SICHERHEITS STUDIE 2021

BETRUG IM ONLINEHANDEL

HANDELS VERBAND | 100+1 JAHRE

Bundesministerium Inneres
Bundeskriminalamt

TRUSTMARK AUSTRIA

Einfach sicher shoppen.

- **VERTRAUENSWÜRDIGES DIGITAL SHOPPING**
- **ORIENTIERUNGSHILFE FÜR VERBRAUCHER:INNEN**
- **TRANSPARENZ UND SICHERHEIT IM ECOMMERCE**
- **OMBUDSSTELLE ZUR VERMITTLUNG**

WWW.TRUSTMARK-AUSTRIA.AT

EXECUTIVE SUMMARY

Bereits in den Vorjahren haben Untersuchungen gezeigt: Unternehmen, die einen Webshop betreiben, sind zunehmend von Betrugsfällen betroffen. Unter den für diese Studie befragten Onlinehändler:innen wurden bereits **62% Opfer von Betrug**, 24% sogar schon mehrmals. Von den Betrieben mit mehr als 10 Beschäftigten gaben drei Viertel (78%) an, in Verbindung mit ihrem Webshop bereits mit Online-Betrug in Berührung gekommen zu sein, bei den kleineren Betrieben waren es 48%. Im Vergleich zu 2020 (46%) hat die Betrugshäufigkeit in allen Größenklassen deutlich zugenommen.

Zu den gängigsten Betrugsformen zählen der Retourenbetrug (48%), Bestellungen, die nicht bezahlt werden können (50%), die Angabe verfälschter Namens- oder Adressdaten (55%) und insbesondere das **Abstreiten des Erhalts der Ware (63%).**

Bei den kleineren Handelsbetrieben beläuft sich die durch Online-Betrug verursachte Schadenssumme in den meisten Fällen (48%) bis 500 Euro, in 44% zwischen 500 und 10.000 Euro. Unternehmen mit mehr als zehn Beschäftigten erlitten im Schnitt wesentlich höhere Verluste: 36% der entstandenen Schäden machten zwischen 5.000 und 10.000 Euro aus, bei 22% beliefen sich die finanziellen Einbußen auf 10.000 bis zu einer Million Euro. Um das Betrugsrisiko zu reduzieren, kombinieren Webshops meist verschiedenste Schutzmaßnahmen – und verzichten dafür auch auf potentielle Mehrumsätze. So setzen 55% der Befragten auf sichere Zahlungsmethoden und 29% auf eingeschränkte Lieferoptionen wie ausschließliche Inlandslieferungen.

Als gängigste Zahlungsmethode erweist sich die Kreditkarte, mit der in 88% der Webshops bezahlt werden kann, dicht gefolgt von PayPal (85%) und Vorkasse (64%). Die Hälfte 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. 30% der Unternehmen nutzen derzeit auch keine spezielle Lösung zur Betrugsvermeidung, etwa keine Identitätsprüfung. In Sachen Anzeigeerstattung bei Online-Betrug bestätigten 76% der Händler, zukünftige Betrugsfälle bei der Polizei anzeigen zu wollen.

Das Hauptaugenmerk liegt dabei auf der Servicequalität: 79% wünschen sich, eine Anzeige jederzeit erstatten zu können, 76% möchten mit einem Besuch alles erledigt wissen.

Auch eCommerce-Gütesiegel wurden im Zuge der Umfrage thematisiert. **Am bekanntesten** unter den Befragten ist das **Trusted-Shops-Gütesiegel mit 80%**, gefolgt vom Österreichischen eCommerce-Gütezeichen (72%) und den Siegeln Trustmark Austria sowie Ecommerce Europe Trustmark mit einem Bekanntheitsgrad von 57% bzw. 49%.

Neben der Unternehmensseite wurde für die SICHERHEITSSTUDIE 2021 auch die **Konsumentenperspektive** beleuchtet. Das Ergebnis: Ein Drittel der heimischen Verbraucher:innen hat bereits negative Erfahrungen mit Schadsoftware wie Viren oder Trojanern gemacht. 15% waren schon von Datendiebstahl durch Phishing-Angriffe betroffen, weitere 14% waren Opfer von Betrug bei Online-Transaktionen.

78% der Österreicher:innen versuchen, sich mit Virenschutz-Programmen vor Cyberangriffen zu schützen. 68% setzen auf regelmäßige Software Updates und immerhin 63% haben eine Firewall implementiert. Beunruhigend ist, dass bereits **fast ein Fünftel aller Konsument:innen (19%) Opfer von Fake-Webshops** geworden sind.

INHALT

VORWORT

Sehr geehrte Damen und Herren!

Die Digitalisierung öffnet uns weltweit zwar viele Türen, doch leider mit einem bitteren Beigeschmack. Denn egal ob es sich um Schadsoftware, Datendiebstahl oder digitale Erpressung handelt, die Möglichkeiten von Cyber-Kriminellen sind gerade in diesem Bereich zahlreich und kreativ.

Allein 2021 sind Cybercrime-Delikte im Vergleich zu 2020 um 26 Prozent angestiegen. Ein Grund dafür ist gewiss die COVID-19-Pandemie, die Auswirkungen auf unterschiedlichste Bereiche unseres Zusammenlebens hat. Auffallend ist, dass sich Kriminalität von traditionellen Formen hin zu neuen Phänomenen wendet.

Zahlreiche Studien zeigen seit 2019 unter anderem einen starken Anstieg der Opfer von Online-Betrug, auf der Seite der Käufer:innen und der Händler:innen. Dem gilt es entgegenzuwirken, insbesondere dadurch, dass der Bereich des Kampfes gegen Cybercrime stärker forciert wird. Wichtig ist hierbei die Präventionsarbeit, um einerseits potenziellen Schaden zu vermeiden, aber auch um ein Zeichen für die Steigerung der Sicherheit zu setzen.

Als Innenminister liegt mir die Sicherheit der Menschen in Österreich am Herzen. Besonders in einer Zeit, in der Cybercrime-Delikte zunehmen, soll gesagt sein: Auch die Kriminalität im Internet ist eine Straftat, die nicht hingenommen wird.

Studien wie diese ermöglichen es, Maßnahmen zu setzen, um „Modi Operandi“ entgegenzuwirken. Hierbei möchte ich mich beim Handelsverband und dem Bundeskriminalamt für die Umsetzung dieser wichtigen Studie zu einer sicheren Zukunft bedanken.

In diesem Sinne wünsche ich Ihnen interessante Erkenntnisse aus der vorliegenden Studie.

Bleiben Sie gesund!
Ihr Gerhard Karner

GERHARD KARNER
Bundesminister für Inneres

Bundesministerium
Inneres

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. eCommerce boomt, im Corona-Jahr 2021 wächst der Online-Handel in Österreich um mehr als 20 Prozent. Mit steigendem Umsatz wächst aber auch das Risiko für Betrug.

Jeder zweite heimische Handelsbetrieb war bereits Opfer von Kriminalität im Netz. 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. Für Online-Shopper zählt Sicherheit mittlerweile zu den wichtigsten Kaufkriterien.

Doch die Abwehr von Datendiebstahl, Identitätsmissbrauch und Bestellbetrug stellt Webshops und Marktplätze vor immer größere Herausforderungen. Vor allem KMU-Händler:innen zählen zu den beliebtesten Zielen von Hackern und Betrüger:innen, da viele davon ausgehen, kleine Webshops seien nicht ausreichend geschützt. Auch die EU hat auf die Gefahr von Online-Betrug reagiert und in ihrer Zahlungsdienste-Richtlinie (PSD2) die sogenannte 2-Faktor-Authentifizierung (2FA) vorgeschrieben.

