OeNB Report 2026/22
20 Seiten

115,4 Mio EUR Schaden durch Betrug im Zahlungsverkehr im Jahr 2025

In Österreich machte die Schadenssumme durch Betrug im unbaren Zahlungsverkehr 2025 115,4 Mio EUR aus. Insgesamt schlugen Betrüger:innen 351.000-mal zu. Von 2024 auf 2025 stieg das Betragsvolumen betrügerischer Zahlungen um 17,6 %. Hauptgrund für diesen Anstieg sind betrügerische Überweisungen. In Bezug auf alle Transaktionen war damit jedoch nur eine von 16.000 Transaktionen betrügerisch. Betrüger:innen manipulieren häufig Zahler:innen, damit diese die Zahlung selbst tätigen. Bezogen auf die Gesamtschäden liegt der Österreich-Wert der Betrugsrate bei den meisten Zahlungskategorien unter dem EU-Mittelwert.

Autor:innen

Patrick Thienel
Oesterreichische Nationalbank,
Abteilung Statistik – Außenwirtschaft, Finanzierungsrechnung und Monetärstatistiken
patrick.thienel@oenb.at

Katharina Ederer,
Susanne Reich-Rohrwig
Oesterreichische Nationalbank,
Abteilung Digitaler Euro, Marktinfrastrukturen und Zahlungsverkehrsstrategie
katharina.ederer@oenb.at
susanne.reich-rohrwig@oenb.at

Veröffentlichung

20. August 2026

Anstieg der Schadens-summen durch Betrug

Der Anstieg der Schadens-summen durch Betrug im Jahr 2025 um 17,6 % ist vor allem auf betrügerische Überweisungen zurückzuführen.
Zahler:innen werden häufig von Betrüger:innen manipuliert, um solche Zahlungen sogar selbst zu tätigen.

Höchste Anzahl an Betrugs-fällen bei Kartenzahlungen

Neun von zehn Betrugsfällen beim unbaren Bezahlen entstehen bei Kartenzahlungen. Dieser Wert ist seit einigen Jahren konstant. 2025 betrug die Schadenssumme bei Kartenzahlungen rund 23,5 Mio EUR. Die Einzelbeträge je Schadensfall sind geringer als bei Überweisungen.

Meldepflicht zu Betrugsfällen

Zahlungsdienstleister haben im Rahmen der Zahlungsverkehrs-statistik Daten zu Betrugsfällen mit den unterschiedlichen Zahlungsmitteln der Oesterreichischen Nationalbank bzw. der Finanzmarktaufsichts behörde halbjährlich vorzulegen.

1 Abstract

Dieser Report analysiert die Entwicklung des Betrugs im unbaren Zahlungsverkehr in Österreich im Jahr 2025. Die Analyse basiert auf den Betrugsdaten, die österreichische Zahlungsdienstleister gemäß den gesetzlichen Meldepflichten an die Oesterreichische Nationalbank (OeNB) übermitteln. Im Jahr 2025 wurden insgesamt 351.000 betrügerische Transaktionen mit einer Schadenssumme von 115,4 Mio EUR registriert, was einen Anstieg um 17,6 % gegenüber 2024 bedeutet. Das Gesamtvolumen aller unbaren Zahlungen blieb mit rund 7,2 Billionen EUR weitgehend unverändert. Trotz des beschriebenen Anstiegs war lediglich eine von rund 16.000 unbaren Transaktionen betrügerisch. Insgesamt flossen je 1.000 EUR durchschnittlich 1,6 Cent an Betrüger:innen.

Die Analyse zeigt deutliche Unterschiede zwischen den einzelnen Zahlungsinstrumenten: 90 % aller Betrugsfälle entfielen auf Kartenzahlungen. Den größten finanziellen Schaden verursachten jedoch betrügerische Überweisungen. Sie machten mit 89,6 Mio EUR rund 78 % der gesamten Schadenssumme aus. Der durchschnittliche Schaden betrug über alle Zahlungsinstrumente hinweg rund 329 EUR je Betrugsfall, bei betrügerischen Überweisungen rund 3.000 EUR. Die Analyse zeigt zudem eine zunehmende Verlagerung von technischen Angriffen hin zu Betrugsformen der sozialen Manipulation (auch: „Social Engineering“). Dabei werden Zahlungsdienstnutzer:innen gezielt dazu gebracht, betrügerische Zahlungen selbst zu autorisieren.

Der Report beschreibt die Entwicklung des Betrugs nach einzelnen Zahlungsinstrumenten und stellt aktuelle Betrugsformen dar. Darüber hinaus enthält er einen internationalen Vergleich der Betrugsraten, Informationen zu regulatorischen Entwicklungen und Haftungsfragen sowie Maßnahmen zur Betrugsprävention und zum Schutz der Verbraucher:innen. Damit wird ein aktueller Überblick über das Betrugsgeschehen im österreichischen Zahlungsverkehr gegeben und wesentliche Entwicklungen und Herausforderungen für Zahlungsdienstleister, Behörden und Zahlungsdienstnutzer:innen aufgezeigt.

2 Einleitung

In Österreich ansässige Zahlungsdienstleister (Kreditinstitute, Zahlungsinstitute, E-Geld-Institute und die Oesterreichische Nationalbank – OeNB) müssen Daten zu Betrug im Zusammenhang mit verschiedenen unbaren Zahlungsinstrumenten an die OeNB melden. Neben der internen Verwendung dieser Daten leitet die OeNB diese an die Finanzmarktaufsichtsbehörde (FMA) sowie an die Europäische Zentralbank bzw. an die Europäische Bankenaufsichtsbehörde weiter. Die Zusammenarbeit und Vernetzung der unterschiedlichen Behörden ist ein wesentlicher Faktor, um die Sicherheitsrisiken im internationalen Zahlungsverkehr besser zu verstehen und zu bekämpfen.

Neben der Erfassung, Analyse und Weiterleitung der Daten analysiert die OeNB die aktuellen Trends im Zahlungsverkehr und informiert die Öffentlichkeit darüber. Das beinhaltet auch die Aufklärung über aktuelle Betrugsmaschen, die Vermittlung von konkreten Schutzmaßnahmen und die Darstellung von aktuellen regulatorischen Entwicklungen im Zahlungsverkehr und in der Betrugsprävention.

Die von den Zahlungsdienstleistern gemeldeten Daten beziehen sich auf den „unbaren“, also „bargeldlosen“ Zahlungsverkehr (eine Ausnahme stellen Bargeldbehebungen dar, die auch erhoben werden). „Unbar“ ist nicht zu verwechseln mit dem „elektronischen“ Zahlungsverkehr. Auch wenn die Initiierung einer Transaktion nicht elektronisch durchgeführt wird (z. B. am Schalter einer Bank, am Telefon oder per Brief bzw. in Papierform bei Schecks und Zahlscheinen) sind die Transaktionen meldepflichtig.

