand für Aufklärung und Rückabwicklung ist meist hoch, die Erfolgsaussichten gering.

> Auch im B2B-Segment mehren sich Fälle von Identitätsdiebstahl. Angreifer geben sich hier als Mitarbeiter eines bekannten Kunden aus, bestellen hochpreisige Waren auf Rechnung und manipulieren Lieferadressen oder Ansprechpartner. Diese Form des Betrugs ist besonders tückisch und nicht selten auch erfolgreich, da sie auf vertrauliche Geschäftsbeziehungen und den gewohnten Ablauf im Firmenkundengeschäft abzielt.

Eine weitere geläufige Masche ist der Missbrauch des Namens öffentlicher Einrichtungen oder gemeinnütziger Organisationen. Bestellungen im Namen von Schulen, Behörden oder Vereinen wirken zwar zunächst glaubwürdig, sind aber nicht immer authentisch. Besonders heikel sind SEPA-Lastschriften, wenn kein valider Namensabgleich bei der Zahlungsabwicklung erfolgt. Händler sollten in solchen Fällen prüfen, ob die genannte Institution tatsächlich der Auftraggeber ist. Bei Unklarheiten empfiehlt es sich, die Lieferung nur gegen Vorkasse auszuführen.

Zunehmend nutzen Betrüger emotionale Geschichten, um Vertrauen aufzubauen, z. B. angebliche Hilfsaktionen für Kinder oder soziale Einrichtungen. Solche Nachrichten sind zwar häufig mit generischen Texten oder grammatikalischen Ungenauigkeiten versehen, gerade in hektischen Phasen werden sie

jedoch oft unkritisch durchgewunken, besonders wenn interne Freigaben auf Vertrauen statt auf Regeln basieren oder Zeitdruck durch die Betrüger aufgebaut wird.

Eine neuere Entwicklung sind synthetische Identitäten und sogenannter „Deepfake Fraud“. Dabei werden reale und gefälschte Daten kombiniert, um scheinbar plausible Kundenprofile zu erzeugen. Mithilfe von Künstlicher Intelligenz (KI) können Betrüger Gesichter, Stimmen oder mittlerweile sogar Videokonferenzen imitieren, um Authentizität vorzutäuschen. Solche Angriffe sind bislang noch eher selten durch klassische Prüfverfahren zu erkennen und werden künftig eine wachsende Herausforderung darstellen.

Betrug im Onlinehandel ist längst die Regel, nicht die Ausnahme: Laut einer Umfrage des Wirtschaftsinformationsdienstleisters Crif aus dem Jahr 2024 berichten 94 Prozent der deutschen E-Commerce-Unternehmen von Betrugsversuchen.[2] Als häufigste betrügerische Praxis wurde dabei der Identitätsdiebstahl genannt, bei dem sich ein Kunde als eine komplett andere reale Person ausgegeben hatte (92 Prozent). Zudem berichteten 81 Prozent der befragten Händler, bereits mit Betrugsversuchen konfrontiert gewesen zu sein, bei denen gefälschte Namen oder Adressangaben verwendet wurden.[3]

# Technische Präventionsmaßnahmen

Ein sicheres E-Commerce-Geschäft stützt sich auf eine stabile und zeitgemäße technische Basis. Zu den zentralen Maßnahmen zur Betrugsprävention gehört in diesem Zusammenhang zunächst die konsequente Verschlüsselung sämtlicher Datenübertragungen zwischen Browser und Server durch kryptografische Protokolle und Zertifikate. Hierzu zählen z. B. „Transport Layer Security“ (kurz: TLS), „Secure Sockets Layer“ (kurz: SSL) und „Hypertext Transfer Protocol Secure“ (kurz: HTTPS).

Diese Protokolle stellen sicher, dass Informationen, z. B. persönliche Daten, Passwörter oder Zahlungsdetails, nicht von Dritten mitgelesen oder verändert werden können, während sie über das Internet übertragen werden. Eine ordnungsgemäß eingerichtete Verschlüsselung ist daher ein zentrales Element technischer Integrität: Sie schützt nicht nur die Kommunikation zwischen Händler und Kunden, sondern verhindert auch Manipulationen durch sogenannte „Man-in-the-Middle“-Angriffe, bei denen Datenpakete unterwegs abgefangen und verändert werden. Darüber hinaus wirkt sich eine sichtbare Verschlüsselung, etwa durch das Schloss-Symbol in der Browserzeile oder die HTTPS-Adresse, unmittelbar auf die Vertrauenswahrnehmung der Kundschaft aus. Nutzer orientieren sich an solchen Sicherheitsindikatoren, um einzuschätzen, ob ein Onlineshop seriös ist. Damit trägt Verschlüsselung nicht nur zur Datensicherheit bei, sondern stärkt zugleich die Glaubwürdigkeit und Professionalität des Unternehmens im digitalen Raum.