Diese besagt, dass sich Kund:innen bei Bezahlung über das Internet zumindest doppelt identifizieren müssen – etwa mittels Passwort und SMS TAN. Seit 14. März 2021 können Online-Zahlungen nur noch mit Starker Kundenauthentifizierung (Strong Customer Authentification, kurz SCA) durchgeführt werden. Das sorgt für mehr Sicherheit im europäischen Zahlungsverkehr.

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. Worauf es besonders ankommt, erfahren Sie im vorliegenden Whitepaper.

RAINER WILL
Geschäftsführer Handelsverband

Board of Directors
Ecommerce Europe

MANUEL SCHERSCHER
Leiter der Initiative „GEMEINSAM.SICHER“ und stellvertr. Direktor des Bundeskriminalamts

PUBLIC PRIVATE PARTNERSHIP

Der Schlüssel zu mehr Sicherheit im Onlinehandel

Bundesministerium Inneres
Bundeskriminalamt

GEMEINSAM.SICHER im Online-Handel

Das Internet und die damit einhergehende Digitalisierung hat unser Leben in vielen Bereichen verändert, so auch unser Einkaufsverhalten. Neben dem klassischen stationären Handel erfreuen sich Onlineshops immer größerer Beliebtheit. Der Ausbruch der Corona Pandemie hat diese Entwicklung zusätzlich verstärkt, insbesondere während der Zeit, in der die Geschäfte geschlossen halten mussten. Das ist auch Kriminellen nicht entgangen. Sie nutzen die „vermeintlichen Schwachstellen“ im Bestellprozess für ihre Machenschaften. Die missbräuchliche Verwendung real existierender Identitäten beim „Kauf auf Rechnung“ stellt den Großteil der angezeigten Delikte im Jahr 2021 dar. Gekonnt werden von den Kriminellen auch Webshops nachgebildet. Diese „Fakeshops“ werden dazu benützt, Kund:innen zu täuschen und Bestellungen durchzuführen. Die bezahlten Waren werden jedoch nicht geliefert. Die Polizei registriert ständig neue Vorgehensweisen der Kriminellen, daher wird neben der Verfolgung der Täter:innen auch vermehrt auf Präventionsmaßnahmen gesetzt. Bestellbetrug ist längst ein internationales Phänomen, weshalb das Bundeskriminalamt auch an mehreren Projekten von Europol aktiv teilnimmt, um aktuelle Trends sofort zu registrieren und daraus nationale Strategien abzuleiten. Die Initiative „GEMEINSAM.SICHER in Österreich“ bietet eine Plattform zum Austausch zwischen Polizei, Händler:innen und Kund:innen.

Eine 100%ige Sicherheit kann Ihnen leider niemand garantieren. Wenden Sie sich jedoch an Unternehmen mit Erfahrung im Onlinehandel und tauschen Sie sich über die Möglichkeiten der Risikominimierung aus. Setzen Sie beim Online-Shopping auf ein gesundes Misstrauen, besonders bei sehr günstigen Angeboten. Auch Kund:innen können Kontrolle ausüben: Auf

vielen Shopping-, Preisvergleich- und Auktionsseiten werden Handelsbetriebe beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein.

Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter. Im Schadensfall ist die Erstattung einer Anzeige in jeder Polizeiinspektion möglich.
Herzlichen Dank an den Handelsverband für die partnerschaftliche Zusammenarbeit. Die Kooperation zwischen Polizei und Privatsektor stellt ein wesentliches Element dar, die Sicherheit im Onlinehandel zu verbessern.

GASTKOMMENTARE

PATRICIA GRUBMILLER
Head of Legal
Handelsverband

VERTRAUEN SPIELT EINE WESENTLICHE ROLLE

Um sich von unseriösen Angeboten abzugrenzen, sollten mehrere vertrauensbildende Maßnahmen gesetzt werden.

HANDELS VERBAND

Transparenz, Sicherheit, der Einsatz von Kundenbewertungen und Gütesiegeln stellen bei Webshops die wichtigsten Säulen dar, um sich von unseriösen Angeboten abzugrenzen.

Befeuert durch die Coronakrise setzen nun auch vermehrt kleine Handelsbetriebe auf einen eigenen digitalen Kanal. Insbesondere jene Webshops, die noch vergleichsweise unbekannt sind, müssen ihre Kund:innen umso intensiver davon überzeugen, dass sie in einem seriösen Onlineshop gelandet sind. Der erste Eindruck ist natürlich immer der wichtigste. Dabei spielen ein ansprechendes Design, gute Usability, eine übersichtliche Struktur und hochwertige Produktbilder eine wichtige Rolle. Vertrauen kann am einfachsten mithilfe unabhängiger Dritter aufgebaut werden. Dafür eigenen sich einerseits Kundenbewertungen und andererseits Gütesiegel, wie auch die vorliegende Sicherheitsstudie belegt. Kundenbewertungen im Internet sind zu vergleichen mit der klassischen Mund-zu-Mund Propaganda. Wenn bereits viele andere in einem Onlineshop gekauft haben und eine positive Bewertung hinterlassen haben, steigt das Vertrauen. Nichts ist aussagekräftiger als Empfehlungen von anderen Käufer:innen.

Gütesiegel, etwa das Trustmark Austria des Handelsverbandes, bieten eine gute Orientierungshilfe, um auf einen Blick zu erkennen, ob es sich um einen vertrauenswürdigen Webshop handelt. Die Kund:innen sollten durch einen Klick auf das angezeigte Gütesiegel auf die Webseite des Siegel-Betreibers weitergeleitet werden. Auf dieser sind in der Regel alle zertifizierten Shops aufgelistet. So kann rasch überprüft werden, ob der Onlineshop das Gütesiegel befugterweise auf der Website platziert hat.

So machen wir das Shoppen GEMEINSAM SICHER IM ONLINEHANDEL.

THOMAS VON DER GATHEN
General Counsel
PSA – Payment Services Austria GmbH

IDENTITÄTSMISSBRAUCH IST MEIST DIE URSACHE FÜR BETRUG

Kaum je zuvor war der Online-Handel bei Konsument:innen so gefragt wie im vergangenen Jahr.

PSA

Dieser Trend wird weiter anhalten. Komfortable und sichere Zahlungsmittel spielen dabei eine große Rolle. Die vorliegende Studie des Ressorts „Sicherheit im Handel“ des Handelsverbands belegt wieder ganz klar: Zahlungen mit den neuen Bankomat®Karten (Debitkarten) und mit Kreditkarten stehen ganz oben auf der Liste der Zahlungsmittel im Online-Geschäft.

Die Anzahl der eCommerce-Transaktionen mit Bankomat®Karten hat sich 2021 im Vergleich zu 2020 mit 44 Mio. mehr als verdoppelt, ebenso zeigt das Transaktionsvolumen mit Debitkarten im eCommerce eine Verdopplung auf € 1,8 Mrd. Kein Wunder: Sie garantieren Händler:innen ihren Umsatz und gehören für die Kund:innen großteils schon zum Alltag.

41% der befragten Händler:innen bieten ihren Kund:innen auch schon eps-Überweisungen an, ein sicheres Online-Bezahlsystem für Konsument:innen und Webshop-Betreiber. Dabei werden Kund:innen direkt in ihr gewohntes Online-Banking-System geleitet, wo ihre Bankdaten schon vorausgefüllt zur Verfügung stehen. Für Handelsbetriebe bringt eps viele Vorteile wie Realtime Zahlungsbestätigung, einfache Umsetzung und kein zusätzlicher Soft- oder Hardwareaufwand.