Der Zwischenbankenverkehr ist bei der Meldung ausgeschlossen. Meldepflichtig sind daher alle Transaktionen, bei denen sich auf zumindest einer Seite (Sende- oder Empfangsseite) eine Nicht-Bank befindet. Zu jeder Zahlungsart (Überweisungen, Lastschriften, Kartenzahlungen, Scheckzahlungen, E-Geld-Zahlungen, Finanztransfers) wird die Anzahl und das Betragsvolumen der Transaktionen von Zahlungsdienstleistern erhoben. Ergänzend dazu wird gemeldet, wie viele dieser Transaktionen betrügerisch waren bzw. wie hoch der jeweilige Schaden war.

Betrugsdaten unterliegen regelmäßigen Revisionen. Ein Grund dafür ist, dass es bei Betrug die Möglichkeit gibt, bis zu 13 Monate nach dem Schadensfall eine Rückerstattung zu fordern. Daher werden auch noch ältere Betrugsfälle für die Periode, in der der Betrug stattgefunden hat, nachgemeldet.

3 Überblick über den Betrug im unbaren Zahlungsverkehr

Aktuelle Daten der OeNB zeigen, dass in Österreich die Schadenssumme durch Betrug im unbaren Zahlungsverkehr 2025 insgesamt 115,4 Mio EUR ausmachte (Tabelle 1). Von 2024 auf 2025 stieg das Betragsvolumen betrügerischer Zahlungen um 17,6 %. Das Gesamtvolumen aller ins In- und Ausland ausgehenden Zahlungen blieb dagegen bei mehr als 7 Billionen EUR stabil. Hauptgrund für den Anstieg sind betrügerische Überweisungen. Zahler:innen werden häufig von Betrüger:innen manipuliert, um solche Zahlungen sogar selbst zu tätigen.

Tabelle1

Betrügerische unbare Transaktionen im Jahr 2025

	Transaktionen insgesamt		Betrügerische Transaktionen	
	Anzahl (in Tsd)	Betrag (in Mio EUR)	Anzahl	Betrag (in Mio EUR)
Überweisung	887.209	6.671.616	30.543	89,6
Kartenzahlung (Issuer-Seite[1])	2.080.563	88.135	177.971	16,2
Kartenzahlung (Acquirer-Seite[2])	1.899.141	71.686	137.591	7,3
Geldbehebung am Geldausgabeautomaten mit Karte	196.952	51.032	899	0,4
Lastschrift, E-Geld, Finanztransfers, Schecks	580.421	366350,5	364	1,9
Summe	**5.644.286**	**7.248.819**	350.644	**115,4**

[1] Die Karte ausgebende Seite, in der Regel die Bank des Karteninhabers bzw. der Karteninhaberin.

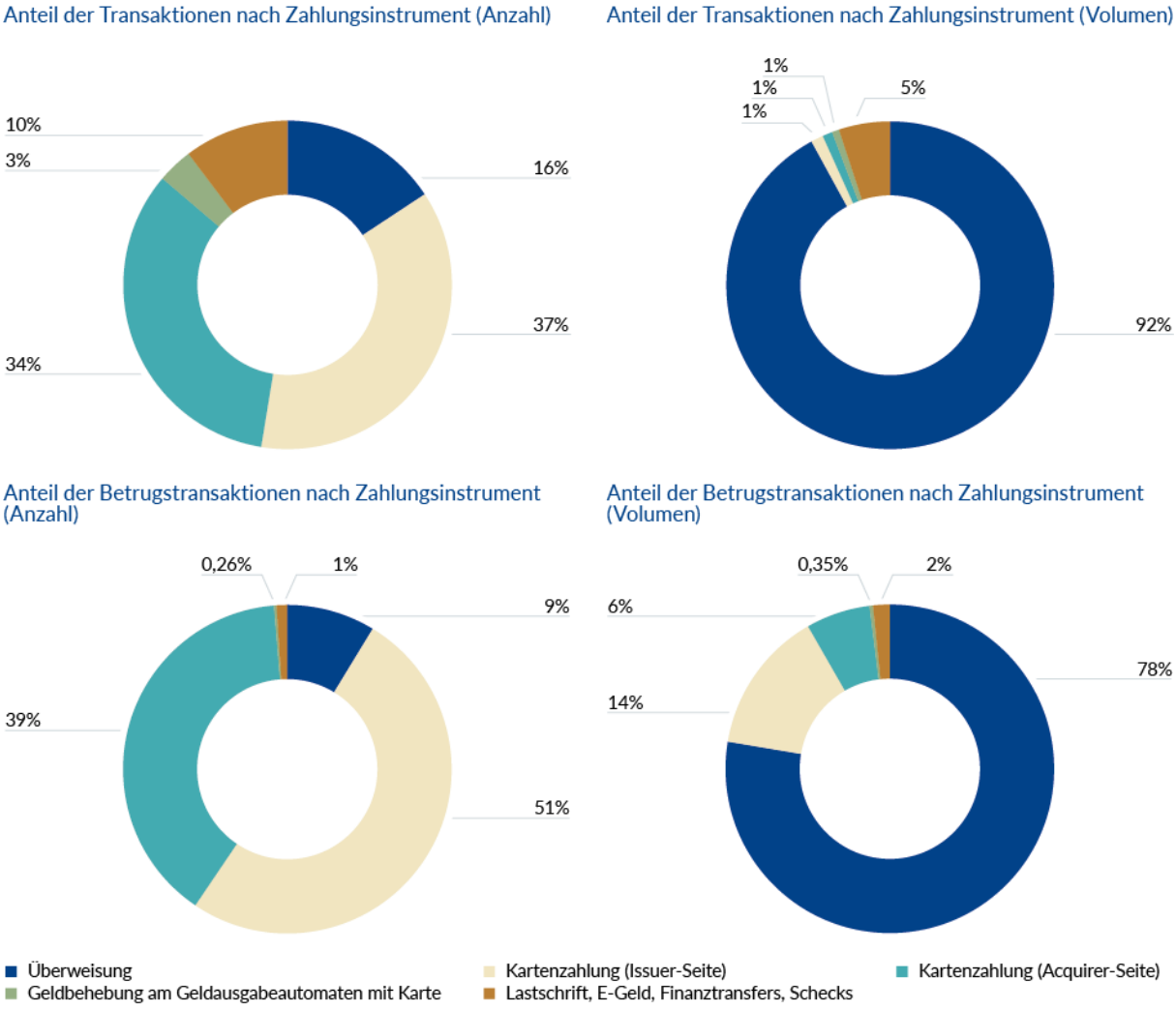
[2] Die Karte akzeptierende Terminal-/Händler:innen-Seite.

