Bundesministerium
Inneres
Bundeskriminalamt

GEMEINSAM.SICHER
mit unserer Polizei

HANDELS
VERBAND

Sicherheitsstudie 2023

Impressum

HANDELSVERBAND – Verband österreichischer Handelsunternehmen
Verein nach dem Vereinsgesetz 2002, zust. Vereinsbehörde. BPD Wien, ZVR: 688103413
Geschäftsführer: Ing. Mag. Rainer Will | **Präsident:** Dr. Stephan Mayer-Heinisch
Vizepräsident:innen: Karin Saey, Mag. Harald Gutschi, Horst Leitner, Norbert W. Scheele

Studiendesign & Textierung: Mag. Gerald Kühberger, MA
Lektorat: Michaela Kröpfl, Barbara Stocker
Design: Gebrüder Pixel

Executive Summary

Ladendiebstähle verursachen im österreichischen Handel einen jährlichen Schaden von rund 500 Mio. Euro. Aber auch Raubüberfälle, Falschgeld, Bankomat-Sprengungen und Bandenkriminalität zählen zu den **Sicherheitsrisiken im stationären Handel.** 82% der für die Sicherheitsstudie 2023 befragten Händler mit physischen Geschäften haben bereits Erfahrung mit Kriminalität im stationären Handel gemacht, 40% sogar mehrfach. Die Liste der **häufigsten Vergehen** wird angeführt vom klassischen **Ladendiebstahl (89%)**, gefolgt von der Bezahlung mit Falschgeld (43%), organisierter Bettelei und Vandalismus im Shop (je 22%) sowie Bandenkriminalität (18%). Fast alle Händler haben konkrete **Maßnahmen zum Schutz** vor Kriminalität im eigenen Geschäft in Verwendung. Am häufigsten setzen die Betriebe auf **Mitarbeiterschulungen (63%)**, Videoüberwachung (59%), das Verschließen aller Betriebsräume (52%), die Nutzung von Warensicherungsanlagen und Einbruchmeldeanlagen (44%) sowie besondere Maßnahmen für „Hot Products“ (40%).

Neben Sicherheitsrisiken im stationären Handel sind im letzten Jahrzehnt zahlreiche neue Gefahren hinzugekommen, die mit dem Aufstieg des Onlinehandels einher gehen. **Cybercrime** und **Bestellbetrug** verzeichnen seit Jahren enorme Zuwachsraten. Unter den für diese Studie befragten Onlinehändlern wurden bereits **64% Opfer von Betrug**, 34% sogar schon mehrmals.

Von den Betrieben mit mehr als 10 Beschäftigten gaben drei Viertel (75%) an, in Verbindung mit ihrem Webshop bereits mit Online-Betrug in Berührung gekommen zu sein, bei den kleineren Betrieben waren es 54%. Im Vergleich zu 2021 (62%) hat die Betrugshäufigkeit in allen Größenklassen zugenommen. Zu den gängigsten Formen von **Cybercrime im Handel** zählen aktuell **Phishing (61%)**, Malware-Angriffe (52%), Cyber-Erpressung durch Hacker (32%), Ransomware (28%) und Botnetze bzw. DDoS Angriffe (16%). Bei den **eCommerce-Betrugsformen** häufen sich zurzeit vor allem Bestellungen, bei denen den Käufer:innen vorab bewusst ist, dass sie die Rechnung nicht begleichen werden können (57%). Auch die Angabe der Identität anderer Personen (51%) und die Nutzung verfälschter Namens- bzw. Adressdaten (50%) sind in der Beliebtheitsskala der Kriminellen nach oben gewandert. Fast jeder zweite Webshop hat schon Erfahrung mit Kund:innen gemacht, die den Erhalt der Ware abstreiten, obwohl sie diese erhalten haben (47%).

Bei den kleineren Handelsbetrieben beläuft sich die durch Online-Betrug verursachte Schadenssumme in den meisten Fällen (30%) bis 500 Euro, in 30% zwischen 500 und 10.000 Euro. Unternehmen mit mehr als zehn Beschäftigten erlitten 2022 im Schnitt wesentlich höhere Verluste: 32% der entstandenen Schäden machten zwischen 5.000 und 10.000 Euro aus, bei 27% beliefen sich die finanziellen Einbußen auf 10.000 bis zu 100.000 Euro. Um das Betrugsrisiko zu reduzieren, kombinieren Webshops meist verschiedenste Schutzmaßnahmen – und verzichten dafür auch auf potentielle Mehrumsätze. So setzen 61% der Befragten auf sichere Zahlungsmethoden und 42% auf eingeschränkte Lieferoptionen wie ausschließliche Inlandslieferungen. Als **gängigste Zahlungsmethode** erweist sich die **Kreditkarte,** mit der in 83% der Webshops bezahlt werden kann, gefolgt von **PayPal** (78%) **Sofort-Überweisung/Klarna** (69%) und **Vorkasse** (65%). Zwei Fünftel der heimischen Handelsbetriebe bietet auch die Option Kauf auf Rechnung an.

Trotz der Vielzahl potentieller Schutzmaßnahmen gegen Online-Betrug gaben 18% der Befragten an, sich bis dato noch nicht mit diesem Thema beschäftigt zu haben. 37% der Unternehmen nutzen derzeit auch keine spezielle Lösung zur Betrugsvermeidung, etwa keine Identitätsprüfung.

In Sachen **Anzeigeerstattung** bei Online-Betrug bestätigten 67% der Händler, zukünftige Betrugsfälle bei der Polizei anzeigen zu wollen. Das Hauptaugenmerk liegt dabei auf der Servicequalität: 89% wünschen sich, eine Anzeige jederzeit erstatten zu können, 68% möchten mit einem Besuch alles erledigt wissen.

Auch **eCommerce-Gütesiegel** wurden im Zuge der Umfrage analysiert. Am bekanntesten unter den Befragten ist das **Trusted-Shops-Gütesiegel** mit 80%, gefolgt vom **Österreichischen eCommerce-Gütezeichen** (66%) und den Siegeln **Trustmark Austria** sowie **Ecommerce Europe Trustmark** mit einem Bekanntheitsgrad von 61% bzw. 44%.

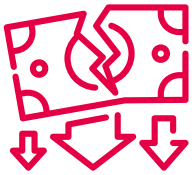
Neben der Unternehmensseite wurde für die SICHERHEITSSTUDIE 2023 auch die **Konsumentenperspektive** beleuchtet. Das Ergebnis: Ein Drittel der heimischen Verbraucher:innen hat bereits negtive Erfahrungen mit Schadsoftware wie Viren oder Trojanern gemacht. 20% waren schon von Datendiebstahl durch Hacker-Angriffe und Phishing betroffen, weitere 18% waren Opfer von Betrug bei Online-Transaktionen und jede:r Zehnte hat Bekanntschaft mit digitaler Erpressung gemacht. 76% der Österreicher:innen versuchen, sich mit Virenschutz- Programmen vor Cyberangriffen zu schützen. 55% setzen auf regelmäßige Software Updates und fast zwei Drittel (63%) haben eine Firewall implementiert. Beunruhigend ist, dass bereits ein Viertel aller Konsument:innen (26%) Opfer von **Fake-Webshops** geworden sind.

Diese alarmierenden Zahlen werden auch von der aktuellen **Kriminalstatistik des BMI** bestätigt. 2022 wurde im Cybercrime-Bereich ein neuer Höchstwert von 60.195 Anzeigen verzeichnet. Besonders der Onlinehandel ist von Betrugsdelikten stark betroffen. Die positive Nachricht? Die Aufklärungsquote der Polizei bleibt konstant hoch.

Sicherheit im stationären Handel

82%
der Händler waren bereits Opfer von Kriminalität im stationären Handel

40%
mehrfach



500 Mio. €
jährlicher Schaden durch Ladendiebstähle in Österreich

Top 5 Delikte

1. Ladendiebstahl
2. Bezahlung mit Falschgeld
3. Vandalismus im Shop
4. Organisierte Bettelei
5. Bandenkriminalität

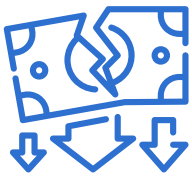
Top 5 Schutzmaßnahmen

1. Personalschulungen
2. Videoüberwachung
3. Verschluss aller Betriebsräume
4. Warensicherungsanlagen
5. Schutz von „Hot Products“

Sicherheit im Onlinehandel

64%
der Händler waren bereits Opfer von Cybercrime & Betrug im Netz

34%
mehrfach



16 Mio. €
jährlicher Schaden durch Cybercrime in Österreich

Top 5 Delikte (Händlersicht)

1. Datendiebstahl/Phishing
2. Malware-Angriffe
3. Cyber-Erpressung
4. Ransomware
5. Botnetze & DDoS Angriffe

Top 5 Delikte (Konsumentensicht)

1. Schadsoftware (Viren, Trojaner)
2. Datendiebstahl/Phishing
3. Betrug bei Online-Transaktionen
4. Digitale Erpressung (Ransomware)
5. Identitätsdiebstahl

Bundesministerium
Inneres
Bundeskriminalamt

Gerhard Karner
Bundesminister für Inneres

Vorwort

Sicherheitsstudie 2023

Die Digitalisierung hat alle Bereiche unseres Lebens nachhaltig verändert. Dazu gehört auch das Einkaufsverhalten, das sich in den vergangenen Jahren sehr oft in den Onlinebereich verlagert hat. Mit dieser Veränderung gehen jedoch neue Kriminalitätsformen einher. Dies schlägt sich auch in der Kriminalitätsstatistik nieder, in der seit Jahren ein Anstieg von Internetkriminalität und Onlinebetrug zu erkennen ist.

Der Onlinehandel bietet für heimische Händler viele Möglichkeiten, neue Absatzwege zu erschließen. Gleichzeitig steigt das Risiko, Opfer von Betrug zu werden. Allein 2022 waren 64 Prozent aller österreichischen Online-Händler mit Online-Betrug konfrontiert. Dazu kommen zahlreiche weitere Formen der Internetkriminalität wie das Ausspähen von Passwörtern, Schadsoftware oder Online-Erpressung.

Das Innenministerium steuert hier konsequent dagegen. Dank der Modernisierung der Polizei in diesem Bereich – Stichwort Cybercobra – bleibt die Aufklärungsquote konstant hoch. Gleichzeitig ist es wichtig, Präventionsarbeit zu leisten und Händlern Möglichkeiten für Schutzmaßnahmen aufzuzeigen. Mit konkreten Maßnahmen lassen sich die Risiken, Opfer von Internetkriminalität zu werden, erheblich senken.

Als Innenminister ist mir die Sicherheit der Bürgerinnen und Bürger ein großes Anliegen. Daher sind Studien wie diese besonders wertvoll, um Erkenntnisse über die Handlungsweise Krimineller zu erlangen und daraus Präventionsmaßnahmen abzuleiten. Ich bedanke mich beim Handelsverband und dem Bundeskriminalamt, die Jahr für Jahr die Sicherheitsstudie umsetzen und damit einen wichtigen Beitrag für mehr Sicherheit im Handel leisten.

Ihr Gerhard Karner

HANDELS VERBAND

Rainer Will
Geschäftsführer Handelsverband

Einleitung

Mit dem Handelsverband auf der sicheren Seite

Die Digitalisierung hat unser Einkaufsverhalten nachhaltig verändert. Wir kaufen ein, wann, wo und wie wir wollen. Den Kern dieses Wandels bildet das Internet, mit allen positiven wie negativen Begleiterscheinungen für den Handel. Wenngleich die eCommerce-Umsätze im Vorjahr – erstmals in den letzten 20 Jahren – zurückgegangen sind, wächst das Risiko für Betrug im Netz weiter. Das ist eine zentrale Erkenntnis der Sicherheitsstudie 2023, die wir gemeinsam mit dem Bundesministerium für Inneres und dem Bundeskriminalamt erstellt haben.

Knapp zwei Drittel der heimischen Handelsbetriebe waren bereits Opfer von Kriminalität im Netz, ein Drittel sogar mehrfach. Damit steht Internetbetrug ganz weit oben auf der Liste potenzieller Bedrohungen für den Handel. Ähnlich ist die Situation auf Konsumentenseite: Jede:r Zweite schätzt die Gefahren im eCommerce als hoch ein. Ein Viertel der Bevölkerung hat bereits Erfahrungen mit Fake-Webshops gemacht. Für Online-Shopper zählt Sicherheit mittlerweile zu den wichtigsten Kaufkriterien. Die Abwehr von Datendiebstahl, Identitätsmissbrauch und Bestellbetrug stellt Webshops und Marktplätze vor immer größere Herausforderungen.

Vor allem KMU-Händler zählen zu den beliebtesten Zielen von Hackern und Betrüger:innen, da viele davon ausgehen, kleine Webshops seien nicht ausreichend geschützt.

Der Handelsverband unterstützt Webshops mit dem eCommerce Gütesiegel TRUSTMARK AUSTRIA sowie im Rahmen der Initiative GEMEINSAM SICHER IM ONLINE-HANDEL mit kompetenten Partnern dabei, sich digital optimal aufzustellen. Das Investment in digitale Sicherheit zahlt sich aus, denn der jährliche Schaden durch Cybercrime liegt hierzulande bereits bei mehr als 16 Mio. Euro.