Des Weiteren sollte mehrstufige Authentifizierung (kurz: MFA; auch „2FA“ für Zwei-Faktor-Authentifizierung genannt) zum Standard werden – nicht nur für Kunden, sondern insbesondere für administrative

[2] https://www.crif.at/aktuelles-events/news-presse/umfrage-betrug-im-e-commerce/
[3] https://www.e-commerce-magazin.de/betrug-im-e-commerce-fast-jeder-onlineshop-in-dach-ist-betroffen-a-dbe30178637acda70fcda5fca60770d2/

Zugänge, Logins bei Zahlungsdienstleistern und interne Systeme im Unternehmen. Bei diesem Verfahren genügt ein Passwort allein nicht mehr, um Zugriff zu erhalten. Erst die Kombination mehrerer, voneinander unabhängiger Faktoren bestätigt eindeutig, dass eine Anmeldung legitim ist.

Als zusätzliche Sicherheitsfaktoren kommen beispielsweise einmalige Codes zum Einsatz, die per SMS oder E-Mail übermittelt werden, Bestätigungen über spezielle Authentifizierungs-Apps (wie Google Authenticator oder Authy) oder physische Sicherheitsgeräte wie RSA-Token. Moderne Verfahren nutzen auch biometrische Merkmale wie Fingerabdrücke oder Gesichtserkennung. Selbst wenn ein Passwort kompromittiert oder über Phishing erlangt wurde, bleibt der Zugriff auf das Konto dadurch wirksam geschützt. MFA zählt heute zu den wirksamsten und zugleich kostengünstigsten Maßnahmen gegen unbefugte Zugriffe. Sie senkt nachweislich das Risiko erfolgreicher Angriffe erheblich und gilt daher als Mindeststandard für digitale Geschäftsprozesse im Handel.

Ein weiterer zentraler Baustein ist der „Payment Card Industry Data Security Standard“ (kurz: PCI DSS). Er definiert verbindliche Sicherheitsanforderungen für den Umgang mit Kreditkartendaten von der Speicherung über die Verarbeitung bis zur Übertragung. Ziel ist es, den Missbrauch sensibler Zahlungsinformationen zu verhindern und ein einheitliches Schutzniveau im weltweiten Zahlungsverkehr zu gewährleisten.

Händler, die Kartenzahlungen akzeptieren, sollten sicherstellen, dass ihre Systeme und Prozesse diesen Standards vollständig entsprechen. Dazu gehört beispielsweise, dass Kartendaten niemals unverschlüsselt gespeichert werden dürfen, der Zugriff darauf klar geregelt ist und Netzwerke regelmäßig auf Schwachstellen überprüft werden. Die Einhaltung des PCI DSS wird von den Kartenorganisationen (z. B. Visa, Mastercard) überwacht und ist häufig vertraglich vorgeschrieben. Unternehmen, die gegen die Vorgaben verstoßen, riskieren nicht nur Bußgelder und erhöhte Haftungsrisiken, sondern auch den Verlust ihrer Berechtigung, Kartenzahlungen abzuwickeln.

Auch sogenannte „Device Intelligence“ bietet einen wichtigen Mehrwert. Dabei werden technische Merkmale eines genutzten Endgeräts wie Betriebssystem, Browsertyp, Bildschirmauflösung oder installierte Schriftarten zu einem eindeutigen Geräteprofil zusammengeführt. Dieses Profil ermöglicht es, verdächtige Aktivitäten zu erkennen, z. B. wenn mehrere Kundenkonten oder Bestellungen mit denselben Geräteinformationen verknüpft sind.

Solche Muster können automatisiert analysiert und mit bekannten Risikoprofilen abgeglichen werden. Auf diese Weise lassen sich Anomalien frühzeitig identifizieren, etwa bei auffälligen Bestellhäufungen, ungewöhnlichen Login-Orten oder wiederkehrenden Rückbuchungen von demselben Gerät. Die Geräteprofilanalyse unterstützt damit die Betrugserkennung im Hintergrund, ohne den Kaufprozess für die Kundschaft zu unterbrechen.