Quelle: OeNB.

2025 schlugen Betrüger:innen im unbaren Zahlungsverkehr 351.000-mal zu. In Bezug auf alle Transaktionen war damit jedoch nur eine von sechzehntausend Transaktionen betrügerisch. Betrug kommt daher im unbaren Zahlungsverkehr verhältnismäßig selten vor. Betrachtet man das betrügerische Gesamtvolumen, so fließen von bezahlten 1.000 EUR im Schnitt 1,6 Cent an Betrüger:innen. Die durchschnittliche Schadenssumme pro Betrugsfall liegt seit Jahren bei etwa 329 EUR. Diese unterscheidet sich jedoch erheblich hinsichtlich der unterschiedlichen Transaktionskategorien. In der Kategorie „Überweisungsbetrug“ (gesendete Überweisungen; d. h., das Konto war bei einem inländischen Zahlungsdienstleister) liegt der Durchschnitt bei rund 3.000 EUR, während er bei Kartenzahlungen nur bei ca. 75 EUR liegt. Im Einzelfall wurden beim Überweisungsbetrug jedoch auch Schadenssummen von über 1 Mio EUR beobachtet. Deshalb stellt Zahlungsbetrug ein erhebliches Risiko für Nutzer:innen von Zahlungsdienstleistern, Banken bzw. die Finanzbranche dar.

Grafik 1

Übersicht über die Bedeutung der unterschiedlichen unbaren Zahlungsinstrumente (2025)

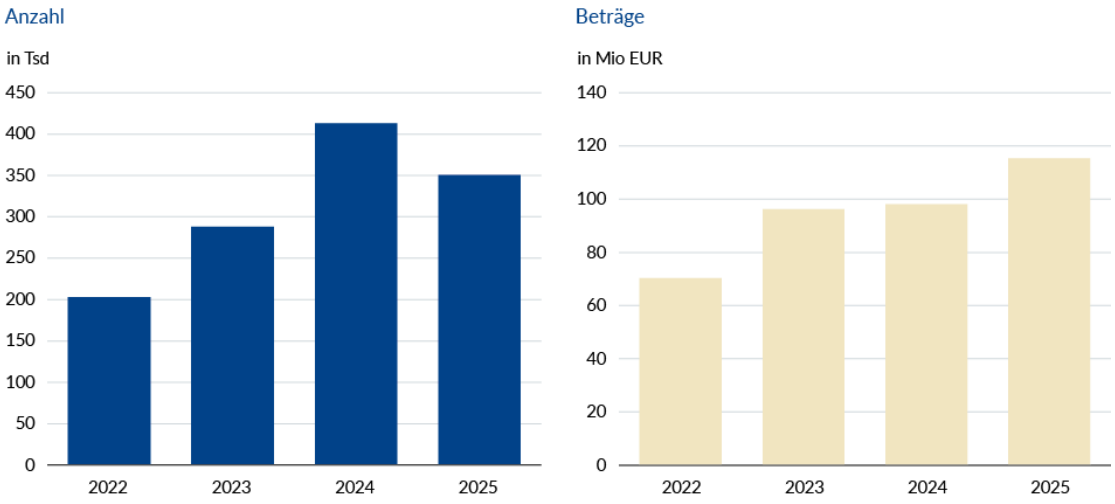


Quelle: OeNB.

In Österreich liegt die durchschnittliche Transaktionshöhe bei allen gesendeten Zahlungskartentransaktionen bei 42 EUR und jene bei gesendeten Überweisungen bei 7.520 EUR. Mit einer Zahlungskarte werden überwiegend kleinere bzw. mittlere alltägliche Zahlungen (z. B. im Supermarkt, in der Tankstelle etc.) durchgeführt, während bei Überweisungen auch sehr hohe Beträge (insbesondere von Unternehmen, z. B. für Wareneinkäufe) üblich sind. Entsprechend überwiegen Kartenzahlungen bei der Betrachtung der Anzahl an Transaktionen im unbaren Zahlungsverkehr bzw. haben Überweisungen einen sehr hohen Anteil (92 %) beim zugrunde liegenden Transaktionsvolumen (Grafik 1). Dieses Verhältnis spiegelt sich auch bei den betrügerischen Transaktionen wider. Betrügerische Überweisungen machen in Österreich 9 % aller gemeldeten Betrugsfälle aus. Bezogen auf das betrügerische Volumen richten sie jedoch mit einem Anteil von 78 % den größten finanziellen Schaden an.