Heuer möchten wir aber auch einen besonderen Fokus auf die Sicherheit im stationären Handel richten. Immerhin verursachen Ladendiebstähle hierzulande einen jährlichen Schaden von rund 500 Mio. Euro. Auch Raubüberfälle, die Bezahlung mit Falschgeld, Bankomat-Sprengungen und Bandenkriminalität zählen zu den Sicherheitsrisiken auf der Fläche. Worauf müssen Sie als Händler achten, damit das Geschäft und der Webshop nicht nur florieren, sondern vor allem auch sicher sind? Diese Frage wollen wir mit der Sicherheitsstudie 2023 beantworten.

Bundesministerium
Inneres
Bundeskriminalamt

Manuel Scherscher
Leiter der Initiative „GEMEINSAM.SICHER“
Stellvertr. Direktor Bundeskriminalamt

Prävention als Schlüssel zum Erfolg

Wie bereits in den Jahren zuvor haben wir auch im Jahr 2022 einen deutlichen Anstieg bei der Internetkriminalität verzeichnet. Dieser betrifft natürlich auch den Online-Handel, gerade in der Form des Waren- und Bestellbetrugs. Entsteht bei den einzelnen Taten zumeist kein hoher Schaden, so entsteht in Summe jedoch ein wesentlicher finanzieller Schaden, sowohl bei den Privatpersonen als auch bei den Unternehmen. Gerade im letzten Jahr hat sich wieder gezeigt, wie dreist und rasch die Kriminellen auf geänderte Umstände reagieren. In Krisenzeiten werden die Sorgen und Ängste der Menschen durch die Täter schamlos ausgenutzt, um Profit zu lukrieren. Als Beispiel seien hier Fake-Onlineangebot von Brennmaterial wie Pellets erwähnt, die kurz nach dem Beginn der Energiekrise aufgetaucht sind. Grundsätzlich kann man gerade im Bereich des Warenbetruges sagen, ist ein Angebot „zu gut, um wahr zu sein“, sollte man höchst vorsichtig sein. Durch eine kurze Onlinerecherche können utopische Preise leicht erkannt werden und auch die Online-Bewertungen der Händler geben rasch Aufschluss darüber, ob es sich um ein vertrauenswürdiges Angebot handelt oder nicht. Aber auch hier muss man erwähnen, dass die Kriminellen immer einfallsreicher werden und vor allem professioneller agieren. Fakeshops sind, zumal das Angebot an legalen Möglichkeiten auch ständig expandiert, immer schwieriger von echten Shops zu unterscheiden. Im Gegenteil, um die Daten der Kunden zu erhalten, werden Phising-Seiten erstellt, die der Originalseite oft bis ins letzte Detail nachgebildet wurden. Konto- und Kreditkartendaten sollten daher nur über sichere Verbindungen, diese sind in der Adresszeile aufgrund der Buchstaben „https“ zu erkennen, übermittelt werden. Neben dem Anstieg im Bereich der Kriminalität im Online-Handel, dürfen wir auch die sich verändernden Sicherheitsansprüche im stationären Handel, einen wichtigen und treibenden Faktor der Wirtschaft in unserem Land, nicht außer Acht lassen. Es bedarf einer breiten Phalanx, um in den betroffenen Bereich auf die rasch wechselnden und an die jeweiligen Situationen angepassten Modi Operandi zu reagieren.

Im Rahmen der Initiative „GEMEINSAM.SICHER in Österreich“ sind wir im steten Austausch mit unseren Partnern, um zielgruppenorientiert die Betroffenen zu unterstützen und gemeinsame Strategien zu erarbeiten. Die Prävention ist unsere Möglichkeit, mit umfassenden Informationen der Kriminalität einen Riegel vorzuschieben. Ich möchte mich herzlich beim Handelsverband bedanken, der uns als starker Partner zur Seite steht. Durch die hervorragende Kooperation kann sowohl den Händlerinnen und Händlern als auch den Kundinnen und Kunden, das essenzielle Werkzeug in die Hand gegeben werden, um sich vor Kriminellen zu schützen.

Inhalt

Executive Summary 3

Vorwort 6

Einleitung 7

Gastkommentare 10

Sicherheit im stationären Handel 14

Sicherheit im Onlinehandel 18

Betrugsformen 22

- Schadenshöhe 23
- Maßnahmen 24
  - Risikominimierung 25
  - Betrugsvermeidung 26

Zeitpunkt der Maßnahmen 27

- Anzeigeerstattung 28

Payment & Kundenidentifizierung 30

Gütesiegel 35

Consumer Check 38

Kontaktdaten 44

Gast-kommentare

Patricia Grubmiller
Head of Legal Handelsverband

Das Zauberwort heißt Vertrauen

Transparenz, Kommunikationsbereitschaft und unabhängige Dritte können dabei helfen

Vertrauen spielt beim Online-Shopping eine große Rolle. Um dieses aufzubauen, können Online-Händler verschiedene Strategien anwenden. Transparenz, Sicherheit, der Einsatz von Kundenbewertungen und Gütesiegeln stellen dabei die wichtigsten Pfeiler dar, um sich von unseriösen Angeboten abzugrenzen.

Beim Vertrauensaufbau ist insbesondere die Gestaltung einer professionellen und benutzerfreundlichen Website von besonderer Bedeutung. Diese sollte übersichtlich und leicht navigierbar sein, eine klare Struktur aufweisen und sicherstellen, dass Kund:innen einfach und sicher bestellen können. Zudem sollten Online-Händler klare Informationen über Versand- und Rückgabebedingungen bereitstellen, um Unsicherheiten und Fragen zu vermeiden. Eine klare und verständliche Beschreibung der angebotenen Produkte ist ebenfalls wichtig.

Die Qualität des Kundenservice und die Kommunikationsbereitschaft ist ein weiterer Faktor, der Vertrauen aufbauen kann. Indem Sie verschiedene Support-Kanäle wie E-Mail, Telefon, WhatsApp oder Facebook Messenger zur Verfügung stellen, vermitteln Sie Ihren Kund:innen ein Gefühl der Sicherheit und zeigen, dass Ihnen ihre Anliegen am Herzen liegen. Eine schnelle und professionelle Reaktion auf Anfragen und Beschwerden muss oberste Priorität haben.

Ein weiteres Mittel zur Vertrauensbildung gelingt mithilfe unabhängiger Dritter. Durch die Veröffentlichung positiver Kundenmeinungen und -erfahrungen können Zweifel und Unsicherheiten potenzieller Kund:innen beseitigt werden aber auch unabhängige Gütesiegel, etwa das Trustmark Austria des Handelsverbandes, bieten eine wertvolle Orientierungshilfe, um auf einen Blick zu erkennen, ob es sich um einen vertrauenswürdigen Webshop handelt.

So machen wir das Shoppen GEMEINSAM SICHER IM ONLINEHANDEL.

Weitere Informationen finden Sie auf
www.trustmark-austria.at

Gerald S. Eder
Director Digital Solutions, eCommerce
CRIF Austria

Kauf auf Rechnung mit Sicherheit mehr Conversion

Für Konsument:innen die sicherste Zahlungsmethode, für Onlinehändler ein erhöhtes Risiko. Kauf auf Rechnung ist europaweit ein Trend, der richtigen Sicherheitsmaßnahmen benötigt.

Die beiden häufigsten Betrugsformen im eCommerce sind mit 57% die Rechnung bewusst nicht zu bezahlen oder eine falsche Identität anzugeben (51%). Folglich ist es für viele Onlineshops die erste Reaktion, zur Betrugsvermeidung auf sichere Zahlungsmethoden wie die Kreditkarte zu setzen. Dem gegenüber steht die beliebteste Zahlungsart der Onlineshopper, mit Rechnung erst nach Erhalt der Ware zu bezahlen.

Da bereits ein Viertel aller Konsument:innen negative Erfahrungen mit Fake-Webshops gemacht haben, bietet ihnen Kauf auf Rechnung mehr Sicherheit. Dieses diametrale Sicherheitsverhalten lässt sich durch geeignete Sicherheitsmaßnahmen zu aller Zufriedenheit zusammenführen. Bei Kauf auf Rechnung ist für den Händler, der in Vorleistung geht, wichtig, eine Risikoprüfung durchzuführen: sicherzustellen, dass die Konsument:innen die Rechnung tatsächlich bezahlen. Wer jemand ist, ist für Händler ein weiterer Sicherheitsaspekt, der wesentlich das Betrugsrisiko reduziert.

Eine sichere digitale Identität hilft dabei, Betrug und Identitätsdiebstahl zu vermeiden, indem sie sicherstellt, dass das Onlinegeschäft von einer echten Person durchgeführt wird. Je nach Wert des Warenkorbs und Art des Onlinegeschäftes zeigen die Erfahrungen, dass der Einsatz von Identifikations-Verfahren das Betrugsrisiko nachweislich senkt.

Für das erfolgreiche Onlinegeschäft sind für den Händler Sicherheit und Conversion essentiell. Durch Technologie und Automatisierung wird die Digital Customer Journey so gestaltet, dass die Konsument:innen in ihrem Shoppingerlebnis nicht gestört werden, der Händler jedoch eine maximale Sicherheit hat, was das Geschäft erfolgreich macht. So sind beide zufrieden und eine loyale Kundenbeziehung entsteht.

www. crif.at

Robert Spevak
Abteilungsleiter Revision, Sicherheit, Arbeitsschutz
METRO Österreich

Vertrauen ist gut, Kontrolle ist besser

Das schwächste Glied in der Security-Kette ist der Mensch. Der ist immerhin lernfähig.

Vertrauen ist gut, Kontrolle ist besser – dieses Credo gilt natürlich auch in der Unternehmenspraxis. Die unternehmenseigenen Spezialist:innen überprüfen alle funktionalen Geschäftsbereiche des Betriebs auf mögliche Risiken. Sie sind traditionell für die Einhaltung interner Gesetze und Richtlinien verantwortlich. Keine oder nicht effektiv getroffene Maßnahmen und die damit verbundenen Kosten können ohne ein Kontrollsystem böse Überraschungen zur Folge haben. Wer die Risikofaktoren im Auge behält, kann sich besser auf die Konsequenzen/Maßnahmen vorbereiten. Mit einem Satz – Sicherheit geht uns alle an. Daher: Schätzen Sie ihre Spezialist:innen im Haus und schenken Sie deren Worten Aufmerksamkeit. Dies kann Ihr Unternehmen vor möglichen Schäden bewahren.

Kriminelle stehlen im stationären österreichischen Handel jährlich Waren in Höhe von rund 500 Mio. Euro. Das entspricht fast einem Prozent des Gesamtumsatzes. Hinzu kommen Schäden von rund 16 Mio. Euro durch Cybercrime. Wie weit verbreitet Ladendiebstahl, Vandalismus oder die Bezahlung mit Falschgeld im Handel tatsächlich sind, das zeigt die vorliegende Sicherheitsstudie 2023: 82% aller österreichischen Händler mussten schon Erfahrungen mit Kriminalität auf der Fläche machen, 64% waren bereits Opfer von Cyberkriminalität oder Betrug im Netz.

Die Angriffe auf Unternehmen sind heute häufiger, raffinierter und gefährlicher als je zuvor. Betriebe und ihre Beschäftigten bieten vielfach erhebliche Angriffsflächen für Schadsoftware oder gezielte Recherchen von Cyberkriminellen, um in das Unternehmensnetzwerk einzudringen. Und: Cyberkriminalität macht auch vor (privaten) Social Media-Kanälen nicht halt. Um Mitarbeiter:innen auf Onlinebetrug zu sensibilisieren, ist die Zusammenarbeit mit der Polizei entscheidend. Die Beamten kommunizieren, was aktuell im Umfeld passiert, die Betriebe können Hinweise an das eigene Personal weitergeben, damit diese vorbereitet sind. Denn der überwiegende Teil aller Security-Vorfälle ist auf menschliches Versagen zurückzuführen – das schwächste Glied in der Security-Kette ist der Mensch. Der ist aber lernfähig.

Sicherheit im stationären Handel

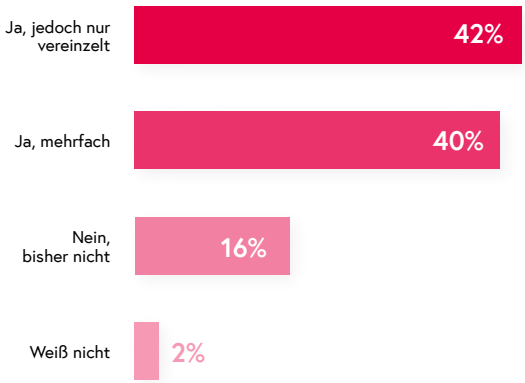
Sicherheit ist ein zentrales Thema für alle Unternehmen

Sie ist auch ein bedeutender Standortfaktor

Gelegenheitsdiebe und organisierte Banden stehlen im österreichischen Einzelhandel jährlich Waren in Millionenhöhe. Sie denken sich dabei immer neue Tricks aus.