Zunehmend gewinnen auch KI-gestützte Betrugserkennungssysteme an Bedeutung. Diese analysieren in Echtzeit hunderte Datenpunkte von der IP-Adresse über den Gerätetyp bis hin zu Bestellverhalten und Zahlungsrhythmus und berechnen daraus die Wahrscheinlichkeit eines Betrugs. Solche Systeme sind besonders effizient, wenn sie den Kunden gegenüber transparent eingesetzt und regelmäßig durch Menschen überprüft werden, um Fehlentscheidungen zu vermeiden.

Der entscheidende Vorteil solcher Systeme liegt in ihrer Lernfähigkeit: Durch den kontinuierlichen Abgleich mit neuen Daten und Feedback aus echten Fällen werden die Modelle mit der Zeit präziser und können auch subtile Betrugsmuster erkennen, die für herkömmliche Regelwerke unsichtbar bleiben.

Für viele Händler, insbesondere im Mittelstand, ist es wirtschaftlich sinnvoll, Sicherheitsleistungen auszulagern. Anbieter von Payment- oder Shop-Lösungen bieten häufig bereits integrierte Schutzmodule an, die auch ohne große IT-Abteilung genutzt werden können. Bei der Einbindung externer Betrugsanalyse-Dienstleister ist jedoch dringend auf strikte Einhaltung der Datenschutz-Grundverordnung (DSGVO) zu achten. Daten dürfen nur in dem Umfang verarbeitet werden, der für die Betrugserkennung notwendig ist. Transparente Vereinbarungen und regelmäßige Abstimmungen helfen, Datenschutz und Sicherheit miteinander in Einklang zu bringen.

# Organisatorische Sicherheitsstrategien

Technische Systeme können auf dem Gebiet der Betrugsprävention viel leisten, doch sie ersetzen nicht das menschliche Urteilsvermögen. Betrüger nutzen gezielt menschliche Routinen, Zeitdruck oder Vertrauensverhältnisse aus. Daher ist betriebliche Aufmerksamkeit eine der wichtigsten Schutzbarrieren.

Eine wirksame Betrugsprävention beginnt also bei klar definierten Prozessen: Welche Mitarbeiter dürfen Zahlungen freigeben? Wer prüft auffällige Bestellungen oder ungewöhnlich hohe Warenkörbe? Wann wird ein Verdachtsfall dokumentiert und gemeldet? Solche Fragen müssen im Betrieb eindeutig geregelt sein.

Auffällig sind oft nur kleine Unstimmigkeiten: ein zusätzlicher Buchstabe in der Domain oder ein falsch gesetztes Sonderzeichen. Ein Abgleich zwischen E-Mail-Adresse, Unternehmensname und Rechnungsanschrift kann helfen, solche Fälschungen frühzeitig zu erkennen. Gerade im Firmenkundengeschäft, wo Bestellungen auf Rechnung üblich sind, ist diese Kontrolle entscheidend.

Regelmäßige Schulungen helfen zudem, Mitarbeiter zu sensibilisieren und aktuelle Betrugsmethoden frühzeitig zu erkennen. In verschiedenen Unternehmensbereichen werden dabei vermutlich unterschiedliche Warnsignale auffallen: Während im Kundenservice Unstimmigkeiten bei Tonalität, Formulierungen und Domainabweichungen ins Auge fallen werden, kann die Buchhaltung Kontobewegungen, Rücklastschriften und Anomalien im Zahlungsfluss prüfen. Im Lager deuten der Versand an wiederkehrende Packstationen, ungewöhnliche Zeitfenster oder die Häufung bestimmter Produkttypen auf Missbrauch hin. Ein wirksames Instrument ist dabei das Vier-Augen-Prinzip: Kritische Freigaben, etwa bei Rückzahlungen oder Erstbestellungen von Neukunden mit hohem Warenwert, sollten immer hinterfragt und von zwei Personen geprüft werden.

Auch ein geübter Umgang mit Rücksendungen ist wichtig. Manipulierte Retouren, wie durch vertauschte Ware oder den Rückversand von Fälschungen, verursachen hohe Schäden. Standardisierte Prüfprozesse, Bilddokumentation und der Abgleich von Seriennummern können helfen, solche Verluste zu vermeiden.

# Rechtliche Anforderungen

Auch die rechtlichen Anforderungen an Cybersicherheit nehmen weiter zu. Mit der NIS2-Richtlinie verpflichtet die Europäische Union künftig deutlich mehr Unternehmen als bisher, verbindliche Sicherheitsstandards einzuhalten und ihre IT-Sicherheitsstrukturen nachweislich zu stärken. Betroffene Unternehmen müssen künftig ein systematisches Risikomanagement aufbauen, Schutzmaßnahmen dokumentieren und erhebliche Sicherheitsvorfälle innerhalb festgelegter Fristen an die zuständigen Behörden melden.