Grafik 2

Entwicklung der Betrugstransaktionen bei unbaren Zahlungsmitteln in Österreich

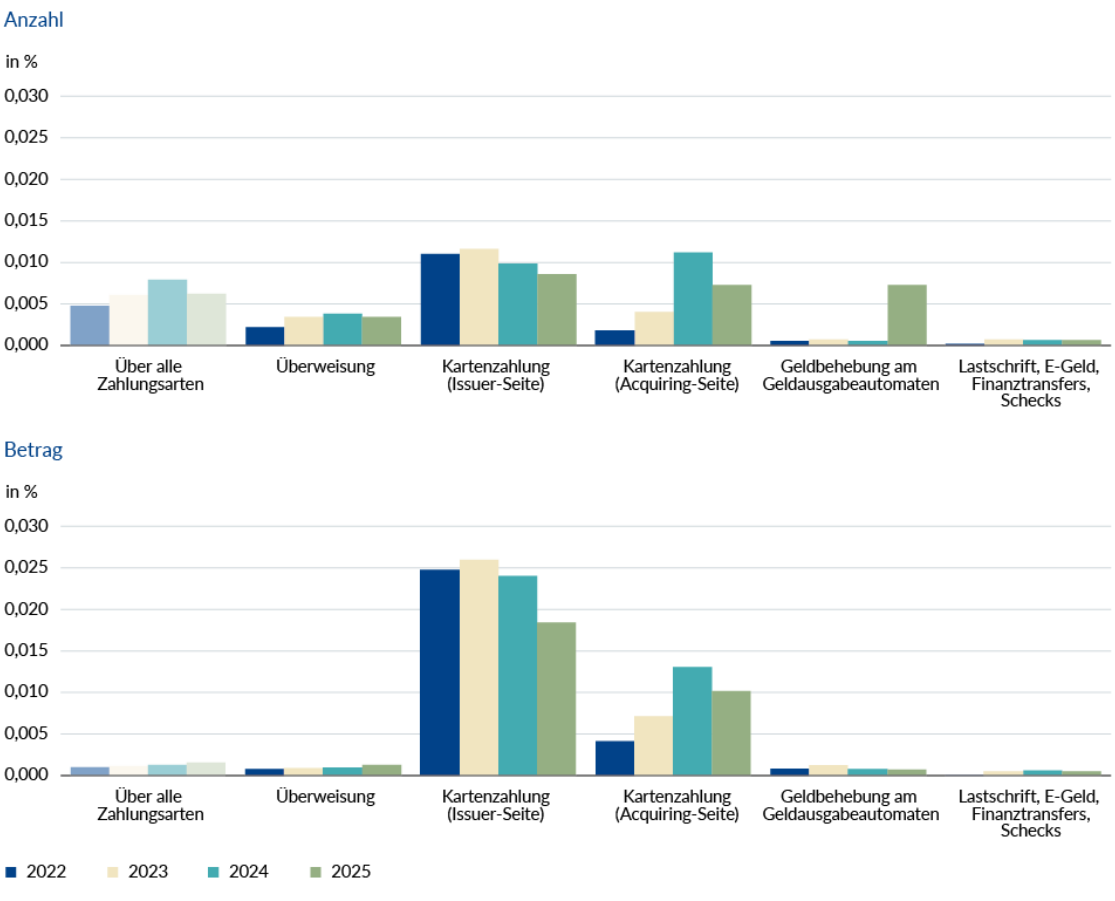


Quelle: OeNB.

Seit 2022 stiegen sowohl die Anzahl an betrügerischen Transaktionen als auch die Schadenssummen an (Grafik 2). Lag die Anzahl der Betrugstransaktionen 2022 noch bei 203.000, stiegen diese bis 2025 um 73 % auf 351.000 an. Zwischenzeitlich (2024) lag der entsprechende Wert sogar bei 413.000. Die Schäden lagen 2022 bei 70,3 Mio EUR und sie stiegen mittlerweile um 66 % auf 115,4 Mio EUR an.

Grafik 3

Betrugsfälle in Österreich als Anteil an den Transaktionen



Quelle: OeNB.

Über alle Zahlungsinstrumente hinweg blieb die jährliche Betrugsquote[1] – bezogen auf die Anzahl an Transaktionen – im Zeitraum 2022–2025 mit zuletzt 0,006 % relativ stabil und niedrig (Grafik 3). Die am Gesamtwert der Transaktionen gemessene Betrugsquote lag mit 0,001 % sogar noch deutlich darunter.

In beiden Fällen zeigt sich, dass die Betrugsquote bei Kartenzahlungen auf der Issuer-Seite im Jahr 2025 (0,009 % bezogen auf die Anzahl bzw. 0,018 % bezogen auf das Volumen) überdurchschnittlich hoch ist. Dass der Betrug auf der Issuing-Seite (= die Karte ausgebende Seite, in der Regel die Bank des Karteninhabers bzw. der Karteninhaberin) höher ist als auf der Acquiring-Seite (= die Karte akzeptierende Terminal-/Händler:innen-Seite) liegt daran, dass es sich beim Betrug im Zahlungskartengeschäft primär um Zahlungen mit gestohlenen Zahlungskarten handelt. Betrug auf der Terminal-/Händler:innenseite kommt seltener vor.

Dass die Betrugsquote gemessen am Wert (Betrag) der Zahlung bei Karten überdurchschnittlich hoch ist, liegt an dem bereits erwähnten Umstand, dass mit einer Zahlungskarte viele alltägliche Zahlungen durchgeführt werden und der Durchschnittbetrag mit 42 EUR entsprechend gering ausfällt.

Die Betrüger:innen versuchen, mit den gestohlenen Karten einen unter den jeweiligen Rahmenbedingungen höchstmöglichen Betrag zu lukrieren. Der Durchschnittsbetrag bei betrügerischen Kartenzahlungen liegt bei 91 EUR.

Anders verhält es sich bei Überweisungen, bei denen die durchschnittliche Überweisungshöhe (7.520 EUR) stark von großvolumigen Überweisungen von Unternehmen beeinflusst wird, während der durchschnittliche betrügerische Betrag mit 2.934 EUR darunter lag.

Die Analyse der Länderverteilung der betrügerische Zahlungsempfänger:innen zeigt, dass 2025 7,3 % aller betrügerischen Transaktionen nach Österreich und 50,7 % in die EU gingen. 42 % der betrügerischen Transaktionen gingen in Länder außerhalb der EU. Die Länderverteilung unterscheidet sich allerdings sehr nach Zahlungsart (siehe auch Kapitel 5 bis 7).

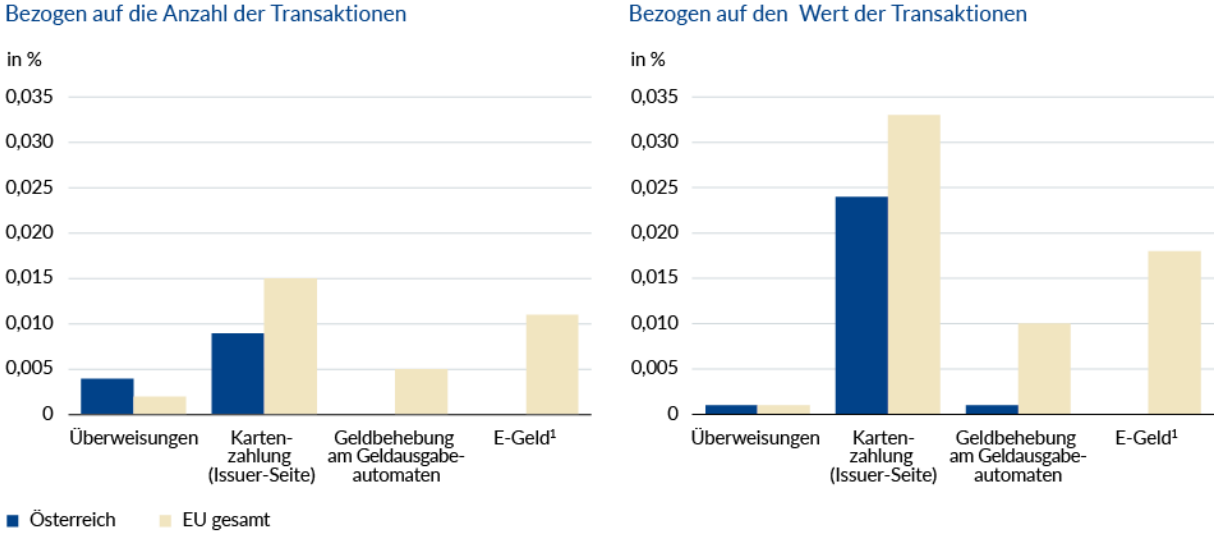
[1] Die Betrugsquote ist der Anteil der Betrugsfälle an der Gesamtzahl an Transaktionen.