Immer wichtiger wird es für Online-Händler:innen auch, ihre Kund:innen zu kennen. 90% der Befragten geben in der aktuellen Studie an, dass ihnen eine verlässliche Authentifizierung/Identifizierung ihrer Kund:innen sehr wichtig oder wichtig ist. 72% geben an, dass dies vor allem bei Neukund:innen wichtig für sie ist.

PSA bringt dafür im Jahr 2022 mit der ich.app eine vielseitige Lösung auf den Markt. Sie ermöglicht es Unternehmen und Menschen auf einfache und zugleich sichere Art, sich online eindeutig zu identifizieren, digitale Services anzubieten und Geschäfte abzuschließen. Die Händler:innen erhalten mit der ich.app die gewünschten Kundeninformationen genauso bestätigt, wie sie bei der Bank hinterlegt sind. Damit können sie sicher sein, dass der Kunde „echt“ ist. Darüber hinaus bieten sie ihren Kund:innen eine besserer Convenience, weil diese sich die Eingabe von Daten ersparen. Ein weiterer Nutzen ist der Rückgang von Passwort-Recovery-Prozessen, also das notwendige Zurücksetzen und Neudefinieren eines Passwortes, auf Grund von falscher Eingabe. Das kostet auch die Händler:innen Zeit und Geld und manchmal auch den Umsatz. Und ein wichtiges Plus: Mit der ich.app ist eine Integration in Online-Shops einfach umsetzbar. Gerade Banken-basierte eID Modelle haben sich als besonders erfolgreich herausgestellt, wie es etwa in Schweden und Norwegen zu beobachten ist.

Neben dem Angebot hochsicherer Technologien unterstützen wir von PSA auch mit Knowhow und langjähriger Expertise die Initiative GEMEINSAM SICHER IM ONLINE-HANDEL aus voller Überzeugung. Dabei helfen uns die langjährige gute Zusammenarbeit und der Erfahrungsaustausch zwischen Polizei, Finanzdienstleistern, Handel und Logistikunternehmen und PSA. Gemeinsam arbeiten wir alle an der Minimierung von Betrugsrisiken und unterstützen den Handel gerne dabei mit allen Initiativ-Partnern in den Austausch über erfolgreiche Betrugs-Prävention zu kommen.

WOLFGANG GRAUSENBURGER
Leitung Marketing & Innovation
Österreichische Post AG

WEIL SICHERHEIT WIRKLICH WICHTIG IST

Die Post bietet mehr im eCommerce. Das haben wir uns in vielen Belangen vorgenommen – und auch umgesetzt.

Seien es die flexiblen Services auf der letzten Meile für Privatkund:innen wie z.B. die Paketumleitung, seien es die Initiativen im Bereich der Nachhaltigkeit (Stichwort emissionsfreie Zustellung bis 2030) oder unsere Anstrengungen im Business-Bereich.

Ihren Geschäftskund:innen bietet die Österreichische Post neben hoher Qualität auch ein Mehr gegen Bestellbetrüger:innen. Schon seit einigen Jahren beteiligt sich die Post aktiv an der Bekämpfung von Betrug im Onlinehandel. Zum Beispiel als Teilnehmerin der sogenannten Action Days, einer von Europol initiierten Aktionswoche gegen Bestellbetrug in Zusammenarbeit mit dem Bundeskriminalamt und diversen Versandhändlern. Unsere Erfahrung, den Austausch mit Versandhändler:innen sowie die Kooperation mit der Polizei nutzen wir im Rahmen der Möglichkeiten und können so unsere Geschäftspartner:innen bei der Vermeidung von Schäden unterstützen. Auch haben wir beispielsweise mit Services wie dem Sendungsstopp die Möglichkeit geschaffen, ein Paket mitten im Zustellprozess noch zurückzuhalten und so Betrug zu verhindern. Denn im eCommerce ist der Faktor Zeit entscheidend, sodass Fraud-Checks bei dem/der Verkäufer:in oft erst anschlagen, wenn das Paket schon unterwegs zu dem/der Empfänger:in ist.

Wir tun tagtäglich unser Bestes, als Logistikpartnerin Pakete schnell, bequem und sicher zuzustellen und unsere Kund:innen in ihrem Geschäft ideal zu unterstützen.

GERALD S. EDER
Sales Director Digital Solutions, eCommerce
CRIF Austria

DIE RECHNUNG BITTE

Erfolgreiche Handelsbetriebe wissen: Wer online shoppt, schätzt die unbegrenzte Auswahl – auch bei Zahlungsoptionen. Kauf auf Rechnung steigert dabei die Conversion.

Die Angst vor Betrug ist mit den richtigen Sicherheitsmaßnahmen unbegründet. Bereits mehr als 60% der österreichischen Onlinehändler:innen haben Erfahrung mit Betrug gemacht. Sich davor zu schützen, indem man nur sichere Zahlungsmethoden anbietet, ist eine beliebte Schutzmaßnahme, die von 55% der Befragten vorgenommen wird. Ein Lösungsansatz, der jedoch auf Kosten der Usability und Conversion geht – und der nächste Onlineshop ist nur einen Klick entfernt.

Für 77% der befragten Konsument:innen ist Kauf auf Rechnung die sicherste Zahlungsart und sie lieben es, auf Rechnung einzukaufen. Für den Händler ein großes Risiko, jedoch hinsichtlich der Conversion muss er es anbieten, da er damit seinen Umsatz um bis zu 40% steigern kann.

Es gilt hier ausschließlich abgesichert vorzugehen. Mit einer Bonitätsprüfung ist das Risiko eines Zahlungsausfalles kontrollierbar und die Conversion gesichert. Über 60% der befragten Onlinehändler:innen setzen in der Betrugsvermeidung bereits auf automatisierte Lösungen. Denn Betrüger:innen sind meist organisiert und bestens technologisch ausgerüstet. Den Betrug zu erkennen und zu verhindern, funktioniert nur mit datenbasierter Technologie. Diese erkennt in Echtzeit, vernetzt automatisiert Anomalien und Verdachtsmomente. Dieser Prozess läuft im Hintergrund ab und die Kund:innen bekommen davon im Einkaufsprozess nichts mit. Schlägt bei der Überprüfung ein Risiko an, so kann eingestellt werden, dass im Kaufprozess zusätzliche Sicherheitsvorkehrungen automatisiert vorgenommen werden: z.B. eine Identifizierung zu verlangen.

Die automatisierte Betrugsvermeidung bietet maximalen Schutz für Handelsbetriebe und maximales Einkaufsvergnügen für alle Kund:innen.

GOTTFRIED TONWEBER
Leitung Cybersecurity & Data Privacy
EY Österreich

„IN ALLEN DINGEN HÄNGT DER ERFOLG VON DEN VORBEREITUNGEN AB.“

Dieses Zitat des chinesischen Philosophen Konfuzius gilt fast immer. Auch dann, wenn Handelsunternehmen überlegen, die Präsenz im Internet auf- und auszubauen.

Die Pandemie hat enorme Auswirkungen – gerade auf den stationären Handel. Viele Unternehmen, die noch über kein digitalisiertes Angebot verfügen, sehen sich zunehmend gezwungen, ihre Kund:innen auch über das Internet zu erreichen und ihnen die Möglichkeit zur Interaktion und zum Warenkauf zu bieten. Hand in Hand mit den Möglichkeiten, die dem Händler digitale Plattformen bieten, kommen auch die Risiken. Internet-Kriminalität zielt besonders auf Unternehmen ab, und jeder erfolgreiche Angriff bedeutet Schaden – in Geldwert, in der Reputation, in der Fähigkeit zur Geschäftsfortführung.