Die Richtlinie betrifft nicht nur große Konzerne, sondern kann auch kleinere Handelsunternehmen einbeziehen, etwa dann, wenn sie bestimmte Umsatz- oder Beschäftigtengrenzen überschreiten oder als Zulieferer in sicherheitsrelevante Wertschöpfungsketten eingebunden sind. Ziel ist es, die Widerstandsfähigkeit der europäischen Wirtschaft insgesamt zu erhöhen und die Ausbreitung von Cyberangriffen über Lieferketten zu verhindern.

Auf fitnis2.de können Unternehmen prüfen, ob sie von der NIS2-Richtlinie betroffen sind und welche Schritte sie zur Umsetzung einplanen sollten.

Hinzu kommen neue europäische Regelungen im Zahlungsverkehr: Die Dritte Zahlungsdiensterichtlinie (kurz: PSD3) und die dazugehörige „Payment Services Regulation“ (kurz: PSR) sollen den Zahlungsverkehr in der EU sicherer, transparenter und einheitlicher gestalten. Während PSD3 die bestehenden Vorgaben an nationale Gesetzgebungen anpasst, führt die PSR als unmittelbar geltende Verordnung verbindliche Standards für alle Mitgliedstaaten ein.

Beide Regelwerke zielen darauf ab, den Schutz von Verbrauchern zu stärken, den Wettbewerb im Zahlungsverkehr zu fördern und Betrugsrisiken zu verringern. Für Händler bedeutet das, dass sie künftig noch stärker gegenüber Zahlungsdienstleistern und zuständigen Aufsichtsstellen nachweisen müssen, wie sie Zahlungsdaten verarbeiten, Sicherheitsvorgaben einhalten und Mechanismen zur aktiven Betrugsprävention betreiben. Auch die Zusammenarbeit mit Zahlungsdienstleistern wird verbindlicher geregelt, um eine einheitliche Sicherheitsarchitektur im europäischen Onlinehandel zu gewährleisten.

# Unterstützung und Ressourcen

Zahlreiche Organisationen bieten praxisnahe Hilfestellungen bei Fragen rund um das Thema Betrugsprävention im E-Commerce. Die folgenden Anlaufstellen helfen Unternehmen, Risiken im Onlinehandel besser zu erkennen, Betrug vorzubeugen und den eigenen Schutz zu stärken:

Bayerischen Unternehmen steht die Zentrale Ansprechstelle Cybercrime (ZAC) als wichtige Ressource zur Verfügung. Neben Präventionsarbeit leistet die Bayerische Polizei damit Betroffenen von Onlinekriminalität schnell Unterstützung bei der Klassifizierung von Schadensfällen, Strafverfolgung und Schadensbewältigung.

Außerdem informiert die Initiative Sicher handeln der Polizeilichen Kriminalprävention von Bund und Ländern über Betrugsrisiken im Onlinehandel und zeigt, wie man sich als Unternehmen effektiv vor ihnen schützen kann. Im Mittelpunkt steht die SHS-Regel: Stoppen – Hinterfragen – Schützen. Sie ruft

dazu auf, in verdächtigen Situationen innezuhalten, Angebote kritisch zu prüfen und aktiv vorzugehen, etwa durch Meldung verdächtiger Vorfälle oder sicheres Verhalten im Netz. Die Kampagne richtet sich in erster Linie an Verbraucher, ihre Empfehlungen sind jedoch auch für Onlinehändler von großer Bedeutung, um betrügerische Aktivitäten frühzeitig zu erkennen und ihre Kundschaft sowie das eigene Unternehmen besser zu schützen.

Zudem ist der CyberRisikoCheck des Bundesamts für Sicherheit in der Informationstechnik (BSI) ein standardisiertes Verfahren zur Einschätzung der IT-Sicherheitslage in kleinen und mittleren Unternehmen. Er basiert auf der DIN SPEC 27076 und wird von qualifizierten IT-Dienstleistern durchgeführt. In einem strukturierten Interview werden 27 Anforderungen aus sechs Themenbereichen abgefragt, z. B. zu Organisation, Notfallvorsorge, Systemschutz und Mitarbeitersensibilisierung. Die Ergebnisse werden ausgewertet und in einem Bericht zusammengefasst, der den aktuellen Sicherheitsstatus des Unternehmens darstellt, Schwachstellen aufzeigt und konkrete, priorisierte Handlungsempfehlungen liefert. Der CyberRisikoCheck ist keine Zertifizierung, sondern ein praxisnahes Instrument zur Standortbestimmung und Verbesserung der Cyberresilienz. Zudem bietet er Hinweise auf Fördermöglichkeiten und trägt durch anonymisierte Auswertungen zur allgemeinen Sicherheitslage von KMU in Deutschland bei.