4 Internationaler Vergleich

Daten der Europäischen Bankenaufsichtsbehörde und der Europäischen Zentralbank (EZB) zeigen, dass Betrugsverluste im Europäischen Wirtschaftsraum (EWR) im Jahr 2024 auf rund 4,2 Mrd EUR angestiegen sind. Insgesamt fanden rund 19,6 Millionen Betrugsfälle im unbaren Zahlungsverkehr statt.

Grafik 4

Betrugsraten (Stand 2024)



¹ Die EU-Vergleichdaten sind nur für E-Geld verfügbar.
Quelle: EZB/EBA.

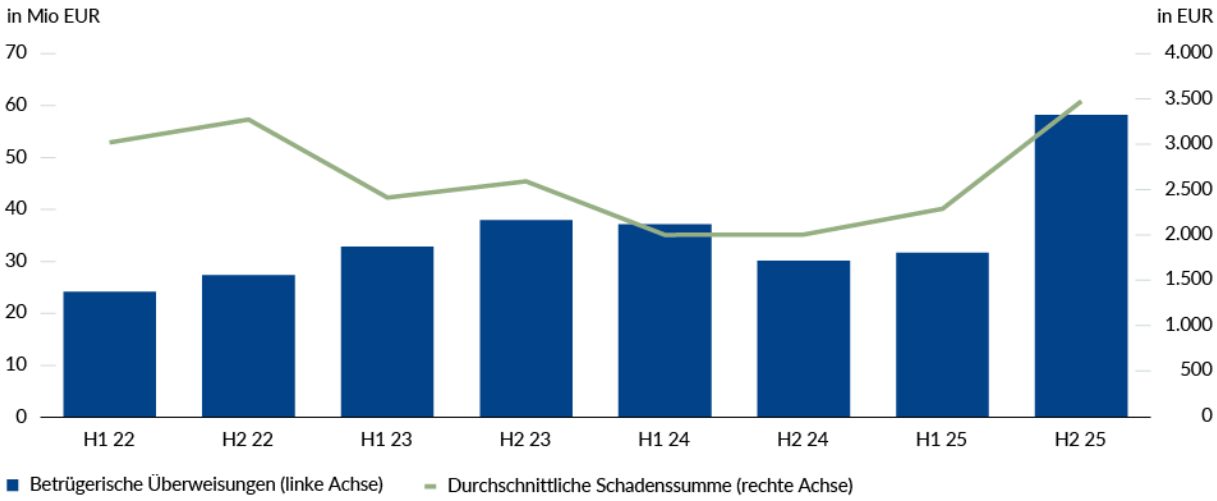
Relativ gesehen findet in Österreich weniger Betrug statt als in vielen anderen EU-Ländern. Das trifft auf alle Zahlungsarten mit Ausnahme von Überweisungen zu. Hier ist der Österreich-Wert der Betrugsrate (0,004 %) doppelt so hoch wie der EU-Wert (0,002 %). Bezogen auf die Gesamtschäden liegt der Österreich-Wert der Betrugsrate für Überweisungen genau im EU-Mittelwert (0,001 %) und bei den restlichen Transaktionsarten weit darunter (Grafik 4). Das bedeutet, dass es in Österreich zwar mehr Betrugsfälle bei Überweisungen als im EU-Schnitt gibt, die Schadenssummen pro Transaktion aber geringer sind als im EU-Schnitt.

5 Betrügerische Überweisungen

Betrügerische Überweisungen erreichten im Jahr 2025 mit rund 89 Mio EUR den höchsten absoluten Wert seit dem Beginn der Erhebung im Jahr 2022. Das ist ein Anstieg um 74 % gegenüber 2022. Insbesondere im zweiten Halbjahr 2025 stieg die Schadenssumme durch betrügerische Überweisungen deutlich auf 58 Mio EUR an (Grafik 5). Das ist ein fast doppelt so hoher Wert wie im selben Zeitraum des Vorjahres. Gleichzeitig sank die Anzahl der Betrugsfälle bei Überweisungen leicht auf 30.500 Fälle im Jahr. Charakteristisch ist hier die Kombination aus einer vergleichsweise niedrigen Zahl an Betrugsfällen und sehr hohen durchschnittlichen Schadensbeträgen. Der durchschnittliche Betrugsbetrag lag im zweiten Halbjahr 2025 bei knapp 3.500 EUR. Er stieg damit innerhalb eines Halbjahres um mehr als 1.000 EUR.

Grafik 5

Betrügerische Überweisungen in Österreich



Quelle: OeNB.

83 % der Verluste bei Überweisungen entstanden 2025, weil es Betrüger:innen gelang, Zahler:innen zu täuschen und sie zu einer Zahlung zu überreden. Hier zeigt sich eine zunehmende Verlagerung von technischen Angriffen hin zu sozialer Manipulation. Dabei nutzen Betrüger:innen gezielt das Vertrauen oder die Hilfsbereitschaft der Opfer aus, um an sensible Daten zu kommen oder Zugriff auf Konten und Geräte zu erhalten (siehe Infobox 1). Betrüger:innen versenden täuschend echte E-Mails, die scheinbar von der eigenen Bank, einem bzw. einer Vorgesetzten oder einem Krypto-Anbieter stammen. Die Opfer klicken auf den Link, geben ihre Zugangsdaten ein und autorisieren dadurch unwissentlich betrügerische Zahlungen. Beim Anlagebetrug wiederum locken Betrüger:innen mit unrealistisch hohen Renditeversprechen.

Täter:innen entwickeln ihre Betrugsmaschen kontinuierlich weiter und passen sie an neue Technologien, Kommunikationskanäle und das veränderte Zahlungsverhalten an. Neben klassischen Phishing-Angriffen (siehe Infobox 1) gewinnen insbesondere von künstlicher Intelligenz (KI) gestützte Betrugsformen sowie professionell organisierte Betrugsnetzwerke zunehmend an Bedeutung. Der Einsatz von KI erleichtert zusätzlich die Erstellung täuschend echter E-Mails, Webseiten, Stimmen und Videobotschaften, und erhöht dadurch die Glaubwürdigkeit betrügerischer Inhalte.