Dieses Problem erkennen auch Unternehmen der Handels- und Konsumgüterbranche in Österreich: Rund zwei Drittel der Unternehmen nehmen laut EY-Datendiebstahlstudie an, dass die Gefahr durch Cyberangriffe steigen wird — auch wenn nur ein verschwindend geringer Teil der Unternehmen einen Zuwachs von Cyberangriffen seit Ausbruch der Pandemie im März 2020 feststellen konnte. Zwei Drittel der Betriebe hatten im Lockdown Mitarbeiter:innen im Homeoffice – häufig ohne genügend Vorbereitungszeit. So steigt natürlich auch das Risiko, Ziel eines Angriffs zu werden.

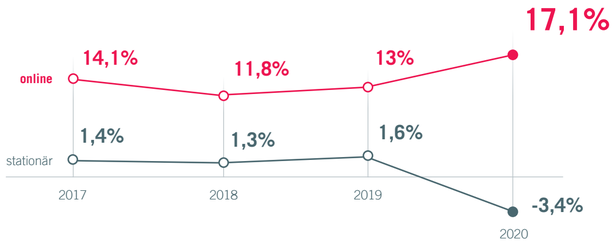
Sicherheit im digitalen Zeitalter gelingt nur dann, wenn Menschen nach effizienten und sicheren Prozessen arbeiten und Vorgaben umsetzen. Bewusstseinsbildung ist das beste Gegenmittel gegen jede Form von Schädigung durch illegale Aktivitäten über digitale Plattformen. Aufmerksame und vor allem regelmäßig geschulte Mitarbeitende bilden eine breite Abwehrlinie gegen Betrugsversuche, Ransomware und Phishing. Jede noch so leistungsfähige technische Sicherheitsmaßnahme verliert ihre Kraft, wenn die Belegschaft nicht ausreichend sensibilisiert ist.

Mit guter Planung, abgestimmten Prozessen und aktueller Technik zur Schaffung von Cybersecurity ist Ihre Transformation in Sachen Digitalisierung kein experimentelles Abenteuer mehr. Wir stehen bereit, Sie und Ihr Unternehmen sicher zu machen. Vollumfänglich, mit dem Know-how eines internationalen Beraters und lokaler Expertise.

BETRUG IM ONLINEHANDEL

EINKAUFEN IM WORLD WIDE WEB IST ALLTAG GEWORDEN. ONLINE BETRUG EBENFALLS.

ECOMMERCE-WACHSTUM DER LETZTEN 5 JAHRE



Während der Corona-Krise hat der Onlinehandel einen noch stärkeren Boom erfahren. Unabhängig von der Unternehmensgröße ist Fakt: Wer seine Produkte zusätzlich übers Internet anbietet, eröffnet sich neue, von Öffnungszeiten unabhängige Absatzwege.

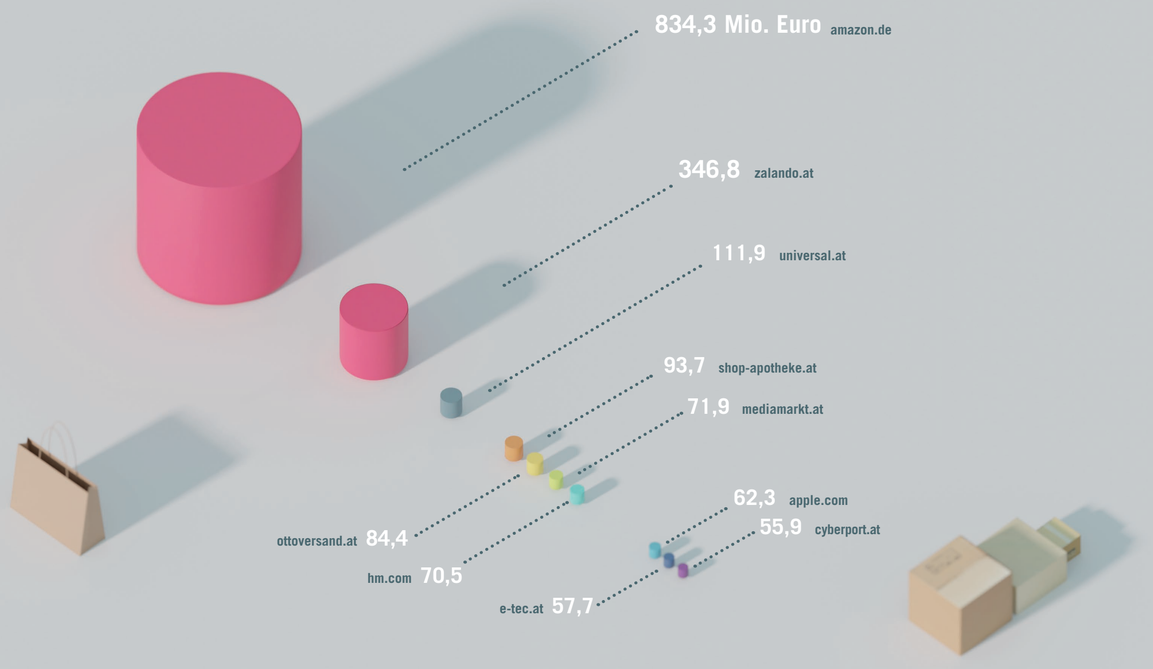
Wie immer hat allerdings auch die eCommerce-Medaille eine Kehrseite: **Je mehr Webshops, desto mehr damit verbundene Betrugsfälle.** Gerade in Krisenzeiten steigen Cyberkriminalität und Online-Betrug massiv an.

Um das Ausmaß der Online-Betrugsfälle in Österreich zu erfassen, hat der Handelsverband eine Umfrage unter 143 Webshop-Betreiber:innen durchgeführt. Das Ergebnis: **62% aller österreichischen Händler wurden 2021 Opfer von Online-Betrug,** bei den größeren Unternehmen sogar 78%. 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. Die gute Nachricht: Effektive Betrugsprävention ist nicht unmöglich. So, wie man sein Geschäftslokal mit Schlössern und Überwachungskameras absichert, kann man das auch bei seinem Onlineshop tun – sei es durch verschiedenste Technologien, die bei verdächtigen Verhaltensmustern Alarm schlagen, Betrüger:innen im sprichwörtlichen Sinn die Tür vor der Nase zusperren oder durch sichere Zahlungsmethoden bzw. eingeschränkte Lieferoptionen, die das Betrugsrisiko von vornherein reduzieren.

Natürlich kostet diese Art von Sicherheit Geld – aber unbestritten ist auch: **Weniger Sicherheit kostet im Endeffekt mehr Geld**. Ein durchdachter Mix aus verschiedensten Schutzmaßnahmen schont infolge nicht nur die Unternehmensbilanz, sondern auch die Nerven.