Der zeitliche und finanzielle Aufwand für den CyberRisikoCheck ist nicht zentral festgelegt und variiert je nach Dienstleister und Unternehmensgröße. Das Interview selbst dauert in der Regel nur wenige Stunden, der gesamte Prozess erstreckt sich meist über wenige Tage. Konkrete Kostenangebote erhalten Unternehmen direkt bei den qualifizierten Anbietern, teilweise stehen zudem Förderprogramme zur Verfügung.

Das Service-Center des BSI ist bei Verdacht auf Betrug oder sicherheitsrelevanten Vorfällen telefonisch unter der Nummer 0800 274-1000 oder per E-Mail an service-center@bsi.bund.de erreichbar.

Eine weitere hilfreiche Anlaufstelle ist die Transferstelle Cybersicherheit im Mittelstand, die durch das Bundesministerium für Wirtschaft und Energie gefördert wird. Diese richtet sich an KMU, Start-ups und Handwerksbetriebe, die ihre IT- und Cyber-Sicherheit verbessern wollen. Für Händler besonders relevant sind folgende ihrer kostenfreien Angebote**:**

- CYBERsicher Check: Hier können Unternehmen prüfen, wo im Betrieb konkrete Schwachstellen bestehen (z. B. in Systemen, Prozessen oder Zugängen).
- CYBERDialoge: In Erstgesprächen, in denen einfache Fragen zu Cyber-Sicherheit gestellt und praktischer Rat eingeholt werden kann, erhalten Unternehmen eine Einschätzung ihres Sicherheitsniveaus und konkrete Empfehlungen für geeignete nächste Schritte.
- CYBERsicher Notfallhilfe: Wenn eine Datenpannen oder ein Angriff tatsächlich auftritt, erhalten betroffene Unternehmen schnelle Unterstützung und Maßnahmenempfehlungen, um Schäden zu begrenzen, Abläufe wiederherzustellen und weitere Risiken zu vermeiden.
- Materialien und Leitfäden: Hier finden Interessierte Checklisten, Schritt-für-Schritt-Anleitungen und allgemeine Handlungsempfehlungen, die Händler direkt im Alltag umsetzen können.
- Workshops und Veranstaltungen: Angeboten werden auch spezielle Schulungen, Webimpulse und Fachveranstaltungen mit Inhalten, die auf Geschäftsabläufe in Handel und Mittelstand zugeschnitten sein können.

Darüber hinaus informieren sowohl der Handelsverband Bayern (HBE) als auch die örtlich ansässigen IHKn regelmäßig über aktuelle Betrugsmaschen neue Sicherheitsanforderungen und Präventionsmaßnahmen im Onlinehandel.

# Richtiges Handeln im Ernstfall

Kein System bietet vollständigen Schutz vor Betrug. Entscheidend ist daher, wie ein Unternehmen reagiert, wenn es zu einem Betrugsfall kommt. In einer solchen Situation kommt es vor allem auf folgende Schritte an:

- Zunächst sollten alle relevanten Informationen dokumentiert werden: Bestelldaten, Kommunikationsverläufe, Zahlungsinformationen und technische Logfiles. Diese Beweise sind wichtig für Ermittlungsbehörden und Zahlungsdienstleister.
- Kunden, deren Daten betroffen sind, sollten transparent informiert werden – nicht erst auf Nachfrage. Ein offener Umgang signalisiert Verantwortungsbewusstsein, selbst wenn ein Fehler passiert ist.
- Parallel müssen betroffene Systeme überprüft, Passwörter geändert und Sicherheitsmaßnahmen angepasst werden. Wenn finanzielle Schäden entstanden sind, sollte umgehend Kontakt mit Polizei und Versicherungen aufgenommen werden.
- Eine klare interne Kommunikationsstrategie hilft im Schadensfall, Unsicherheit zu vermeiden: Wer informiert wen, in welcher Reihenfolge? Wie wird nach außen kommuniziert? In Krisen ist Klarheit entscheidend, denn Schweigen oder widersprüchliche Aussagen können mehr schaden als der Vorfall selbst.

Trotz sorgfältiger Dokumentation und Anzeige verlaufen viele Ermittlungsverfahren bei Betrugsfällen leider ergebnislos. Die Ermittlungsbehörden stoßen häufig an technische und juristische Grenzen bei der Identifikation und Verfolgung der Täter, insbesondere bei grenzüberschreitenden Delikten. Umso wichtiger ist eine präventive Haltung: Wer Verdachtsfälle früh erkennt und intern handlungsfähig bleibt, minimiert Schäden, auch wenn eine strafrechtliche Aufklärung nicht immer gelingt.