Die starke Kund:innenauthentifizierung (Strong Customer Authentication, SCA) dient dazu, die Identität einer Person bei der Freigabe einer elektronischen Zahlung oder beim Zugriff auf ein Zahlungskonto eindeutig zu überprüfen. Dafür müssen mindestens zwei voneinander unabhängige Authentifizierungsmerkmale aus den Kategorien Wissen (z. B. Passwort oder PIN), Besitz (z. B. Smartphone oder TAN-Gerät) und Inhärenz (z. B. Fingerabdruck oder Gesichtserkennung) verwendet werden.

Die starke Kund:innenauthentifizierung bietet somit einen wirksamen Schutz vor unbefugten Zugriffen auf Konten. Sie kann jedoch nicht verhindern, dass Kund:innen durch Manipulation dazu verleitet werden, betrügerische Zahlungen selbst freizugeben.

2025 wurden 85 % aller elektronischen Überweisungen mit starker Kund:innenauthentifizierung freigegeben. Der Rest fiel unter bestimmte Ausnahmen wie Zahlungen an die eigene Person, vertrauenswürdige Empfänger:innen bzw. von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle.

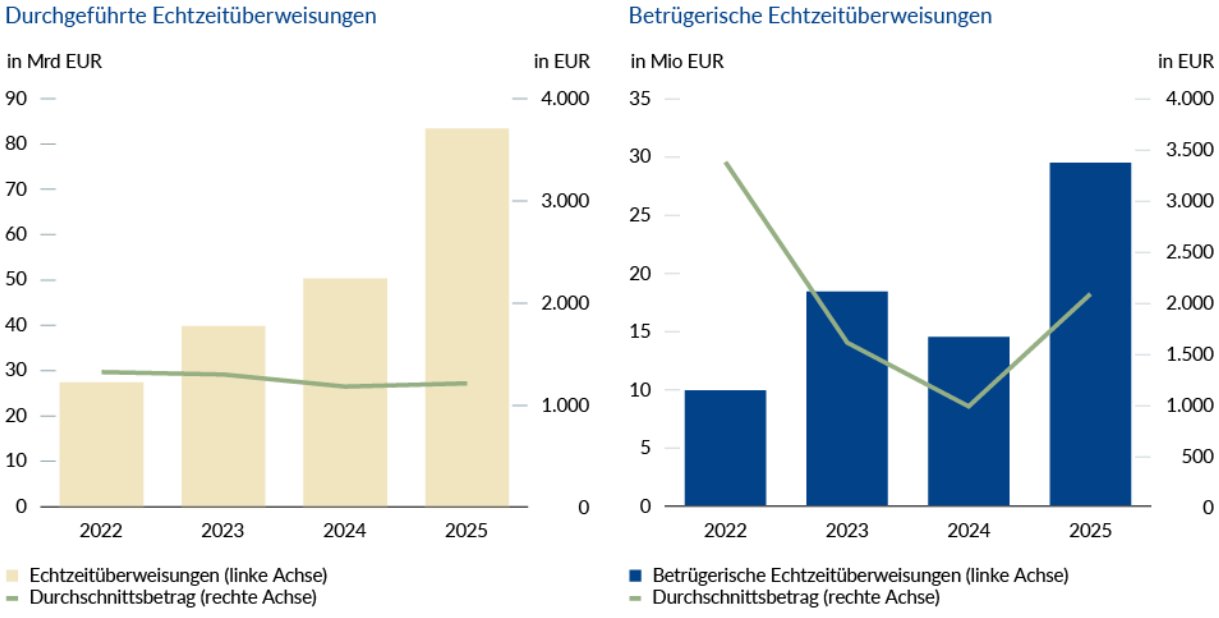
Die Analyse der Länderverteilung der betrügerischen Zahlungsempfänger:innen zeigt, dass ein Fünftel aller betrügerischen Überweisungen 2025 auf Konten in Österreich und 78 % auf Konten in die EU gingen. Betrügerische Überweisungen außerhalb der EU spielen eine klar untergeordnete Rolle.

Seit Oktober 2025 sind Banken verpflichtet, Echtzeitüberweisungen durchführen zu können. Das sind Zahlungen, die innerhalb weniger Sekunden durchgeführt werden. Zusätzlich sind Echtzeitüberweisungen rund um die Uhr, sieben Tage in der Woche, 365 Tage im Jahr möglich. 2025 stieg der Gesamtbetrag an Echtzeittransaktionen auf 83 Mrd EUR an (Grafik 6). Seit 2023 kam es zu mehr als einer Verdoppelung sowohl bei der Anzahl (+124 %) der Echtzeitüberweisungen als auch beim Wert (+109 %). Gleichzeitig stieg der Betrug in diesem Segment aber nur um 23 % (Anzahl) bzw. 60 % (Wert). 2025 umfassten betrügerische Echtzeitüberweisungen einen Gesamtbetrag von 29,5 Mio EUR.

Während der durchschnittliche Wert einer Echtzeitüberweisung relativ stabil bei rund 1.200 EUR lag, schwankt der durchschnittliche Wert einer betrügerischen Echtzeitüberweisung über die letzten vier Jahre zwischen 977 EUR (2024) bzw. 3.380 EUR (2025).

Grafik 6

Echtzeitüberweisungen

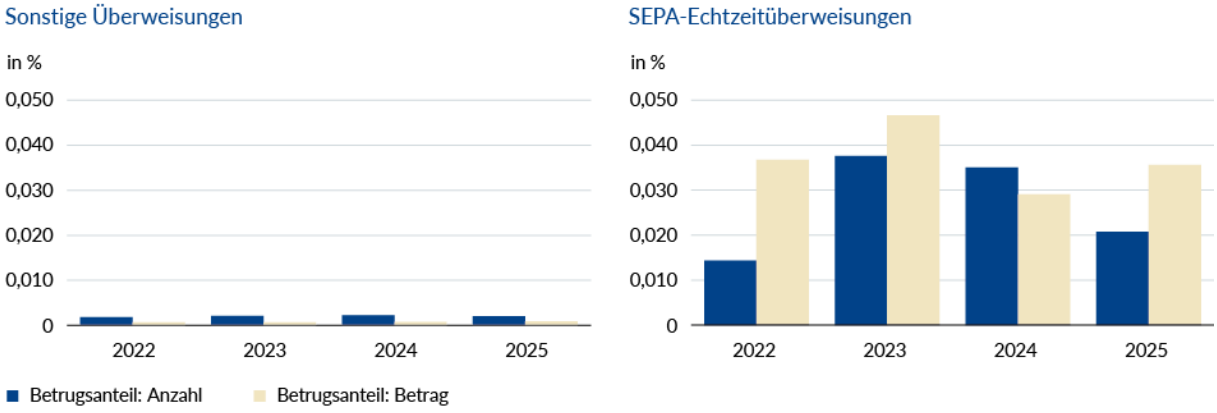


Quelle: OeNB.