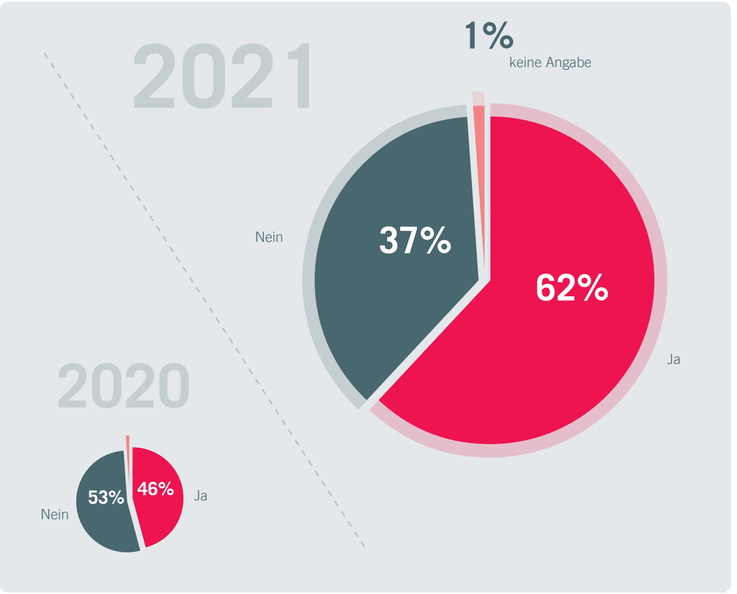
DIE 10 UMSATZSTÄRKSTEN ONLINESHOPS IN ÖSTERREICH (UMSATZ 2019)



Haben Sie in Ihrer Tätigkeit als Onlinehändler:in **schon Erfahrungen mit Betrug gemacht?**

Die aktuelle Studie rund um Sicherheit im Onlinehandel belegt: Bereits 62% der befragten Onlinehändler:innen haben in irgendeiner Form Erfahrungen mit Betrug gemacht – 24% davon sogar mehrmals. 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 mehr als drei Viertel (78%) an, in Verbindung mit ihrem Webshop bereits mit Online-Betrug in Berührung gekommen zu sein, bei den kleineren Betrieben waren es 48%.



Mit welchen Betrugsformen haben Sie schon Erfahrungen gemacht?

Die Arten von Betrug, mit denen Onlinehändler:innen 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 falsche Namens- oder Adressdaten angeben (55%). In 50% der Fälle ist dem Besteller bzw. der Bestellerin schon beim Bestellvorgang bewusst, dass er/sie die Rechnung nicht begleichen können wird.

Mit 45% Betroffenheit aller Befragten bildet die Angabe einer falschen Identität die vierthäufigste Betrugsform. Absoluter Spitzenreiter ist in dieser Statistik aber mit 63% das das Abstreiten des Erhalts der Ware durch die Kundschaft – obwohl er/sie diese erhalten hat. Auffällig sind die Unterschiede bei mit Lieferung und Retouren verbundenem Betrug zwischen Unternehmen mit weniger bzw. mehr als zehn Beschäftigten. Im Vergleich zu 25% bei den kleineren Händlern haben bereits 64% der größeren Unternehmen Erfahrungen mit Betrugsfällen bei Retouren gemacht.

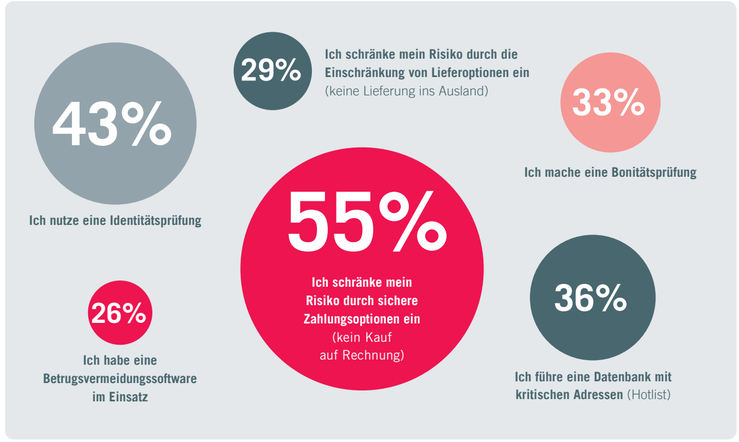
Wie hoch war Ihre durch Online-Betrug verursachte **Schadenssumme im Jahr 2020?**

Bezogen auf die Gesamtstatistik zeigt sich, dass die Schadenssumme der Betrugsfälle im Onlinehandel 2019 noch mehrheitlich (55%) unter 500 Euro lag. In 20% der Fälle betrug die Schadenssumme bis 5.000 Euro, in 13% bis zu 10.000 Euro und in 10% bis zu 100.000 Euro. 2020 hat sich das Schadensausmaß signifikant erhöht: Nur noch ein Fünftel der Schadenssummen lag unter 500 Euro, in 30% 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 13% angewachsen.

Die Studie macht auch deutlich, dass größere Unternehmen durch Online-Betrug im letzten Jahr wesentlich höhere wirtschaftliche Einbußen erlitten. In den meisten Fällen (36%) belief sich die Schadenssumme bei Betrieben mit mehr als zehn Beschäftigten auf Beträge zwischen 5.000 und 10.000 Euro.

Haben Sie konkrete Maßnahmen zum Schutz vor Onlinebetrug in Verwendung?

RISIKOMINIMIERUNG

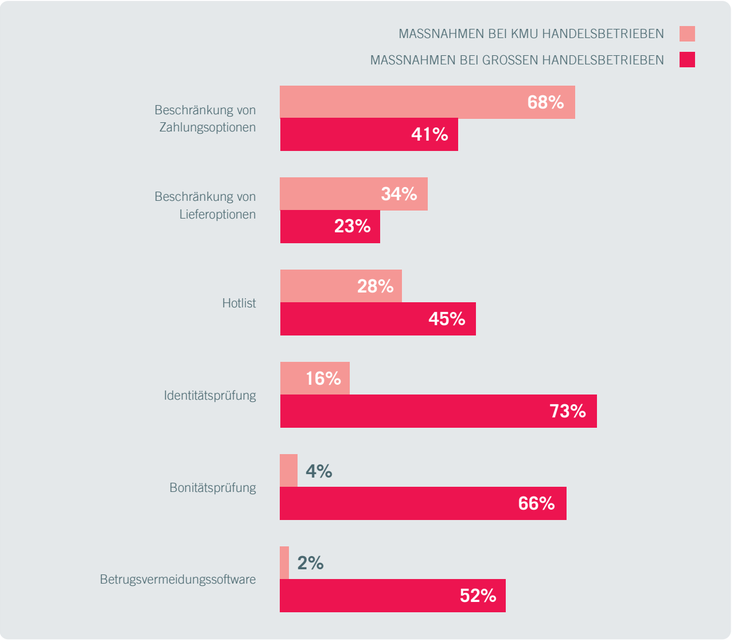


Bei der Frage, wie sich Onlinehändler:innen gegen Betrug schützen, zeigt sich deutlich: Für die meisten wiegt Sicherheit höher als die Chance auf höheren Profit. Um das Betrugsrisiko zu senken, verzichten viele Unternehmen auf potentielle Mehrumsätze bzw. Absatzwege. So setzen 55% der Befragten auf sichere Zahlungsoptionen (kein Kauf auf Rechnung etc.). Auf Platz zwei rangiert die Identitätsprüfung (43%), gefolgt von eigenen Datenbanken mit kritischen Adressen (36%) auf Platz drei. Weit verbreitet sind überdies mit 27% eingeschränkte Lieferoptionen – die Handelsbetriebe liefern zum Beispiel nur innerhalb des eigenen Landes. Hinsichtlich gewisser Schutzmaßnahmen zeigen sich jedoch markante Unterschiede zwischen Unternehmen mit weniger bzw. mit mehr als zehn Mitarbeiter:innen.

Laut Gesamtstatistik nutzen 33% der Betriebe eine Identitäts- bzw. Bonitätsprüfung zur Risikominimierung in ihrem Webshop. Während es jedoch bei den größeren Betrieben 66% sind, wenden bei den kleineren Firmen nur 4% diese Prüfung an. Stolze 45% der größeren Onlinehändler:innen verwenden eine “Hotlist” (eine Datenbank mit kritischen Adressen) – auch dieses Schutzinstrument kommt bei kleineren Unternehmen mit 28% weit seltener zum Einsatz.

Haben Sie konkrete Maßnahmen zum Schutz vor Onlinebetrug in Verwendung?