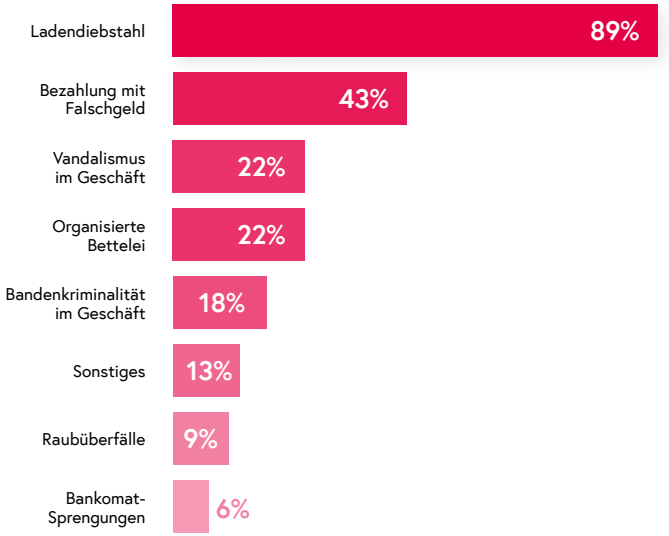
Doch auch der Handel verstärkt den Diebstahlschutz. Wie eingangs erwähnt, verursachen allein Ladendiebstähle im heimischen Handel einen jährlichen Schaden von rund 500 Mio. Euro. Das entspricht fast einem Prozent des Gesamtumsatzes. Auch Raubüberfälle, die Bezahlung mit Falschgeld, Vandalismus, Bankomat-Sprengungen und Bandenkriminalität zählen zu den Sicherheitsrisiken im stationären Handel. Und diese sind durchaus weit verbreitet: 82% aller österreichischen Händler mussten bereits Erfahrungen mit Kriminalität auf der Fläche machen, 40% sogar mehrfach.

Haben Sie in Ihrer Tätigkeit als Händler bereits Erfahrungen mit Kriminalität im stationären Handel gemacht?

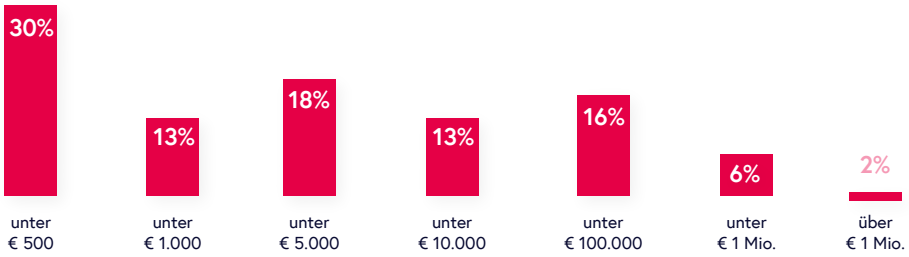


Die häufigsten Delikte

Die Liste der häufigsten Delikte im stationären Handel wird angeführt vom klassischen Ladendiebstahl durch kriminelle Kund:innen. Ein Fünftel der Ladendiebstähle geht allerdings auf unehrliche Mitarbeiter:innen, also auf das eigene Personal zurück. Bereits auf Platz 2 der häufigsten Delikte landet die Bezahlung mit Falschgeld, gefolgt von Vandalismus sowie organisierter Bettelei im bzw. direkt vor dem Geschäftslokal. Rang 5 geht an Bandenkriminalität, wohingegen Raubüberfälle und Bankomat-Sprengungen hierzulande erfreulicherweise relativ selten vorkommen.



Die Schadenssumme liegt in den meisten Fällen unter 500 Euro, bei 2% aller Delikte übersteigt sie allerdings die 1-Million-Euro-Marke.

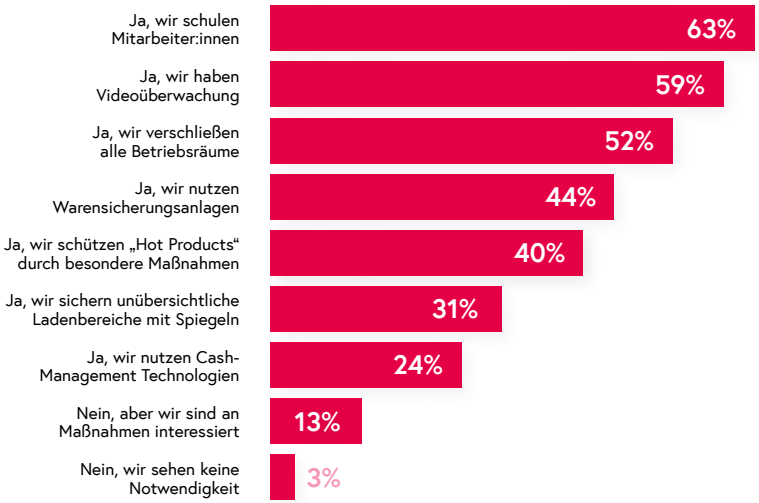


Wie können sich Händler vor Kriminalität schützen?

Die Palette an Gegenmaßnahmen ist vielfältig. Am weitesten verbreitet sind hierzulande Personalschulungen über den richtigen Umgang mit Verdächtigen (63%), die Implementierung einer Videoüberwachung (59%) sowie das Verschließen aller Betriebsräume, etwa Keller Garagen, Anliefertore, Fenster (52%). Fast die Hälfte aller Händler setzen auf Warensicherungs- und Einbruchmeldeanlagen, immerhin 40% schützen „Hot Products" durch besondere Maßnahmen.

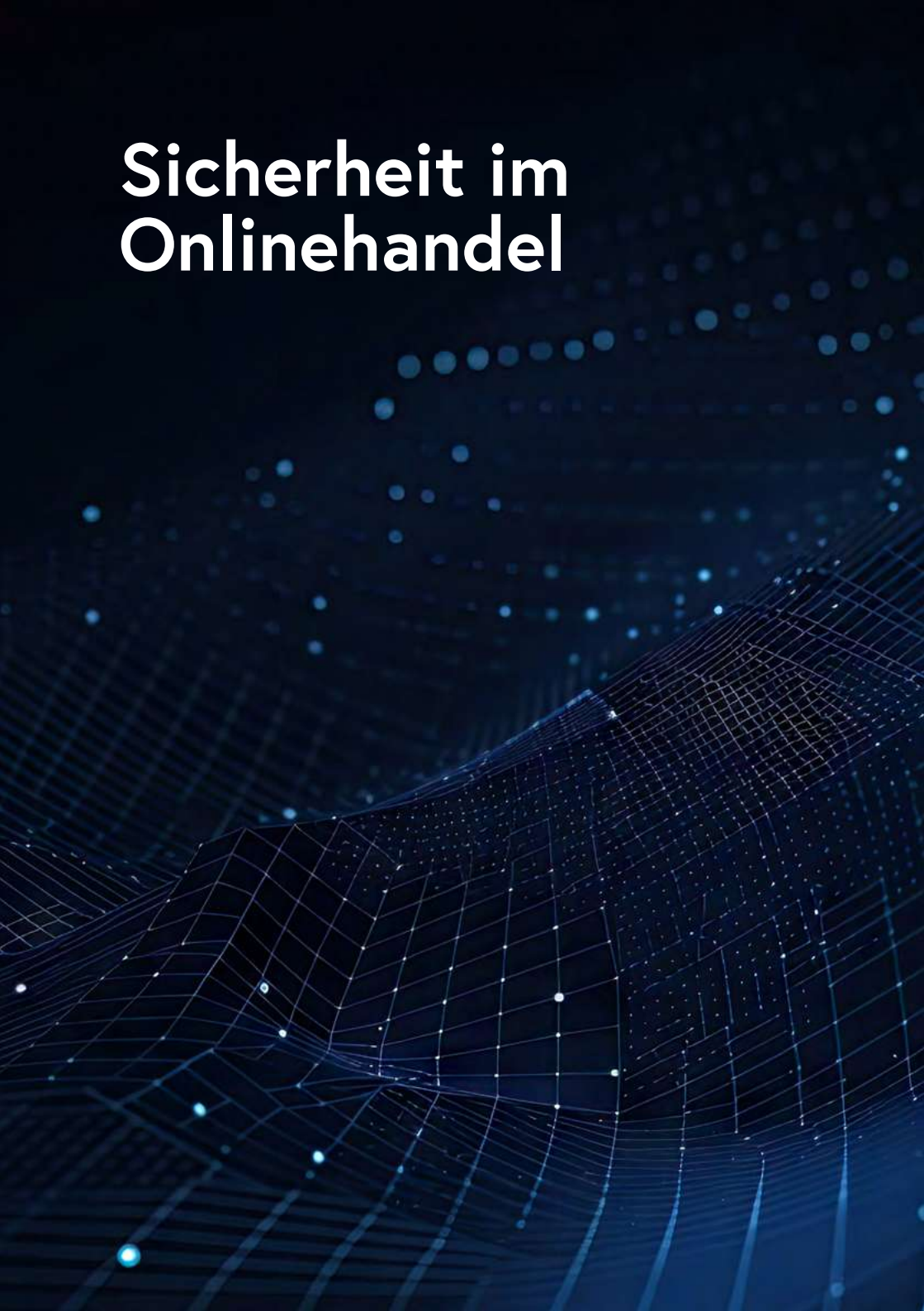
Als Folge von Warendaten-Analysen werden jene Produkte, die häufig geklaut werden, an besser beobachteten Stellen im Geschäft platziert. Knapp ein Drittel verwendet Spiegel zur Sicherung und Überwachung unübersichtlicher Ladenbereiche, ein Viertel nutzt überdies Cash-Management-Technologien oder eine automatisierte Bargeldverarbeitung. Lediglich 3% sehen überhaupt keine Notwendigkeit, Präventionsmaßnahmen zu ergreifen.

Haben Sie konkrete Maßnahmen zum Schutz vor Kriminalität im stationären Handel in Verwendung?



Sicherheit ist nicht nur ein Grundbedürfnis aller Menschen, es ist ein entscheidendes Wettbewerbskriterium für den Handelsstandort Österreich. Um diese Sicherheit gewährleisten zu können, bedarf es der täglichen Arbeit vieler Menschen in Behörden, Blaulicht- und Freiwilligenorganisationen, sowie Sicherheitsexpert:innen aus der Wirtschaft und aus den Unternehmen. Der Handelsverband erarbeitet in langjähriger Kooperation mit dem Bundesministerium für Inneres, dem Bundeskriminalamt, der Polizei und anderen Stakeholdern aus dem Sicherheitsbereich laufend Informations- und Serviceprodukte, um Sie als Händler bei der Umsetzung sicherheitsrelevanter Maßnahmen bestmöglich zu unterstützen. Einmal jährlich veranstalten wir den Sicherheitsgipfel, den alle Mitglieder des Handelsverbandes völlig kostenfrei besuchen können. Weitere Informationen dazu finden Sie auf www.sicherheitsgipfel.at

Sicherheit im Onlinehandel



Der Alltag im World Wide Web

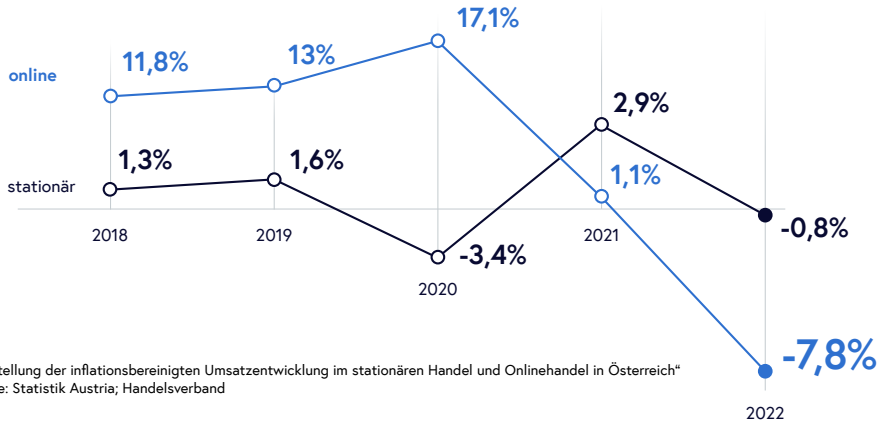
eCommerce-Entwicklung der letzten 5 Jahre

Während der Corona-Krise hat der Onlinehandel einen starken Boom erfahren. Im ersten Pandemiejahr 2020 sind die Umsätze um stolze 17,1% nach oben geklettert. 2022 musste der heimische eCommerce im Zuge der Teuerungskrise allerdings erstmals in seiner Geschichte ein reales Minus von fast 8% verkraften. Heuer gehen die Expert:innen wieder von einem moderaten Wachstum aus.

Unabhängig von der Unternehmensgröße ist Fakt: Wer seine Produkte zusätzlich über das Internet anbietet, eröffnet sich neue, von Öffnungszeiten unabhängige Absatzwege. Wie immer hat allerdings auch die eCommerce-Medaille eine Kehrseite: Je mehr Webshops, desto mehr damit verbundene Betrugsfälle. Gerade in Krisenzeiten steigen Cyberkriminalität und Online-Betrug massiv an. 2022 wurde in der Kriminalstatistik im Cybercrime-Bereich ein Höchstwert von 60.195 Anzeigen verzeichnet. Immerhin bleibt die Aufklärungsquote laut Bundeskriminalamts (BK) konstant hoch.