# Fazit

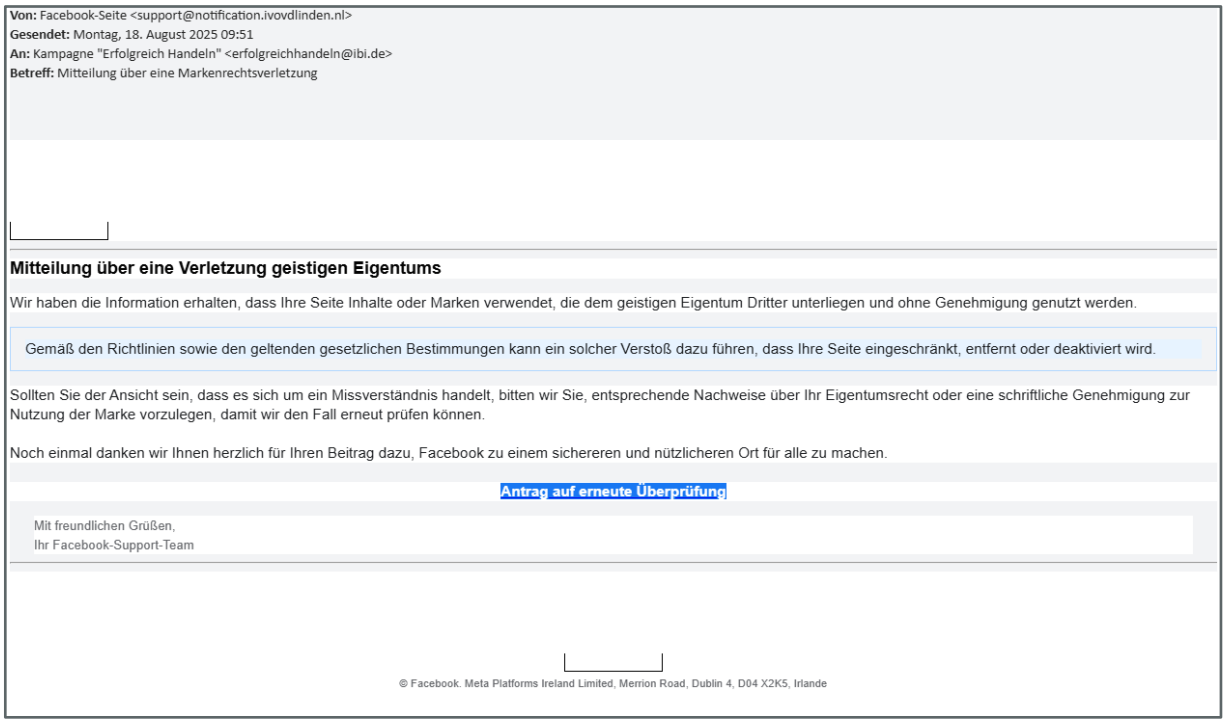
Betrug im E-Commerce ist heute ein strukturelles Risiko des digitalen Handels. Die Angriffsmethoden sind vielfältig, technisch ausgefeilt und oft international organisiert. Händler müssen deshalb technische, organisatorische und rechtliche Schutzmechanismen konsequent miteinander verbinden.

Wirksam sind vor allem Maßnahmen, die aufeinander abgestimmt sind: Sichere IT-Systeme mit aktuellen Standards, klare interne Prozesse, geschulte Mitarbeiter und eine regelmäßige Überprüfung verdächtiger Bestellungen. Ergänzend braucht es ein funktionierendes Netzwerk aus Zahlungsdienstleistern, Plattformen und Behörden, um neue Betrugsmuster frühzeitig zu erkennen.

Prävention ist dabei weniger eine Frage teurer Technologie als der Konsequenz im Alltag. Wer seine Abläufe dokumentiert, Risiken regelmäßig bewertet und verdächtige Vorgänge ernst nimmt, reduziert Verluste und bleibt handlungsfähig.

# Testen Sie sich selbst!

Sie sind Empfänger der nachfolgenden E-Mail geworden. Sie haben einen Facebook-Account und interagieren dort regelmäßig mit Anzeigen und Beiträgen Ihres Geschäfts, immer mit gutem Gewissen. Nun erhalten Sie folgende E-Mail, in der Ihnen eine Markenrechtsverletzung vorgeworfen wird. Sie nehmen sich daher einen kurzen Moment Zeit und betrachten die E-Mail genauer.