RISIKOMINIMIERUNG

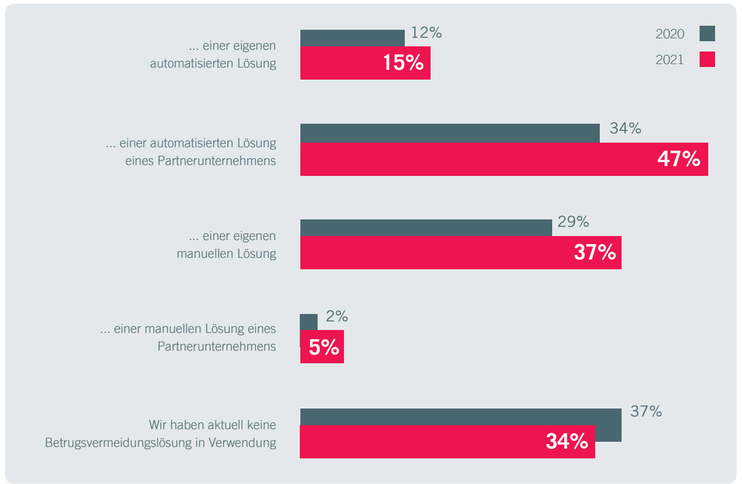


Wir vermeiden Betrug im Unternehmen mit …

BETRUGSVERMEIDUNG

Bei der Frage, mit welchen Methoden sich Unternehmen gegen Betrug schützen, ergeben sich eklatante Unterschiede zwischen kleineren und größeren Betrieben. 73% der Unternehmen mit mehr als zehn Beschäftigten setzen auf automatisierte Lösungen von Partnerunternehmen, während das nur bei 24% der kleineren Handelsbetriebe der Fall ist.

Mehr als die Hälfte der Betriebe mit unter 10 Mitarbeiter:innen (52%) gab außerdem an, derzeit überhaupt keine Lösung zur Betrugsvermeidung anzuwenden – bei den größeren Unternehmen sind es aktuell 14%.

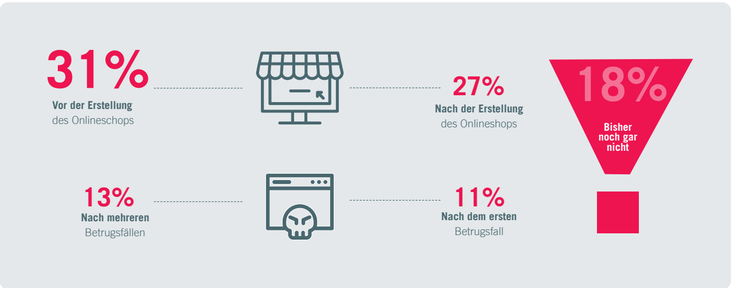


Wann erfolgte die Einführung von Maßnahmen zur Betrugsvermeidung?

ZEITPUNKT DER MASSNAHMEN

Über potentielle Schutzmaßnahmen für ihren Onlineshop haben sich 31% der Umfrageteilnehmer:innen bereits vor dessen Launch informiert. 27% kümmerten sich nach Erstellung des Shops darum, und wiederum 11% 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 24%. Spannend: Die Bedeutung der Eindeutigkeit von Kundendaten, also die „Echtheit" der Kund:innen, wird im ständig wachsenden eCommerce immer größer. Bereits 5% der Befragten ist eine verlässliche Authentifizierung/Identifizierung ihrer Kund:innen im Online-Geschäft sehr wichtig.



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

ANZEIGENERSTATTUNG

Hinsichtlich zukünftiger Betrugsfälle im Zusammenhang mit ihrem Webshop gab die Mehrheit der befragten Unternehmen (76%) an, solche bei der Polizei zur Anzeige bringen zu wollen. 16% hingegen erwarten sich durch die Anzeigeerstattung kein Ergebnis und 7% haben eine Anzeige bislang gar nicht in Erwägung gezogen.

Als entscheidendste Faktoren für eine Anzeige nennen Unternehmer die damit verbundene Servicequalität: 79% erwarten sich, eine Anzeige jederzeit erstatten zu können, 76% möchten mit einem Besuch alles erledigt wissen. 63% erklären sich auch bereits mit einer Anzeigebestätigung zufrieden. Nach erfolgter Anzeigeerstattung wünschen sich 49% der Befragten von der Polizei laufende Updates zu den Ermittlungsergebnissen, 65% 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.

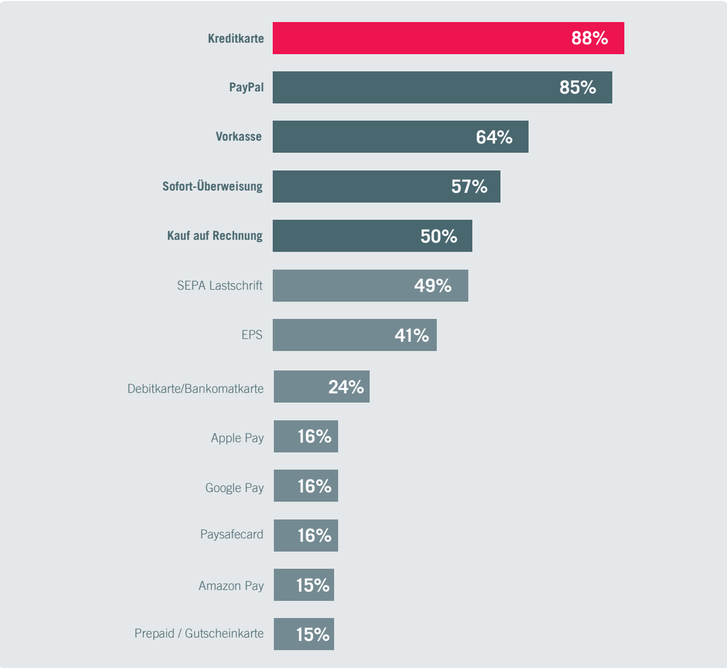
ERWARTUNGSHALTUNG WÄHREND DER ANZEIGEERSTATTUNG	Trifft voll zu	Trifft eher zu
Eine Anzeigeerstattung muss jederzeit möglich sein.	****	
Wenn kein/e Fachspezialist:in der Polizei verfügbar ist, lasse ich mir einen Termin geben bis eine/r verfügbar ist		***
Es muss alles auf einmal erledigt sein, ein weiteres 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	****	

ZAHLUNGSMETHODEN

Welche Zahlungsmethoden bieten Sie in Ihrem Webshop an?

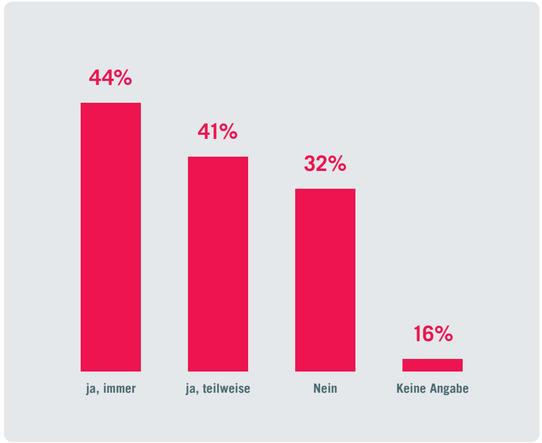
Fast neun von zehn Händler:innen bieten in ihrem Webshop die Zahlung per Kreditkarte – bei den großen Onlinehändlern sind es sogar mehr als 97%. Im Gesamtranking der gängigsten Zahlungsmethoden liegt die Kreditkarte damit auf Platz eins vor PayPal (85%), der Bezahlung per Vorkasse (64%) und der Sofort-Überweisung (57%).

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 34% der befragten KMU-Händler an, den Kauf auf Rechnung als Zahlungsmethode zu akzeptieren. Jeder zehnte KMU-Webshop bietet auch Amazon Pay als Zahlungsmethode an.