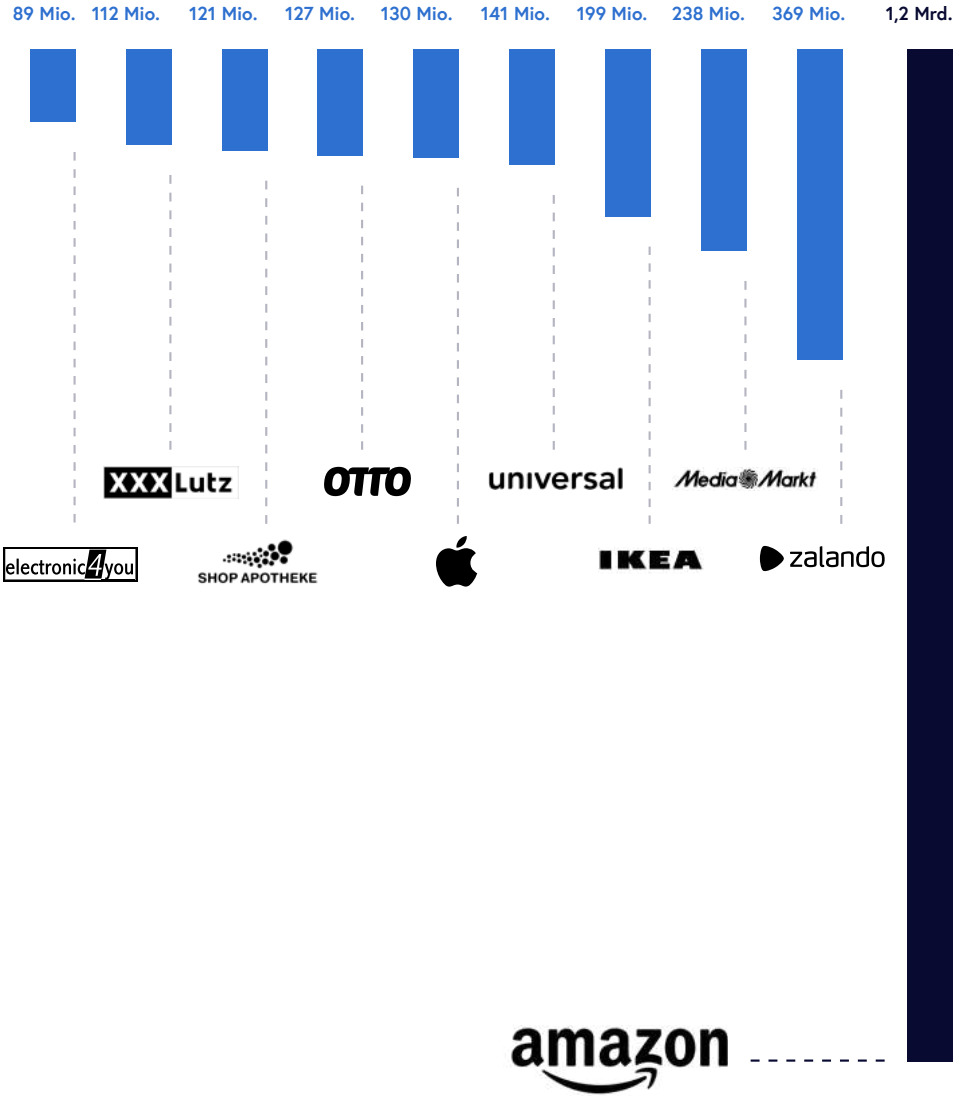
Um das Ausmaß der Online-Betrugsfälle in Österreich zu erfassen, hat der Handelsverband eine Umfrage unter 150 Handelsbetrieben durchgeführt. Das Ergebnis: **64% aller österreichischen Online-Händler wurden 2022 Opfer von Online-Betrug**, bei den größeren Unternehmen sogar 75%. Trotzdem sehen sich vor allem viele kleinere Betriebe nicht als potentielles Betrugsopfer und treffen deshalb diesbezüglich auch keine bzw. zu geringe Schutzmaßnahmen. Fast ein Fünftel aller Befragten (18%) haben sich bislang noch gar nicht mit dem Thema Betrugsprävention beschäftigt.

Zahlen, die klar belegen: In punkto Schutzmaßnahmen gegen Online-Betrug gibt es für Unternehmen noch Aufholbedarf. Vor allem, weil kein Onlinehändler vor Betrug gefeit ist, egal, ob groß oder klein. Und um welche Summe es sich auch handelt – jeder finanzielle Verlust ist ärgerlich und schadet dem Unternehmen.



„Darstellung der inflationsbereinigten Umsatzentwicklung im stationären Handel und Onlinehandel in Österreich"
Quelle: Statistik Austria; Handelsverband

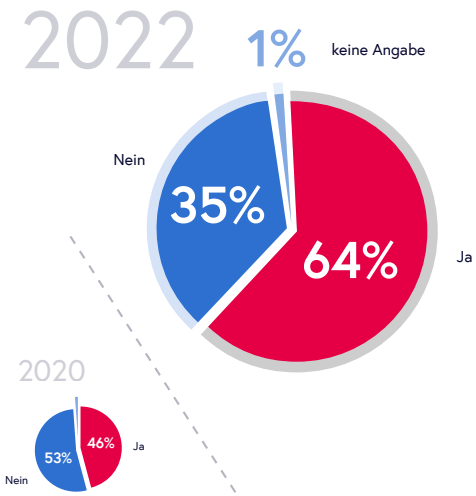
Die 10 umsatzstärksten Onlineshops in Österreich



(Umsatz 2021 in Mio. Euro)
Umsatzangaben beruhen auf Unternehmensinformationen und Hochrechnungen der ecommerceDB
Quelle: ecommerceDB

Erfahrungen mit Betrug & Cybercrime

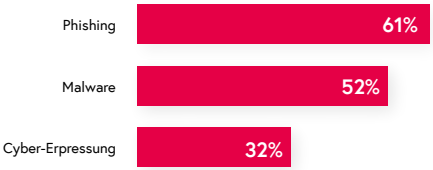
Die aktuelle Studie rund um Sicherheit im Onlinehandel belegt: Bereits 64% der befragten Onlinehändler haben in irgendeiner Form Erfahrungen mit Betrug gemacht – 34% sogar mehrmals. Im Vergleich mit 2020 sind die Betrugsfälle deutlich angestiegen. Ein Prozent der Befragten sind sich nicht sicher bzw. gaben an, nicht zu wissen, ob sie bezüglich ihres Webshops schon einmal Opfer von Betrug wurden. Von den Unternehmen mit über 10 Beschäftigten gaben drei Viertel (75%) an, in Verbindung mit ihrem Webshop bereits mit Online-Betrug in Berührung gekommen zu sein, bei den kleineren Betrieben waren es mehr als die Hälfte (54%).

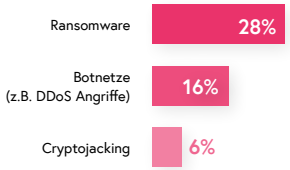


Formen von Cybercrime

Der Blick auf die häufigsten Formen von Cybercrime im österreichischen Handel ergibt ein klares Bild: 61% aller Händler waren bereits Opfer von Phishing-Angriffen, bei denen z.B. Login-Informationen erbeutet wurden. Jeder zweite Betrieb hat Erfahrung mit Malware, also Schadsoftware aus Spam-Mails oder manipulierten Links.

Auf Platz 3 rangiert die klassische Cyber-Erpressung (32%), bei der Hacker Geld verlangen, um angeblich drohende Angriffe noch abzuwenden. Ransomware (Angreifer verschlüsseln Daten und verlangen Lösegeld) belegt mit 28% Rang 4, gefolgt von Botnetzen bzw. DDoS-Angriffen, die zu einer Überlastung der Systeme führen (16%).



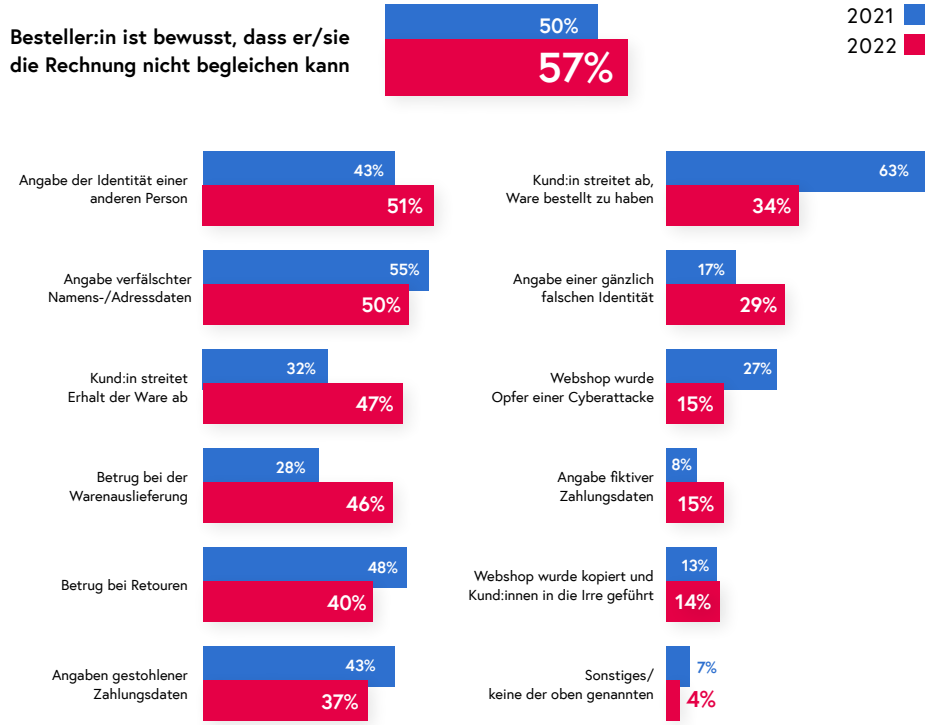


Formen von eCommerce-Betrug

Die Arten von Betrug, mit denen Onlinehändler konfrontiert sind, sind mannigfaltig. Man unterscheidet zwischen Identitätsbetrug, Zahlungsunfähigkeit, Zahlungsmittelbetrug, Bestellbetrug, Betrug im Zusammenhang mit der Lieferung bzw. mit Retouren sowie Cyberattacken.

Die Gesamtstatistik aller befragten Unternehmen – sowohl kleinere Betriebe als auch Unternehmen über 10 Beschäftigte – zeigt, dass Betrüger:innen häufig Waren bestellen, obwohl ihnen vorab bewusst ist, dass sie die Rechnung später nicht begleichen werden können (57%). Weit verbreitet ist auch die Angabe der Identität einer anderen Person (51%) bzw. die Angabe verfälschter Namens- oder Adressdaten (50%). Mit 47% Betroffenheit aller Befragten bildet das Abstreiten des Erhalts der Ware (obwohl diese mit Sicherheit korrekt ausgeliefert wurde) die vierthäufigste Betrugsform.

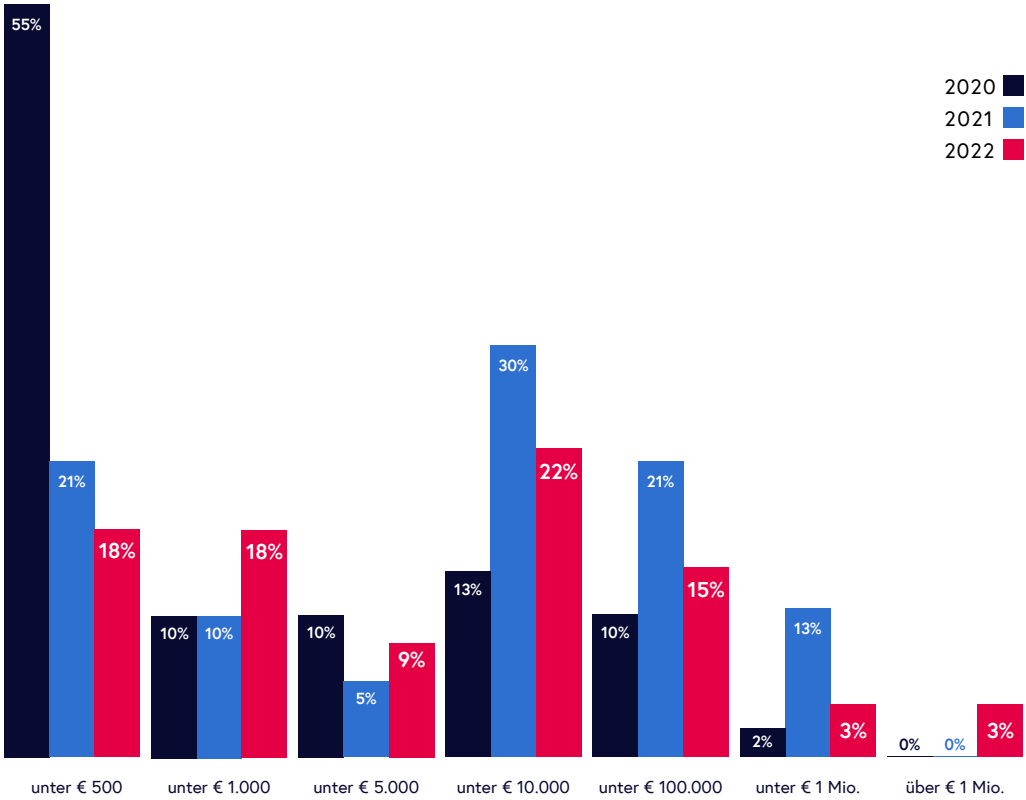
Auffällig sind die Unterschiede bei mit Lieferung und Retouren verbundenem Betrug zwischen Unternehmen mit weniger bzw. mehr als zehn Beschäftigten. Im Vergleich zu 16% bei den kleineren Händlern haben bereits 59% der größeren Unternehmen Erfahrungen mit Betrugsfällen bei Retouren gemacht.