**Von:** Facebook-Seite <support@notification.ivovdlinden.nl>
**Gesendet:** Montag, 18. August 2025 09:51
**An:** Kampagne "Erfolgreich Handeln" <erfolgreichhandeln@ibi.de>
**Betreff:** Mitteilung über eine Markenrechtsverletzung

**Mitteilung über eine Verletzung geistigen Eigentums**

Wir haben die Information erhalten, dass Ihre Seite Inhalte oder Marken verwendet, die dem geistigen Eigentum Dritter unterliegen und ohne Genehmigung genutzt werden.

Gemäß den Richtlinien sowie den geltenden gesetzlichen Bestimmungen kann ein solcher Verstoß dazu führen, dass Ihre Seite eingeschränkt, entfernt oder deaktiviert wird.

Sollten Sie der Ansicht sein, dass es sich um ein Missverständnis handelt, bitten wir Sie, entsprechende Nachweise über Ihr Eigentumsrecht oder eine schriftliche Genehmigung zur Nutzung der Marke vorzulegen, damit wir den Fall erneut prüfen können.

Noch einmal danken wir Ihnen herzlich für Ihren Beitrag dazu, Facebook zu einem sichereren und nützlicheren Ort für alle zu machen.

Antrag auf erneute Überprüfung

Mit freundlichen Grüßen,
Ihr Facebook-Support-Team

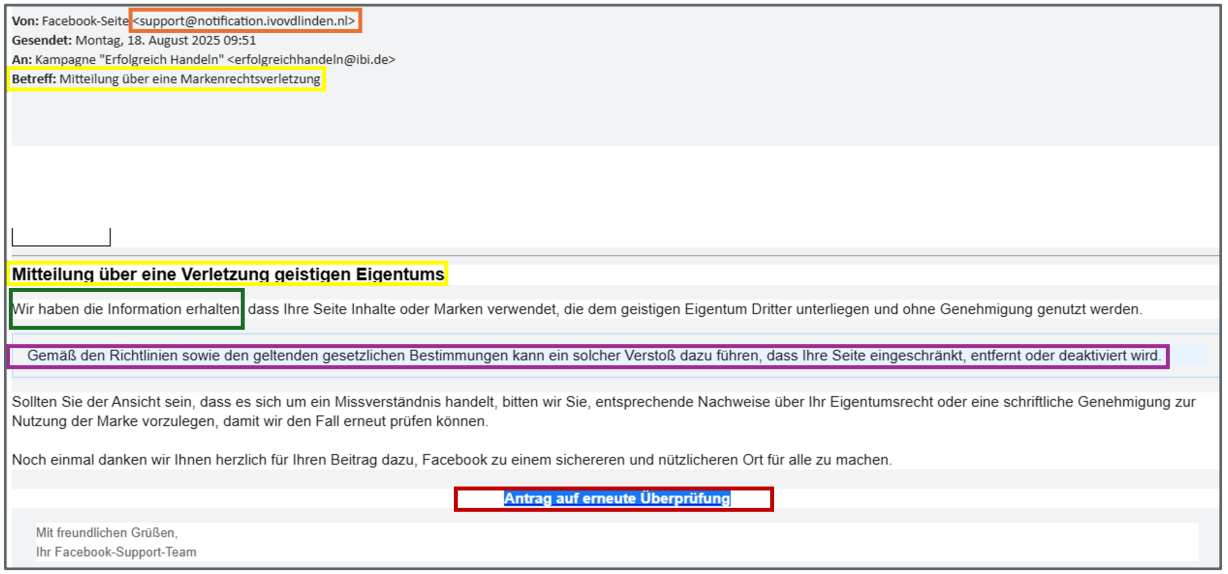
© Facebook. Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Irlande

*Abbildung 1 Beispielhafte E-Mail für den Versuch eines Online-Betrugs*

**Beantworten Sie für sich die folgenden Fragen:**

- Um welche Betrugsform handelt es sich?
- Nennen Sie verdächtige Merkmale dieser E-Mail!
- Begründen Sie kurz, warum diese Merkmale verdächtig auf Sie wirken!
- Was für Konsequenzen befürchten Sie?
- Welche konkreten Schritte würden Sie als Betroffener jetzt sofort unternehmen?

# Lösungsmöglichkeiten




**Um welche Betrugsform handelt es sich?**

↗ Es handelt sich um eine Phishing-E-Mail.