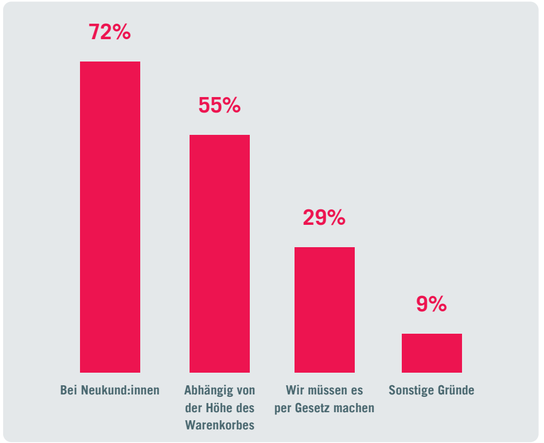


KUNDENIDENTIFIZIERUNG

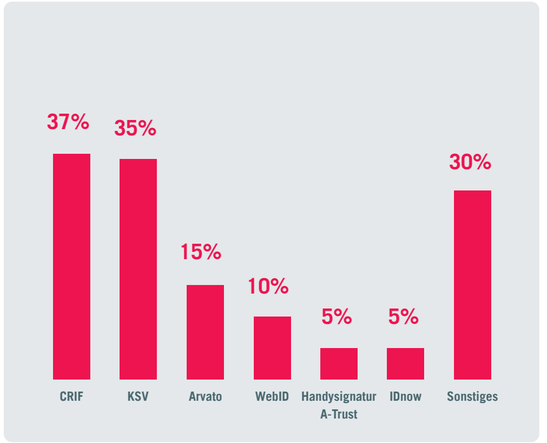
Überprüfen Sie die **Identität Ihrer Online-Shopper?**



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



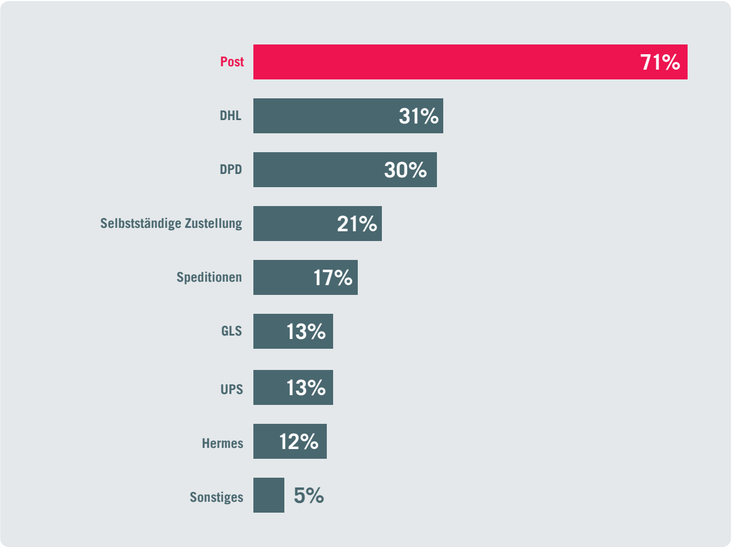
Mit welchen Dienstleistern **arbeiten Sie bei der Identitätsprüfung zusammen?**



Mit welchen Dienstleistern **arbeiten Sie bei der Bonitätsprüfung zusammen?**

LOGISTIKPARTNER

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



GÜTESIEGEL

Kennen Sie bzw. nutzt Ihr Unternehmen **ein eCommerce-Gütesiegel?**

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 war dabei das **Trusted-Shops-Gütesiegel**, das 80% aller Befragten kennen und rund 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 98% und wird von mehr als 63% selbst genutzt. Von den befragten Unternehmen mit weniger als zehn Mitarbeiter:innen kennen 64% das Trusted-Shops-Gütesiegel, 11% nutzen es auch in ihrem Unternehmen.

#36% 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 71% aller befragten Unternehmen ein Begriff ist und das mehr als 27% auch für ihren Onlineshop nutzen. 28% der Umfrageteilnehmer:innen gaben an, das Österreichische eCommerce-Gütezeichen weder zu kennen noch zu nutzen.

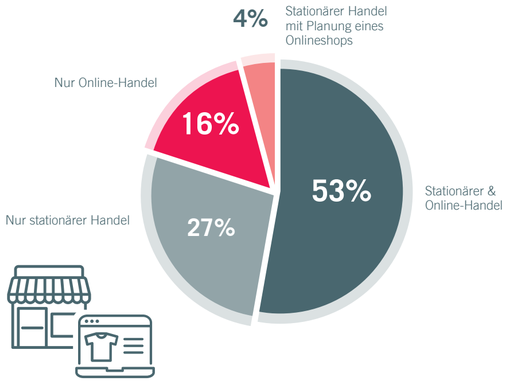
Das vom Handelsverband verliehene **Trustmark-Austria-Gütesiegel** hat unter den Onlinehändlern einen Bekanntheitsgrad von 57%. 23% verwenden das Siegel für ihren Shop, 43% kennen und nutzen Trustmark Austria nicht. Auch das **Ecommerce-Europe-Trustmark-Siegel** ist der Hälfte der Befragten ein Begriff – genutzt wird es derzeit allerdings nur von 13%.

Österreichische Gütesiegel für Webshops	TRUSTMARK HANDELSVERBAND AUSTRIA	trust ECOMMERCE EUROPE	ÖSTERREICHISCHES ECOMMERCE-GÜTEZEICHEN	TRUSTED SHOPS GUARANTEE
nutze ich	23%	13%	27%	35%
kenne ich	34%	37%	44%	44%
kenne und nutze ich nicht	43%	51%	28%	20%

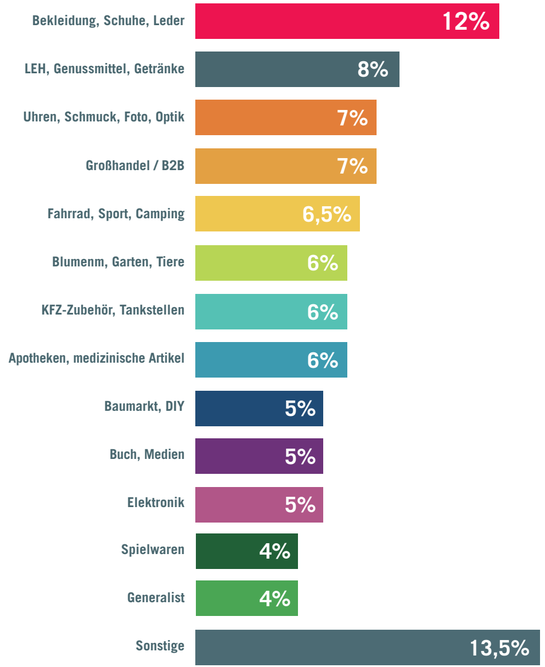
ÜBER DIE STUDIE

Die Sicherheitsstudie 2021 wurde vom österreichischen Handelsverband in Kooperation mit dem Bundesministerium für Inneres (BMI) durchgeführt. 143 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 9. November 2021.