Die Betrugsrate bei Echtzeitüberweisungen ist wesentlich höher (0,021 % bei der Anzahl, 0,036 % beim Betrag) als jene von bei Standardüberweisungen (0,002 % bei der Anzahl, 0,001 % beim Betrag).

Grafik 7

Betrugsrate in Österreich als Anteil an den Überweisungen



Quelle: OeNB.

Durch die sofortige Durchführung erhöht sich das Risiko bei Betrugsfällen, da die Zahlung nicht mehr storniert werden kann. Als Schutzmaßnahme müssen Banken seit Oktober 2025 prüfen, ob der Name des Empfängers bzw. der Empfängerin zur IBAN passt (der sogenannte IBAN-Namensabgleich[2]; siehe auch Infobox 6), um Fehlüberweisungen und Betrug zu vermeiden. Banken führen außerdem eine erhöhte Transaktionsüberwachung durch.

Infobox 1

Die gängigsten Betrugsmethoden bei Überweisungen

Unter den Oberbegriff „soziale Manipulation“ (auch: „Social Engineering“) fällt:

- Kaufbetrug: Waren oder Dienstleistungen werden im Voraus bezahlt, aber nicht geliefert. Häufig nutzen Betrüger:innen gefälschte Online-Shops, Inserate auf Verkaufsplattformen oder Angebote in sozialen Medien, um Käufer:innen zur Vorauszahlung zu bewegen.
- Anlagebetrug: Anleger:innen werden gezielt über den wahren Wert, die Risiken oder sogar die Existenz einer Investition getäuscht. Potenzielle Investor:innen werden dazu bewegt, dem bzw. der Täter:in Kapital zu überlassen. Um Vertrauen zu schaffen, missbrauchen sie häufig die Namen und Logos bekannter Institutionen wie der OeNB, der FMA, des Bundesministeriums für Finanzen oder anderer renommierter Organisationen. Dadurch soll bei potenziellen Anleger:innen der Eindruck besonderer Seriosität, staatlicher Kontrolle und Sicherheit entstehen sowie das Vertrauen in die angebotene Geldanlage gestärkt werden. Oft werben Kriminelle ihre Opfer über soziale Netzwerke, Messenger-Dienste oder Suchmaschinen an.
- Liebesbetrug: Täter:innen täuschen über Online-Kanäle eine emotionale oder romantische Beziehung vor, um das Vertrauen der Opfer zu gewinnen. Anschließend werden die Betroffenen unter Vorwänden dazu gebracht, Geld selbst zu überweisen.
- Rechnungs- oder Überweisungsbetrug: Gefälschte oder manipulierte Rechnungen werden per E-Mail oder Post versendet, die zur Umleitung von Zahlungen auf Konten von Betrüger:innen verleiten.

[2] IBAN-Namensabgleich

- Paketdienst- und Zustellbetrug: Gefälschte Benachrichtigungen im Namen von Paket- und Zustelldiensten zählen weiterhin zu den häufigsten Betrugsformen. Die Empfänger:innen werden per SMS, E-Mail oder Messenger-Dienst dazu aufgefordert, vermeintlich offene Zustellgebühren zu bezahlen oder persönliche bzw. Zahlungsdaten einzugeben. Neben der unmittelbaren Erschleichung von Zahlungen dient diese Betrugsmasche häufig auch dem Diebstahl personenbezogener oder finanzieller Daten, die anschließend für weitere Betrugsversuche oder Identitätsmissbrauch genutzt werden.
- CEO-Betrug: Die Betrüger:innen geben sich als Führungskraft (CEO: Chief Executive Officer) oder andere autorisierte Person des Unternehmens aus und setzen die Betroffenen unter Zeitdruck, um sie zur Überweisung hoher Geldbeträge auf Konten der Betrüger:innen zu bewegen.
- „Behörden"-Betrug: Täter:innen geben sich als Mitarbeiter:innen von Behörden oder anderen öffentlichen Einrichtungen aus und behaupten, die Betroffenen müssen eine angebliche Geldstrafe begleichen, überfällige Steuern nachzahlen oder eine irrtümlich erhaltene Rückerstattung zurücküberweisen. Um ihre Forderungen glaubwürdig erscheinen zu lassen, verwenden sie häufig gefälschte Schreiben, E-Mails, Telefonnummern oder offizielle Logos. Gleichzeitig setzen sie die Betroffenen mit angeblichen rechtlichen Konsequenzen, Kontosperren oder Strafverfahren unter Druck, um eine rasche Zahlung zu erzwingen.
- Enkeltrick/Neffentrick: Betrüger:innen geben sich als Enkel:in, Neffe, Nichte oder andere nahe Angehörige aus und schildern eine angebliche Notlage oder einen dringenden finanziellen Engpass. Unter dem Vorwand, sofort Hilfe zu benötigen, setzen sie die Betroffenen unter Zeitdruck und bewegen sie dazu, Geld zu überweisen oder an vermeintliche Bot:innen zu übergeben.

Unabhängig von den verschiedenen Formen sozialer Manipulation verwenden Betrüger:innen technische Täuschungsmethoden (E-Mail, SMS, Anruf, Webseite), um an sensible Daten oder Zugangsdaten zu gelangen oder unbefugten Zugriff auf Konten zu erlangen. Dazu zählen insbesondere:

- „Phishing" (Wortkombination aus „Password" und „Fishing"): Betrüger:innen versuchen Internetnutzer:innen Geheimdaten (z. B. für Online-Banking, Auktionsplattformen oder Online-Shops) zu entlocken.
- Eine Sonderform des „Phishing" stellt das „Quishing" (QR-Code-Phishing) dar: Hier werden manipulierte oder gefälschte QR-Codes verwendet, um Nutzer:innen auf betrügerische Internetseiten umzuleiten oder in Einzelfällen Schadsoftware auf dem Endgerät zu installieren. Die gefälschten QR-Codes finden sich z. B. auf Parkautomaten, Ladesäulen für Elektrofahrzeuge, Plakaten, Rechnungen oder in E-Mails. Da QR-Codes den eigentlichen Link verbergen, sind betrügerische Webseiten für Nutzer:innen häufig erst nach dem Öffnen erkennbar.
- SIM-Swapping: Betrüger:innen übernehmen die Kontrolle über eine Mobiltelefonnummer eines Opfers, um auf Online-Konten zuzugreifen oder die starke Kund:innenauthentifizierung zu umgehen. Dazu kontaktieren sie den Mobilfunkanbieter, geben sich als betroffene Person aus und veranlassen die Sperrung der bisherigen SIM-Karte sowie die Aktivierung einer neuen SIM-Karte, die sie selbst kontrollieren. Dadurch erhalten sie SMS und Anrufe – etwa Einmalcodes wie TANs („Transaktionsummer") oder OTPs („One-time Passwords") – und können diese für den unbefugten Zugriff auf Konten missbrauchen.