Schadenssumme durch Online-Betrug im Jahr 2022

Bezogen auf die Gesamtstatistik zeigt sich, dass die Schadenssumme der Betrugsfälle im Onlinehandel 2020 noch mehrheitlich (55%) unter 500 Euro lag. 2021 und 2022 hat sich das Schadensausmaß jeweils signifikant erhöht: Im Vorjahr lag nur noch ein Fünftel (18%) der Schadenssummen unter 500 Euro, in 22% der Fälle verloren die Händler hingegen zwischen 5.000 und 10.000 Euro. Auch der Anteil der Fälle mit einem Schaden zwischen 100.000 und einer Million Euro ist von 2% auf 3% angewachsen. Erstmals wurde 2022 auch die Millionenmarke geknackt: in 3% der Betrugsfälle lag die Schadenssumme über diesem Wert. Die Studie macht auch deutlich, dass größere Unternehmen durch Online-Betrug im letzten Jahr wesentlich höhere wirtschaftliche Einbußen erlitten.

In den meisten Fällen (32%) belief sich die Schadenssumme bei Betrieben mit mehr als zehn Beschäftigten auf Beträge zwischen 5.000 und 10.000 Euro

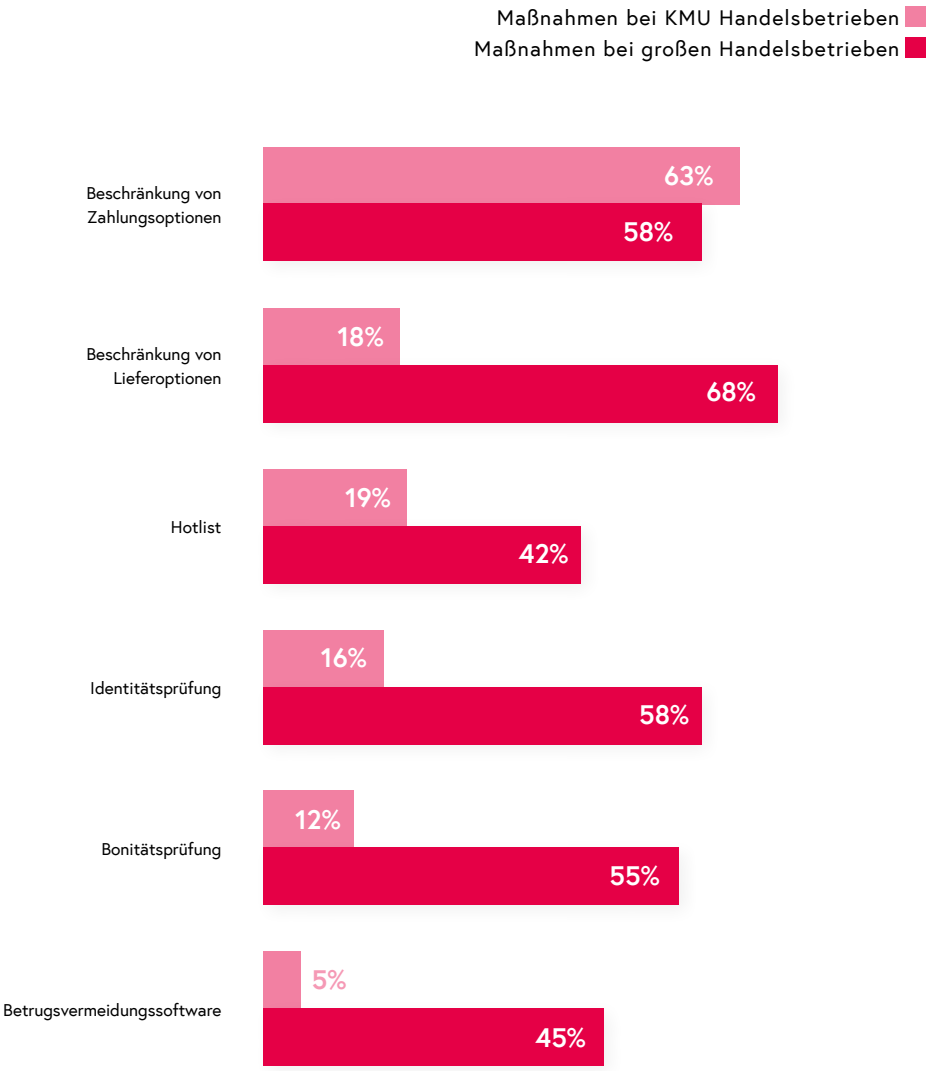


Maßnahmen zum Schutz vor Onlinebetrug

Bei der Frage, wie sich Onlinehändler gegen Betrug schützen, zeigt sich deutlich: Für die meisten wiegt Sicherheit höher als die Chance auf höheren Profit. Um das Betrugsrisiko zu senken, verzichten viele Unternehmen auf potentielle Mehrumsätze bzw. Absatzwege.

So setzen 61% der Befragten auf sichere Zahlungsoptionen (kein Kauf auf Rechnung etc.). Auf Platz zwei rangiert mit 42% die Einschränkung von Lieferoptionen – die Handelsbetriebe liefern zum Beispiel nur innerhalb des eigenen Landes. Rang drei geht an die Identitätsprüfung (36%), gefolgt vom Bonitätscheck (33%) und Hotlists, also eigenen Datenbanken mit kritischen Adressen (30%). Relativ weit verbreitet ist überdies mit 25% der Einsatz einer Betrugsvermeidungssoftware. Hinsichtlich gewisser Schutzmaßnahmen zeigen sich jedoch markante Unterschiede zwischen Unternehmen mit weniger bzw. mit mehr als zehn Mitarbeiter:innen. Während etwa bei den größeren Betrieben 58% auf eine Identitäts- und 55% auf eine Bonitätsprüfung zur Risikominimierung setzen, sind es bei den KMU-Webshops nur 16% respektive 12%. Stolze 42% der größeren Onlinehändler verwenden eine „Hotlist" – auch dieses Schutzinstrument kommt bei kleineren Unternehmen mit 19% weit seltener zum Einsatz. Immerhin zeigt sich im Verlauf der letzten drei Jahre eine verstärkte Nutzung von konkreten Schutzmaßnahmen auch bei den heimischen KMU-Betrieben.

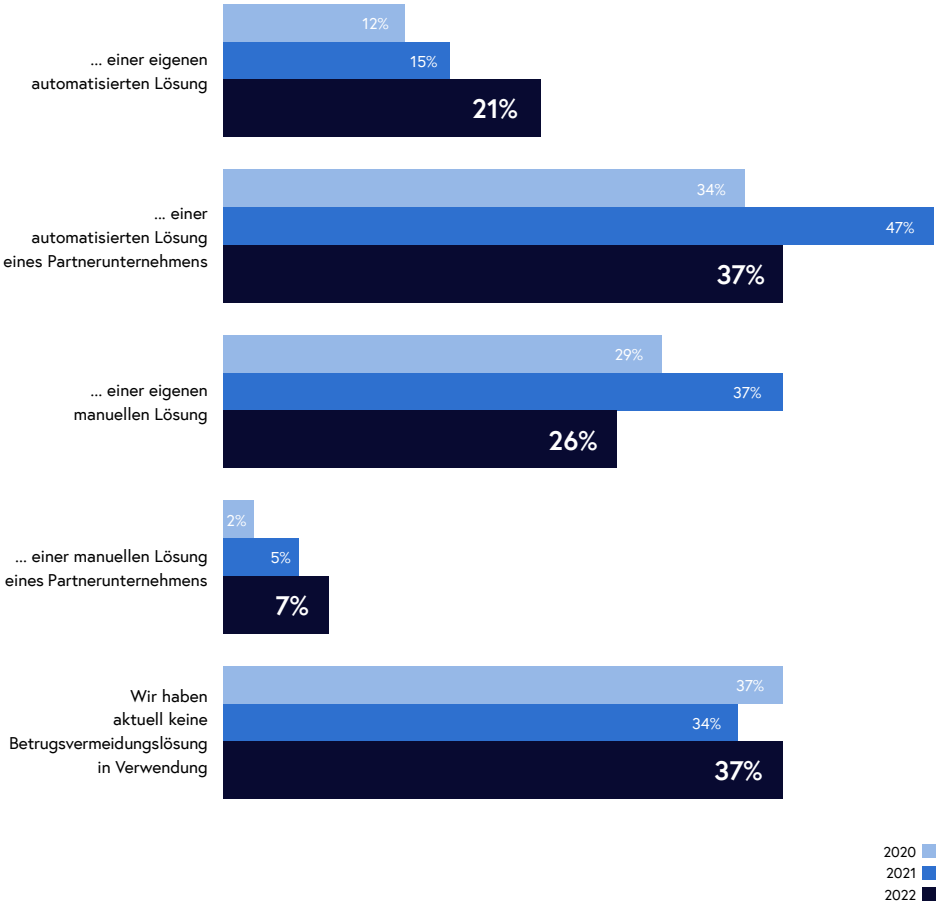
Haben Sie konkrete Maßnahmen zum Schutz vor Onlinebetrug in Verwendung?



Wir vermeiden Betrug im Unternehmen mit...

Bei der Frage, mit welchen Methoden sich Unternehmen gegen Betrug schützen, ergeben sich eklatante Unterschiede zwischen kleineren und größeren Betrieben. 55% der Unternehmen mit mehr als zehn Beschäftigten setzen auf automatisierte Lösungen von Partnerunternehmen, während das nur bei 21% der kleineren Handelsbetriebe der Fall ist.

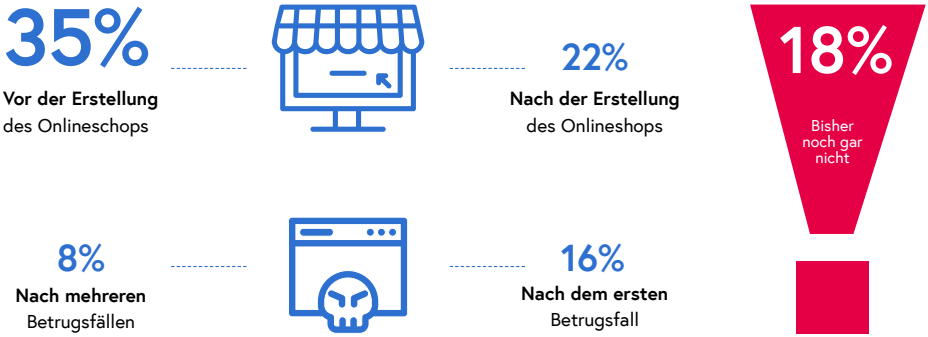
Fast die Hälfte der Betriebe mit unter 10 Mitarbeiter:innen (49%) gab außerdem an, derzeit überhaupt keine Lösung zur Betrugsvermeidung anzuwenden – bei den größeren Unternehmen sind es aktuell 25%. Spannend: 2021 lag dieser Wert noch bei 52% für KMU bzw. 14% für größere Händler.



Wann erfolgte die Einführung von Maßnahmen zur Betrugsvermeidung?

Über potentielle Schutzmaßnahmen für ihren Onlineshop haben sich 35% der Umfrageteilnehmer:innen bereits vor dessen Launch informiert. 22% kümmerten sich nach Erstellung des Shops darum, und wiederum 16% erst nach dem ersten Betrugsfall.

Immerhin 18% aller befragten Unternehmen haben sich bis dato noch gar nicht über Schutzmaßnahmen gegen Onlinebetrug informiert – bei den Unternehmen mit weniger als zehn Beschäftigten sind es sogar 26%. Die Bedeutung der Eindeutigkeit von Kundendaten, also die „Echtheit" der Kund:innen, wird im ständig wachsenden eCommerce immer größer. Bereits 52% der Befragten ist eine verlässliche Authentifizierung/Identifizierung ihrer Kund:innen im Online-Geschäft sehr wichtig.