ZUSAMMENSETZUNG DER STICHPROBE



BRANCHENÜBERBLICK DER BEFRAGTEN

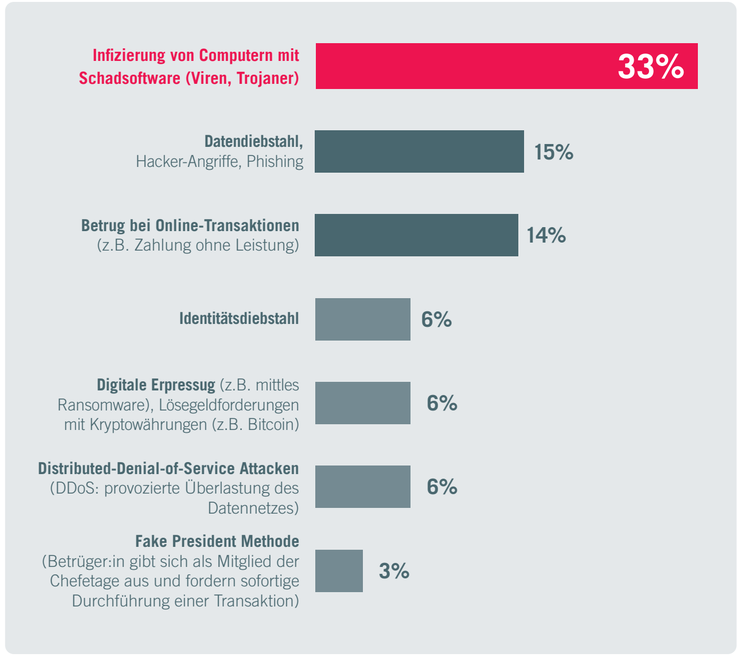


CONSUMER CHECK

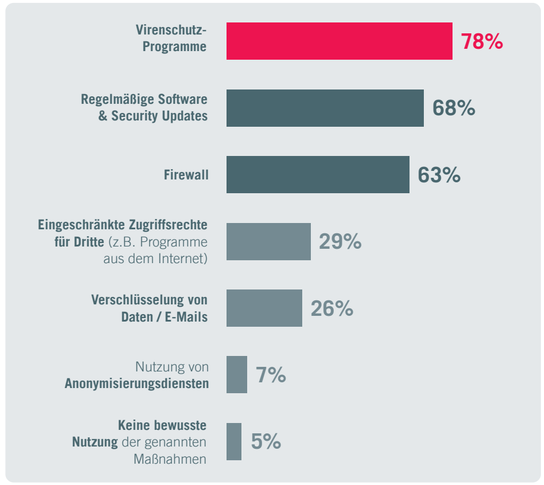
Wie ticken die österreichischen Konsument:innen?

Mit welchen Formen von Cyberkriminalität haben Sie schon Erfahrungen gemacht?

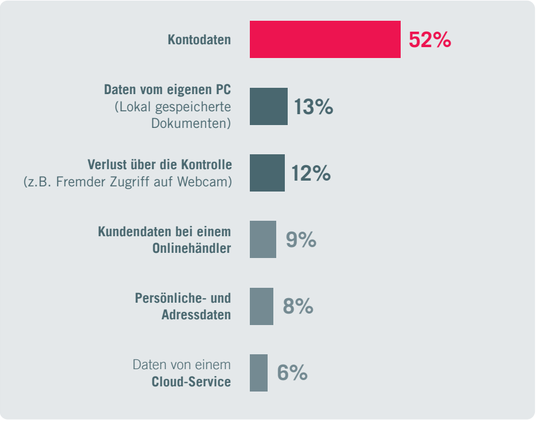
Neben der Unternehmensseite wurde für die SICHERHEITSSTUDIE 2021 auch die Konsumentenperspektive beleuchtet. In Kooperation mit Mindtake Research wurden hierfür 500 österreichische Verbraucher:innen zu ihren Erfahrungen mit Cyberkriminalität befragt. Das Ergebnis: Ein Drittel der Konsument:innen hat bereits negative Erfahrungen mit Schadsoftware wie Viren oder Trojanern gemacht. 15% waren schon von Datendiebstahl durch Phishing-Angriffe betroffen, weitere 14% waren Opfer von Betrug bei Online-Transaktionen.



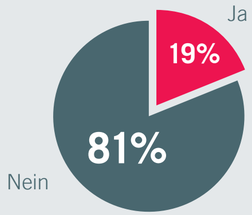
Wie schützen Sie sich **vor Cyberangriffen?**



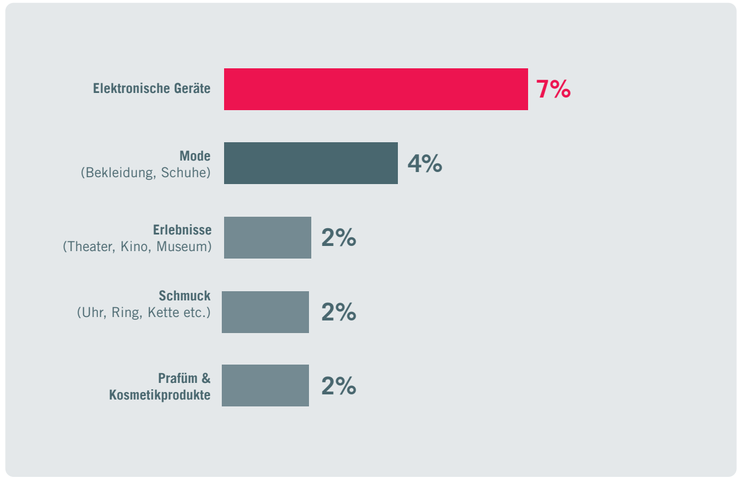
Bei welchen Daten haben Sie **am meisten Angst davor, Opfer von Cyperkriminalität zu werden?**



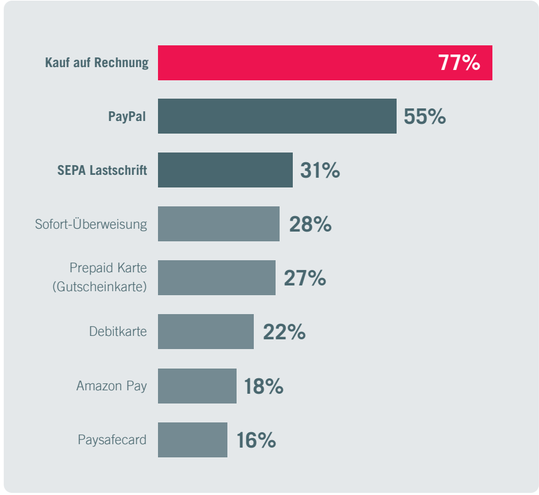
Waren Sie schon mal Opfer **eines Fake-Webshops?**



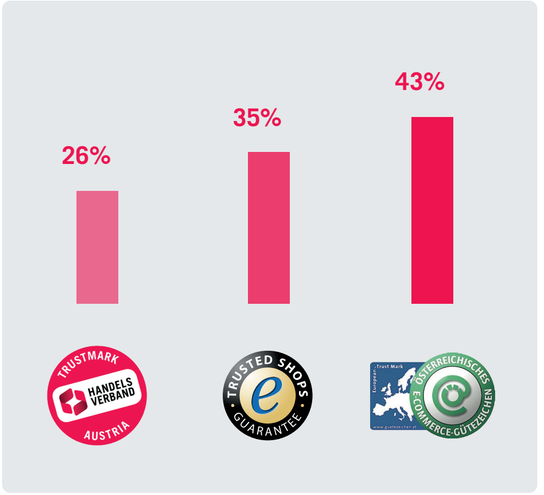
Falls ja, in welcher **Produktgruppe** kam dies vor?



Welche Zahlungsarten sind Ihrer Meinung nach **am sichersten?**



Sind Ihnen die folgenden **Gütesiegel bekannt?**



HANDELSVERBAND
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

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
Vizepräsidenten: Karin Saey, Mag. Harald Gutschi, Horst Leitner, Norbert W. Scheele
Studiendesign & inhaltliche Aufbereitung: Gerald Kühberger
Design: Gebrüder Pixel