**Nennen Sie verdächtige Merkmale dieser E-Mail. Begründen Sie kurz, warum diese Merkmale verdächtig auf Sie wirken!**

| **Merkmal** | **Verdächtig, weil…** |
|---|---|
| Absenderadresse | Die E-Mail wird von der Absenderadresse *„support@notification.ivovdlinden.nl“* anstatt der offiziellen Domain *@facebook.com* versendet. Eine Domain ist der eindeutige Name einer Website.<br>→ Diskrepanzen zwischen der tatsächlichen Domain und der zugestellten Domain sind sehr typisch („domain mismatches“) |
| Keine Übereinstimmung von Betreff und der ersten großen Überschrift | Unstimmigkeit kann auf kopierten oder automatisierten Text hindeuten. |
| Generische oder keine Anrede | Keine Anrede/„Guten Tag“ statt persönlichem Hinweis (z. B. Seitenname, Kundennummer), denn Phisher wissen oft nicht genug Details |
| Dringlichkeits- oder Drohton („12 Stunden“, „rechtliche Schritte“ etc.) | Die E-Mail setzt den Empfänger unter Zeitdruck („innerhalb von 12 Stunden“) bzw. droht mit Konsequenzen wie einer Sperre oder rechtlichen Schritten. Das ist ein typisches Merkmal von **sozialer Manipulation**, bei der durch Angst und Stress schnelle, unüberlegte Handlungen provoziert werden sollen, wie etwa das Klicken auf einen schädlichen Link. |

**Was für Konsequenzen befürchten Sie?**

- Installation von Malware (schädliche Software) oder Ransomware (Erpressungstrojaner oder Verschlüsselungstrojaner)
- Anmeldung auf gefälschter Seite und Verlust von Zugangsdaten
- Account-Übernahme oder Weitergabe sensibler Daten
- Banking- oder Zahlungsdatenverlust, wenn Zahlungsinformationen verlangt werden

**Welche konkreten Schritte würden Sie als Händler sofort unternehmen?**

- Nicht klicken, nicht antworten und keinen Anhang öffnen!
- E-Mail als Beleg kopieren und an den offiziellen Support der Plattform melden (z. B. über den Meta-Hilfebereich für Unternehmen direkt über die Webseite oder die App)!
- URL im Browser nicht öffnen, stattdessen manuell die Plattformseite aufrufen (hier: facebook.com) und dort Sicherheits- oder Benachrichtigungsbereich prüfen!
- IT oder internen Sicherheitsverantwortlichen im Unternehmen informieren; ggf. Passwort ändern und Zwei-Faktor-Authentifizierung (2FA) überprüfen oder aktivieren!
- Falls bereits geklickt: Passwörter sofort ändern, betroffene Zahlungsquellen sperren und verwendetes Gerät mit Antivirus-Software prüfen!
- Meldung an Verbraucher- oder Datenschutzstelle und ggf. Anzeige erstatten (bei finanziellem Schaden)!

# Impressum


### Herausgeber

ibi research an der Universität Regensburg GmbH

Galgenbergstraße 25, 93053 Regensburg

### Geschäftsführung

Dr. Anja Peters und Dr. Georg Wittmann

Registergericht Amtsgericht Regensburg: Registernummer HR Regensburg B 5409

Soweit keine redaktionelle Kennzeichnung für den Inhalt: Verantwortliche im Sinne des Presserechts und des Medienstaatsvertrages:

Dr. Anja Peters und Dr. Georg Wittmann

Galgenbergstraße 25, 93053 Regensburg

www.erfolgreich-handeln.bayern

Tel.: +49 (0)941 788391-0

E-Mail: erfolgreichhandeln@ibi.de

### Titelbild

Foto von Jefferson Santos auf Unsplash (https://unsplash.com/de/fotos/person-die-laptops-benutzt-9SoCnyQmkzI)

### Text und Gestaltung

Susanne Dierl, Dr. Natalie Schmiede


# Über die Kampagne

Die Kampagne „Erfolgreich handeln“ des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie, bietet bayerischen Händlern praxisnahe und kostenfreie Informationsveranstaltungen, um sie bei der Bewältigung aktueller Herausforderungen zu unterstützen und somit deren Wettbewerbsfähigkeit nachhaltig und zukunftsorientiert zu sichern.

Das vielfältige Veranstaltungsangebot in Form von Webinaren und Präsenz-Workshops reicht von Themen wie Online-Handel und Prozessoptimierung (z. B. Warenwirtschaftssysteme) bis hin zu Nachhaltigkeit (z. B. Energieeinsparung) und Kundenbindung. Um bestmöglich auf akute Bedarfe der bayerischen Händler eingehen zu können, können jederzeit eigene Themenwünsche angebracht werden.

Stand: September 2025