Bedeutung der Echtheit von Kundendaten

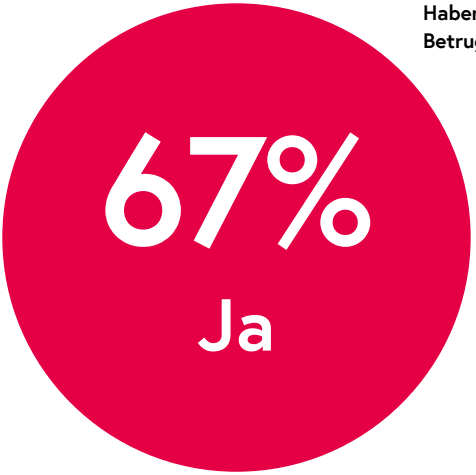
Zusammenarbeit mit der Polizei

Hinsichtlich zukünftiger Betrugsfälle im Zusammenhang mit ihrem Webshop gab die Mehrheit der befragten Unternehmen (67%) an, solche bei der Polizei zur Anzeige bringen zu wollen. 2021 lag dieser Wert mit 76% übrigens noch deutlich höher. 20% hingegen erwarten sich durch die Anzeigeerstattung kein Ergebnis und 5% haben eine Anzeige bislang gar nicht in Erwägung gezogen.

Als entscheidendste Faktoren für eine Anzeige nennen Unternehmer die damit verbundene Servicequalität: 89% erwarten sich, eine Anzeige jederzeit erstatten zu können, 68% möchten mit einem Besuch alles erledigt wissen. 58% erklären sich auch bereits mit einer Anzeigebestätigung zufrieden. Nach erfolgter Anzeigeerstattung wünschen sich 70% der Befragten von der Polizei laufende Updates zu den Ermittlungsergebnissen, 76% erklären sich bereit, selbstständig neue oder etwaige bei der Anzeigeerstattung vergessene Informationen nachzuliefern. 84% möchten ihre Artikel nach Sicherstellung durch die Polizei umgehend wieder erhalten.

ERWARTUNGSHALTUNG WÄHREND DER ANZEIGEERSTATTUNG	Trifft voll zu	Trifft eher zu
Eine Anzeigeerstattung muss jederzeit möglich sein.	****	
Wenn kein/e Fachspezialist:in der Polizei verfügbar ist, lasse ich mir einen Termin geben bis eine/r verfügbar ist.		***
Es muss alles auf einmal erledigt sein, ein weiteres Mal komme ich nicht.	****	
Eine Anzeigebestätigung genügt mir bereits.		***
Eine Beratung zur Verhinderung weiterer Betrugsfälle hat im Zuge der Anzeigeerstattung durch die Polizei stattzufinden.		**
ERWARTUNGSHALTUNG NACH DER ANZEIGEERSTATTUNG		
Ich erwarte mir ständige Updates zu den Ermittlungen der Polizei.		***
Ich liefere selbständig neue oder vergessene Informationen nach.	***	
Werden meine Artikel von der Polizei sichergestellt, so erhebe ich umgehend Anspruch auf Rückgabe.	****	

Haben Sie, bzw. würden Sie zukünftig Ihre Betrugsfälle bei der Polizei anzeigen?



Nein, Zeit/Geld wiegt Anzeige nicht auf

Nein, es kommt sowieso nichts raus

Nein, das habe ich gar nicht in Erwägung gezogen

Nein, wegen Image/Reputations-schaden

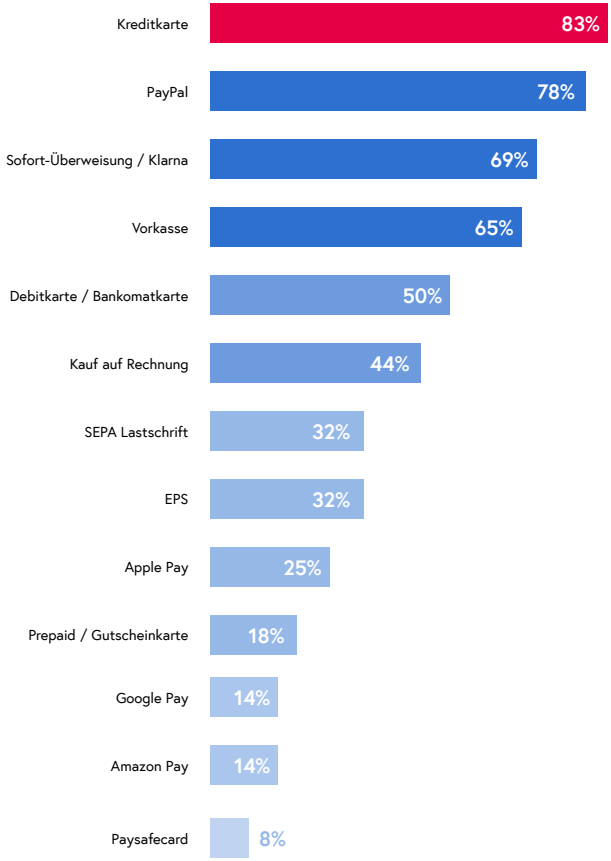
Sonstiges

Payment & Kunden-identifizierung

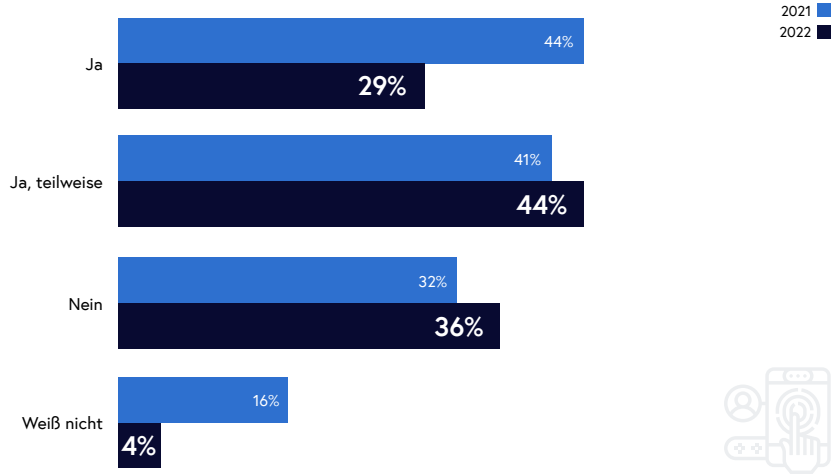
Zahlungsoptionen im Webshop

Mehr als acht von zehn Händlern bieten in ihrem Webshop die Zahlung per Kreditkarte – bei den großen Onlinehändlern sind es sogar mehr als 92%. Im Gesamtranking der gängigsten Zahlungsmethoden liegt die Kreditkarte damit erneut auf Platz eins vor PayPal (78%), und der Sofort-Überweisung/Klarna (69%), die von 2021 auf 2022 deutlich zulegen konnte. Rang 4 belegt die Bezahlung per Vorkasse (65%), gefolgt von der Debitkarte. Letztere konnte ihre Popularität innerhalb eines Jahres mehr als verdoppeln.

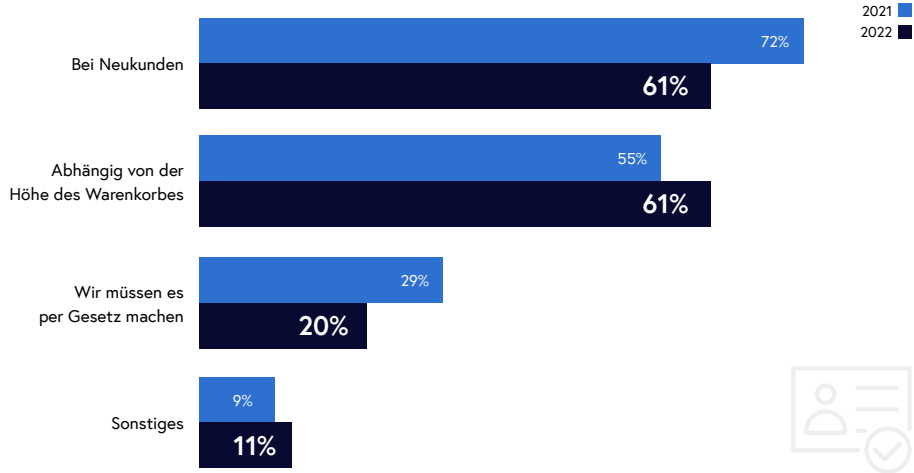
Zahlungsmethoden individueller Anbieter sind den Studienergebnissen zufolge – vor allem bei den kleineren Unternehmen mit bis zu zehn Beschäftigten – noch nicht sehr weit verbreitet. Immerhin gaben 41% der befragten KMU-Händler an, den Kauf auf Rechnung als Zahlungsmethode zu akzeptieren. Jeder achte KMU-Webshop bietet auch Amazon Pay als Zahlungsmethode an. Insgesamt betrachtet zählen auch die Mobile Payment-Optionen Apple Pay (25%) und Google Pay (14%) zu den Gewinnern des letzten Jahres.



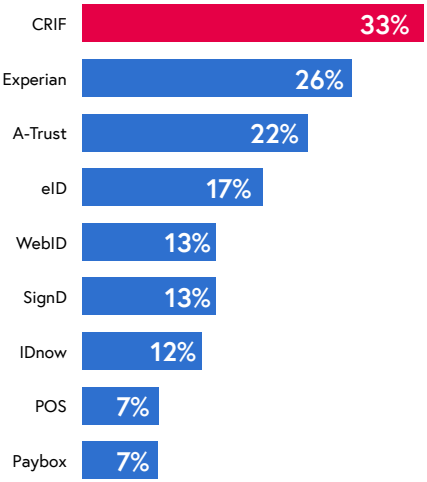
Überprüfen Sie die Identität Ihrer Online-Shopper?



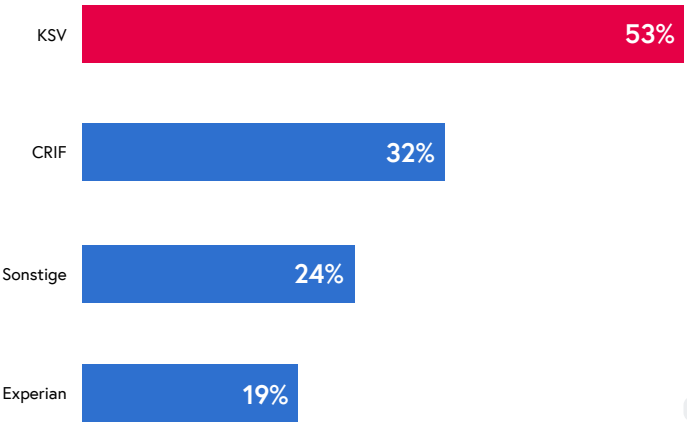
Wann ist es für Sie wichtig, die Identität zu überprüfen?



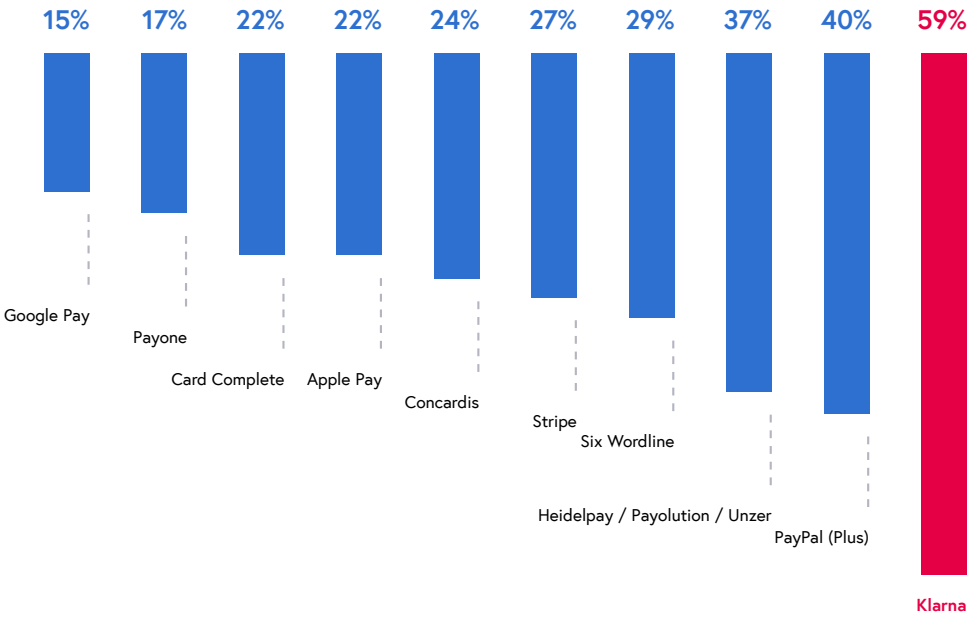
Mit welchen Dienstleistern arbeiten Sie bei der Identitätsprüfung zusammen?



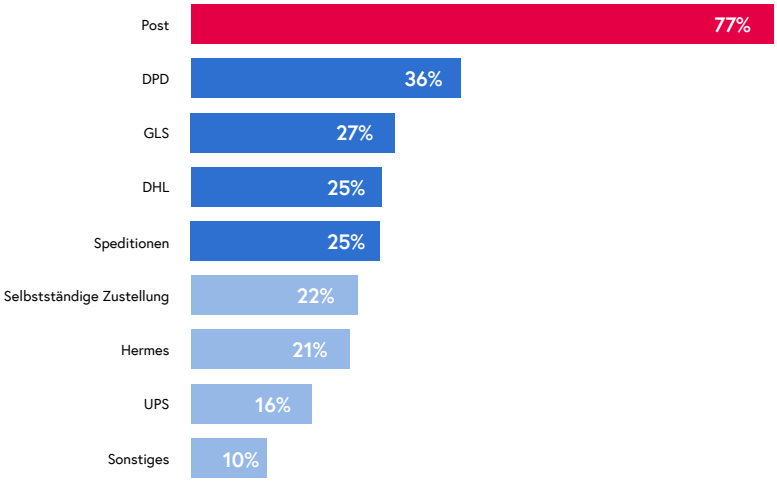
Mit welchen Dienstleistern arbeiten Sie bei der Bonitätsprüfung zusammen?



Mit welchen Zahlungsdienstleistern arbeiten Sie zusammen?



Mit welchen Logistik- / KEP- /Fulfillmentpartnern arbeiten Sie zusammen?



Gütesiegel

Nutzung von eCommerce-Gütesiegeln

Gütesiegel stehen im eCommerce für seriöse und vertrauenswürdige Anbieter. Im Zuge der Umfrage wurden die teilnehmenden Unternehmen auch danach befragt, welche der gängigsten eCommerce-Gütesiegel und Zertifikate sie kennen und nutzen.

Am bekanntesten ist dabei das **Trusted-Shops-Gütesiegel**, das 80% aller Befragten kennen und 35% auch selbst für ihr Unternehmen nutzen. 20% der Umfrageteilnehmer:innen gaben hingegen an, Trusted Shops weder zu kennen noch zu nutzen. Unter den befragten großen Onlinehändlern hat Trusted Shops einen Bekanntheitsgrad von rund 87% und wird von mehr als 57% selbst genutzt. Von den befragten Unternehmen mit weniger als zehn Mitarbeiter:innen kennen 74% das Trusted-Shops-Gütesiegel, 17% nutzen es auch in ihrem Unternehmen. 26% gaben an, das Gütesiegel gar nicht zu kennen und in ihrem Betrieb auch nicht zu nutzen. In Sachen Bekanntheitsgrad an zweiter Stelle steht das **Österreichische eCommerce-Gütezeichen**, das 66% aller befragten Unternehmen ein Begriff ist und das 25% auch für ihren Onlineshop nutzen. 34% der Umfrageteilnehmer:innen gaben an, das Österreichische eCommerce-Gütezeichen weder zu kennen noch zu nutzen.

Das vom Handelsverband verliehene **Trustmark-Austria-Gütesiegel** hat unter den Onlinehändlern einen Bekanntheitsgrad von 61% und belegt damit den dritten Rang im Gesamtranking. 25% verwenden das Siegel für ihren Shop, 39% kennen und nutzen Trustmark Austria nicht. Das **eCommerce-Europe-Trustmark-Siegel** ist fast der Hälfte der Befragten ein Begriff – genutzt wird es derzeit von rund 15%.

Österreichische Gütesiegel für Webshops				
nutze ich	25%	15%	25%	35%
kenne ich	36%	29%	41%	45%
kenne und nutze ich nicht	39%	56%	34%	20%

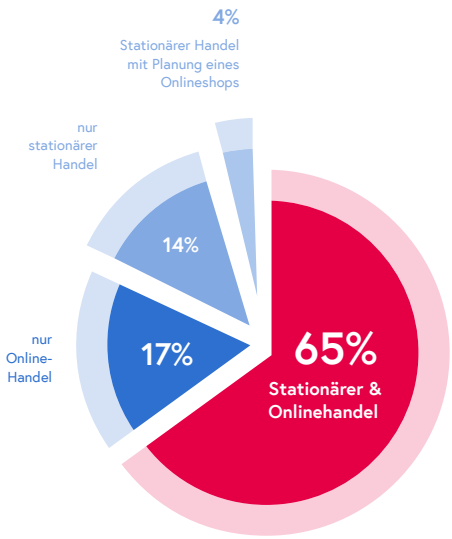
TIPP:

Mit dem gemeinsamen Gütesiegel „Ecommerce Europe Trustmark" setzen der Handelsverband und Ecommerce Europe ein Zeichen für sicheres Onlineshopping in Europa. Das Trustmark Austria sowie auch das Ecommerce Europe Trustmark stehen für ein sicheres Einkaufserlebnis auf höchstem Niveau und stellen – aufgrund der breiten Wiedererkennung des Zeichens im europäischen Raum – die Basis für grenzüberschreitende Kaufentscheidungen dar. Aufgrund der strengen nationalen Kriterien sind alle Trustmark Austria-Träger – bei Erfüllung aller Voraussetzungen – automatisch auch mit dem europäischen Gütesiegel zertifiziert und können das Ecommerce Europe Trustmark gemeinsam mit dem Trustmark Austria auf ihrem Webshop ausweisen.

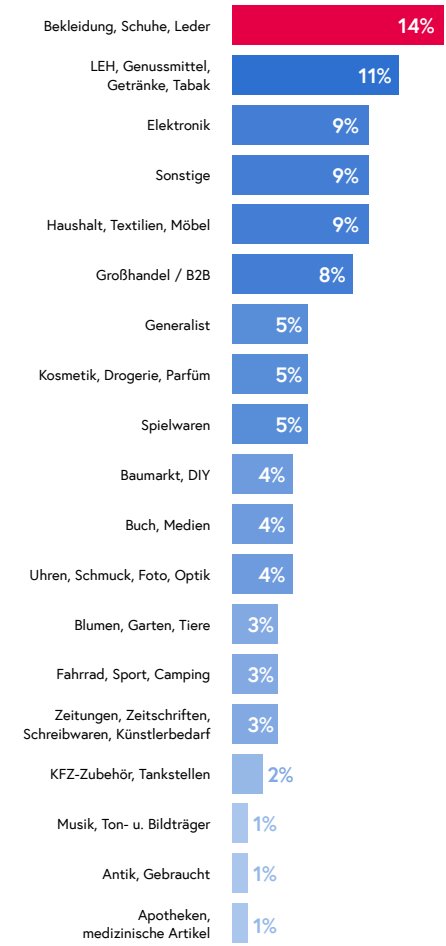
Über die Studie

Die Sicherheitsstudie 2023 wurde vom österreichischen Handelsverband in Kooperation mit dem Bundesministerium für Inneres (BMI), dem Bundeskriminalamt und der Initiative „Gemeinsam.Sicher“ durchgeführt. 150 Unternehmen aller Handelsbranchen und Größenordnungen (vom EPU bis zum Konzern) haben teilgenommen und den Fragebogen vollständig und fristgerecht ausgefüllt. Der Erhebungszeitraum betrug acht Wochen, Studienende war der 31. März 2023.

Zusammensetzung der Stichprobe

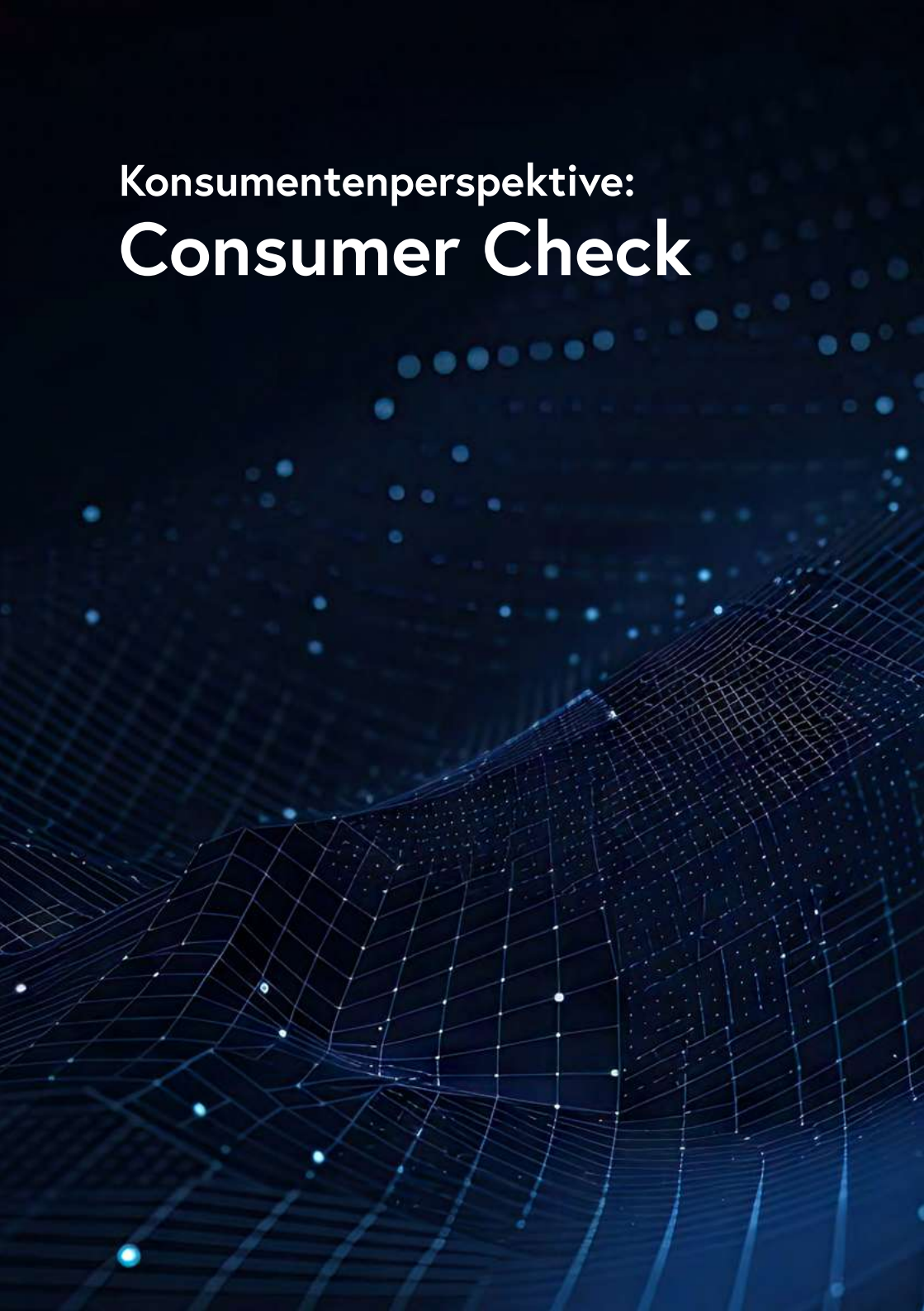


Branchenüberblick der Befragten



Konsumentenperspektive:

Consumer Check

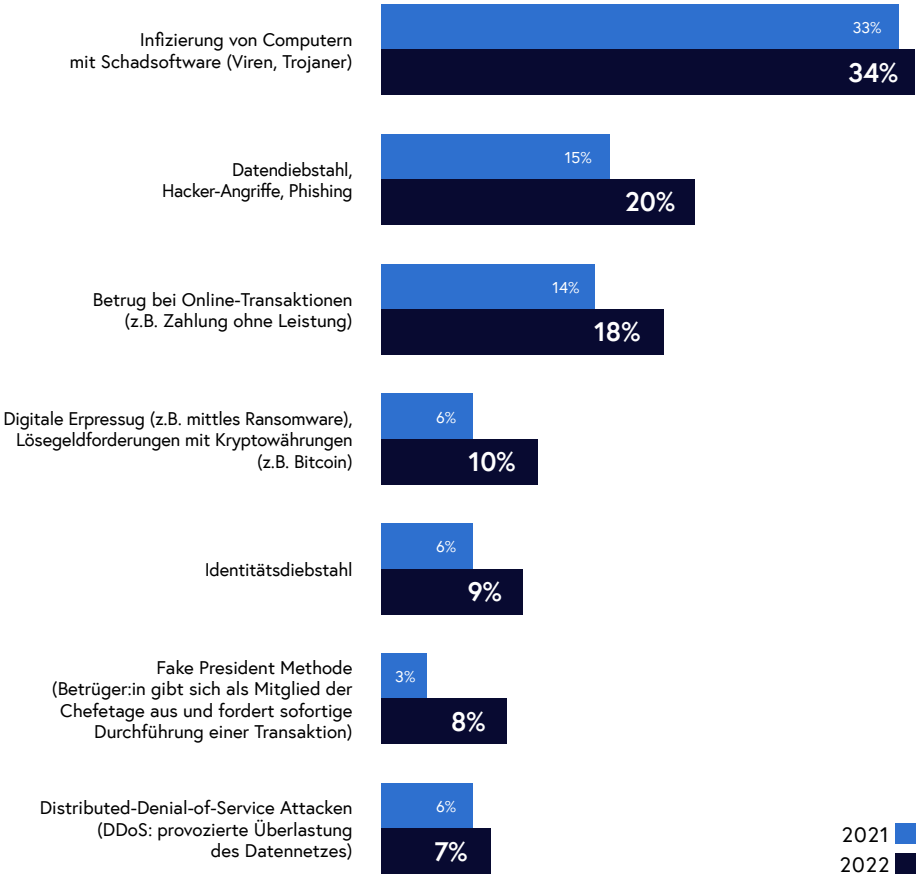


Formen von Cyberkriminalität

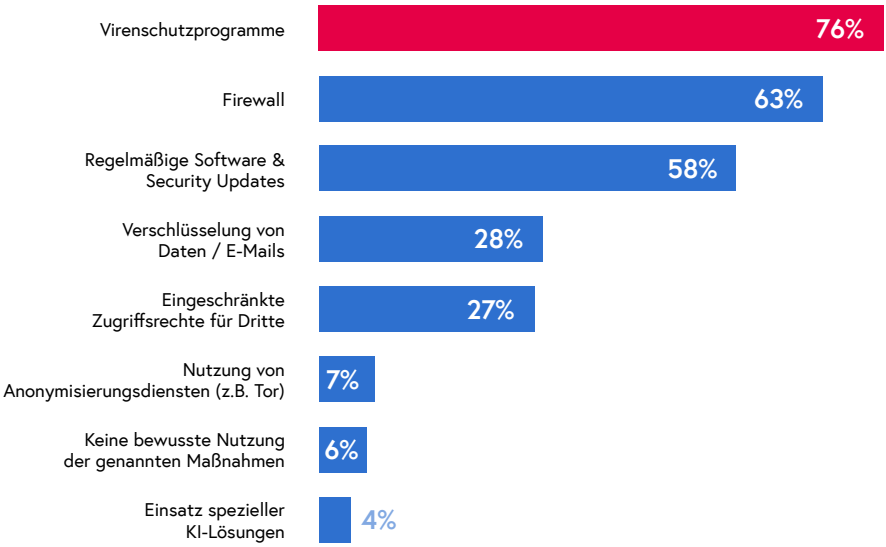
Neben der Unternehmensseite wurde für die SICHERHEITSSTUDIE 2023 auch die Konsumentenperspektive beleuchtet. In Kooperation mit Mindtake Research wurden hierfür 1.026 österreichische Verbraucher:innen zu ihren Erfahrungen mit Cyberkriminalität befragt. Das Ergebnis: Ein Drittel der Konsument:innen hat bereits negative Erfahrungen mit Schadsoftware wie Viren oder Trojanern gemacht.

20% waren schon von Datendiebstahl durch Phishing-Angriffe betroffen, weitere 18% waren Opfer von Betrug bei Online-Transaktionen. Ebenfalls in den Top-5: Digitale Erpressung (10%) und Identitätsdiebstahl (9%). Alarmierend ist, dass die Betroffenheit bei allen Formen von Cyberkriminalität von 2021 auf 2022 teils deutlich angestiegen ist.

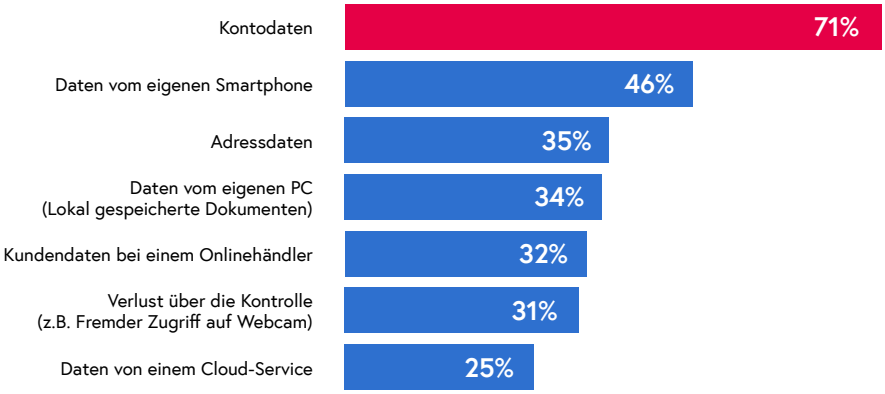
Mit welchen Formen von Cyberkriminalität haben Sie schon Erfahrungen gemacht?



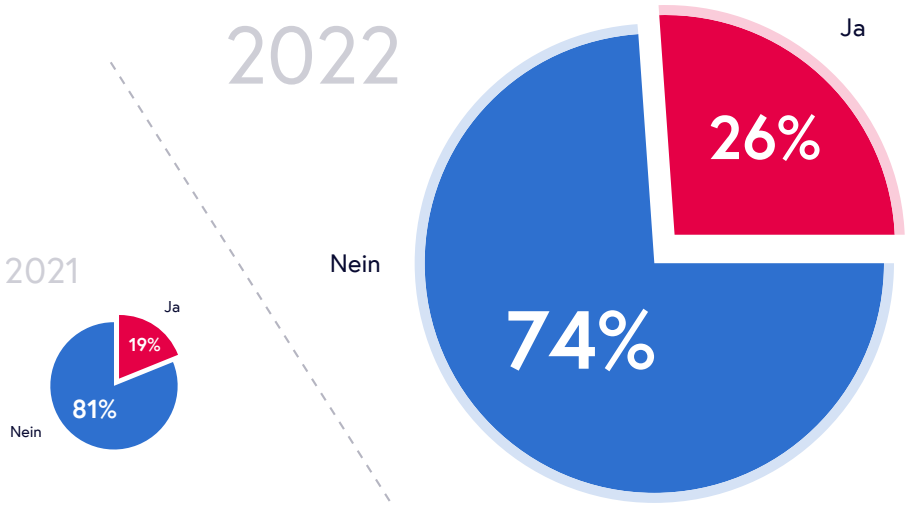
Wie schützen Sie sich vor Cyberangriffen?



Bei welchen Daten haben Sie am meisten Angst davor, Opfer von Cyberkriminalität zu werden?



Waren Sie schon mal Opfer eines Fake-Webshops?

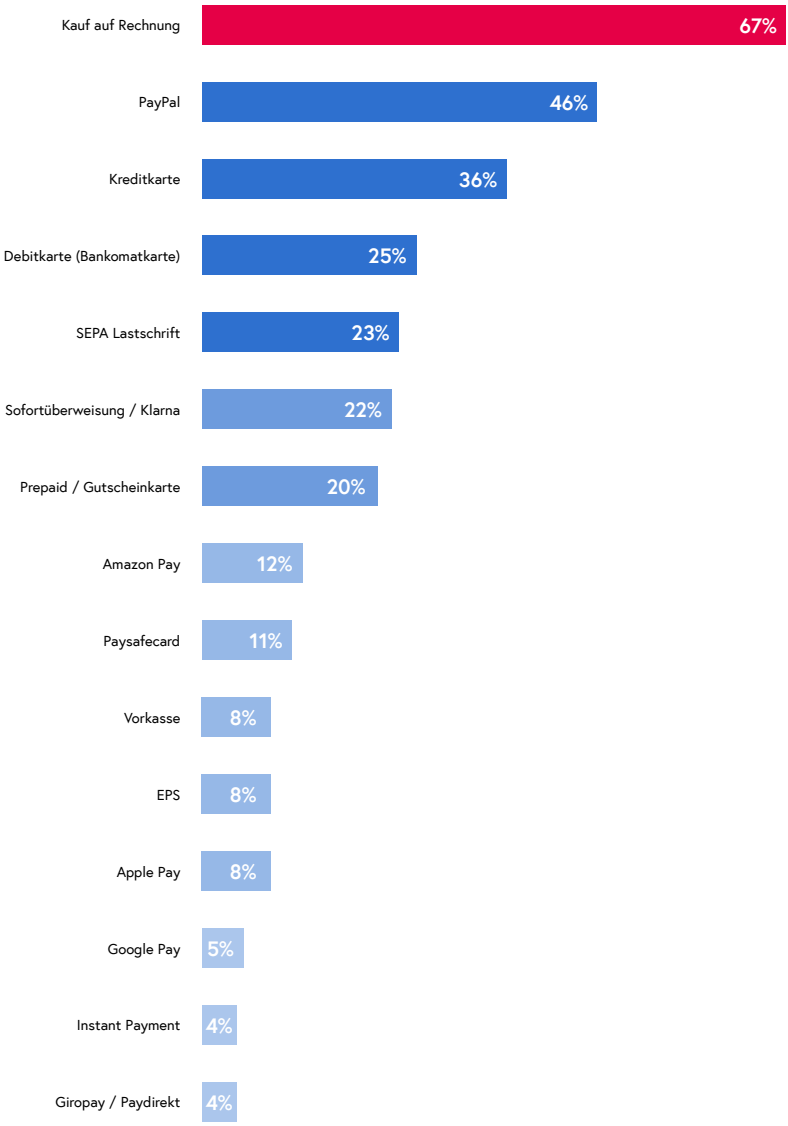


Drei von vier Konsument:innen schätzen die Gefahren von Cyberkriminalität als hoch ein, besonders bei sensiblen Kontodaten (71%) und Daten auf dem eigenen Smartphone (46%) ist die Angst vor einem Angriff weit verbreitet. Drei Viertel der Österreicher:innen versuchen, sich mit Virenschutzprogrammen zu schützen. 63% setzen auf eine Firewall, 58% schützen sich mit regelmäßigen Software- und Security-Updates. Auch die Verschlüsselung von Daten und E-Mails (28%) sowie die Einschränkung von Zugriffsrechten durch Dritte (27%) sind weit verbreitet. Anonymisierungsdienste wie Tor werden hingegen lediglich von 7% der Bevölkerung verwendet.

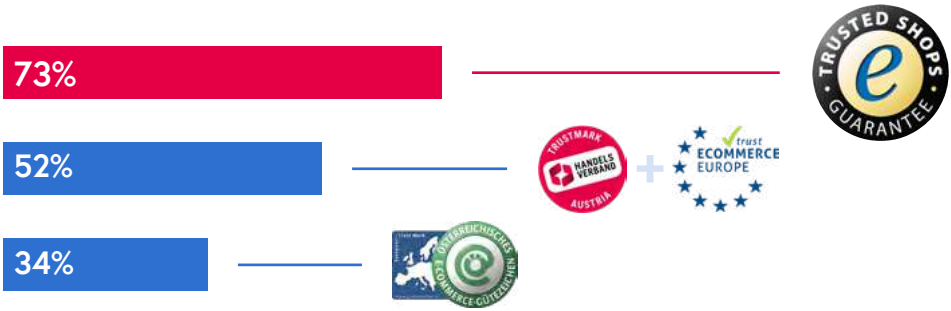
Das Wissen über die verschiedensten Formen von Cyberkriminalität scheint in Österreich sowohl auf Händler-, als auch auf Konsumentenseite stark ausgeprägt zu sein. Einigkeit herrscht auch bei der Frage nach den möglichen Risiken der Digitalisierung: Jeweils mehr als 90% glauben, dass durch die zunehmende Digitalisierung und Vernetzung via Internet die Risiken für Cyberkriminalität künftig noch steigen werden.

Was das Vertrauen in die Sicherheit bei der Verwendung von Onlineshops betrifft, sind Herr und Frau Österreicher durchaus zufrieden. Rund 80% bewerten die Datensicherheit beim Onlineshopping als hoch, mehr als 90% empfinden österreichische Onlineshops im Allgemeinen als sicher und mehr als die Hälfte vertraut heimischen Onlineshops mehr als internationalen Anbietern. Aber: 26% der heimischen Konsument:innen waren bereits Opfer von Fake-Webshops. 2020 lag diese Zahl noch bei unter 20%.

Welche Zahlungsarten sind Ihrer Meinung nach am sichersten?



Sind Ihnen die folgenden Gütesiegel bekannt?



Vertrauen ist gut, Transparenz und Kontrolle noch besser

In punkto bevorzugte Zahlungsmöglichkeiten bei Onlineeinkäufen haben Bezahlsysteme wie Paypal (46%), Kreditkarte (36%), Debitkarte (25%), die SEPA Lastschrift (23%) sowie die Sofortüberweisung (Klarna) aus Gründen der Sicherheit und Einfachheit die Nase vorne. Unangefochten an der Spitze der populärsten Payment-Methoden aus Kundensicht liegt jedoch weiterhin der Kauf auf Rechnung mit stolzen 67%.

Auch das Thema „eCommerce-Gütesiegel" ist mittlerweile im Mainstream angekommen. Ähnlich wie auf Händlerseite belegen auch in der Gunst der Kund:innen das „Trusted Shops"-Siegel (73%), das „Trustmark Austria" des Handelsverbandes sowie das „Ecommerce Europe Trustmark" (gemeinsam 52%) und das „Österreichische E-Commerce-Gütesiegel" (34%) die Spitzenplätze des Beliebtheitsrankings 2023. Fazit: Vertrauen ist gut, Transparenz und Kontrolle sind noch besser.

Kontaktdaten

HANDELSVERBAND – Verband österreichischer Handelsunternehmen
Austrian Retail Association
Alser Str. 45
1080 Wien
+43 1 406 22 36
office@handelsverband.at
www.handelsverband.at

BUNDESKRIMINALAMT
Josef-Holaubek-Platz 1
1090 Wien
+43 1 24836 9850 25
bundeskriminalamt@bmi.gv.at
www.bundeskriminalamt.at