6 Betrügerische Kartenzahlungen bzw. -behebungen

Kartenzahlungen sind das Zahlungsinstrument mit der häufigsten Anzahl an Betrugsfällen: Neun von zehn Betrugsfällen sind auf diese zurückzuführen. Dieser Wert ist seit einigen Jahren konstant. Insgesamt betrug die Schadenssumme bei Kartenzahlungen rund 23,5 Mio EUR. Davon entfielen 16,2 Mio EUR auf die Issuing-Seite[3] (also der kartenausgebenden Seite) und 7,3 Mio EUR auf die Acquiring-Seite[4] (also die Terminal-Seite). Die Einzelbeträge je Schadensfall fallen jedoch bei Kartenzahlungen deutlich geringer aus als bei Überweisungen: Der durchschnittliche Schadensfall lag 2025 bei rund 75 EUR.

Bei Kartenzahlungen ist ein anderes Betrugsmuster als bei Überweisungen festzustellen: 2025 entfielen 79 % der Verluste auf die Ausstellung eines Zahlungsauftrags durch Betrüger:innen. Hierbei wurden die Karte bzw. die Kartendaten vor der missbräuchlichen Verwendung entweder gestohlen, kopiert oder die Karte ist gar nicht erst beim Kunden bzw. bei der Kundin angekommen.

Entsprechend zeigt sich, dass der Großteil der betrügerischen Kartenzahlungen (91 %) im Online- und App-Umfeld initiiert wird, meist infolge gestohlener Kartendaten. Der große Online-Anteil des Betrugs wird noch deutlicher, wenn man sich vor Augen hält, dass nur 5 % aller Kartenzahlungen online vorgenommen werden. Der überwiegende Teil der Kartenzahlungen (80 %) findet vor Ort, am „Point of Sale“ statt. Dabei werden 92 % aller Vorort-Zahlungen im Geschäft kontaktlos mit NFC[5] durchgeführt. Bei Vorort-Transaktionen überwiegt der Kartendiebstahl als gängigste Betrugsmethode. Die durchschnittliche Schadenssumme lag hierbei mit 46 EUR deutlich unter jener mit kopierten Kartendaten (162 EUR).

Besonders auffällig ist der Unterschied bei grenzüberschreitenden Kartenzahlungen: Transaktionen außerhalb des EWR weisen ein Vielfaches der Betrugsraten innereuropäischer Zahlungen auf und unterstreichen die Schutzwirkung der europäischen Sicherheitsanforderungen (z. B. starke Kund:innenauthentifizierung).

2025 waren 46 % aller elektronischen Kartenzahlungen stark authentifiziert. Der Rest fiel unter bestimmte Ausnahmen wie Zahlungen an die eigene Person, vertrauenswürdige Empfänger:innen bzw. von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle. Nur in rund 9 % der Betrugsfälle bei Kartenzahlungen gab es keine starke Kund:innenenauthentifizierung. Für Kartenzahlungen bei Händler:innen außerhalb des EWR gilt die EU-Zahlungsrichtlinie (PSD2) nicht. Daher ist dort eine starke Kund:innenauthentifizierung bei Kartenzahlungen im Geschäft oder online nicht Pflicht. 40 % der Betrugsfälle ohne starke Kund:innenauthentifizierung entfallen auf Zahlungsempfänger:innen außerhalb des EWR.

Die Analyse der Länderverteilung zeigt, dass 5,9 % aller betrügerischen Kartenzahlungen 2025 in Österreich und 48,3 % in der EU erfolgten. Betrügerische Kartenzahlungen außerhalb der EU lagen bei 45,8 %.

[3] Die kartenausgebende Stelle erkennt den Betrug. Die Issuing-Seite ist für Betrugsfälle verantwortlich, die direkt mit der Karte oder dem bzw. der Karteninhaber:in zusammenhängen.

[4] Betrug wird in der Händler:innen- bzw. Terminalüberwachung erkannt. Die Acquiring-Seite ist für Betrugsfälle verantwortlich, die mit Händler:innen oder Zahlungsabwicklern zusammenhängen.

[5] Near Field Communication“ (kurz: NFC) ist ein Übertragungsstandard zur kontaktlosen Kommunikation zwischen elektronischen Geräten über kurze Strecken.

Infobox 2

Die gängigsten Betrugsmethoden bei Kartenzahlungen/-behebungen

- Karten-Diebstahl: Die Zahlungskarte wird gestohlen und anschließend für unbefugte Transaktionen eingesetzt, etwa für Einkäufe oder Bargeldbehebungen. Der PIN wird mittels versteckter Kameras oder durch unerlaubtes Beobachten („Shoulder Surfing“) ausgespäht.
- Nicht erhaltene Karte: Betrüger:innen fangen neu ausgestellte oder ersetzte Zahlungskarten auf dem Postweg ab, z. B. durch Diebstahl aus Briefkästen und verwenden diese anschließend missbräuchlich.
- Kopierte Kartendaten: Betrüger:innen fangen Kartendaten bzw. den PIN ab, was oft zu unbefugten Abbuchungen führt:
    - durch Manipulation von Zahlungsterminals („Skimming“): Betrüger:innen verändern die Hard- oder Software von Kartenterminals, um Kartendaten zu stehlen.
    - Online (z. B. durch Schadsoftware bzw. Fake-Apps auf (mobilen) Geräten), Erschleichung durch
      E-Mails (Phishing), gefälschte Internetdienste und Shops).
    - bei Hackerangriffen auf Händler:innen.

  Gestohlene Kartendaten werden für Einkäufe oder andere Zahlungen verwendet, bei denen die physische Karte nicht vorgelegt werden muss.
- Verlorene Karte: Eine verlorene Zahlungskarte wird von Unbefugten gefunden und für (kontaktlose) Zahlungen missbraucht, bevor sie gesperrt werden kann.
- Händler:innenbetrug: Händler:innen rechnen z. B. nichtexistierende oder gefälschte Dienstleistungen ab oder belasten Kund:innenkarten ohne deren Zustimmung. Überhöhte Rechnungen und doppelte Abbuchungen fallen ebenfalls in diese Kategorie. Fake-Shops sowie Betrugsversuche auf Online-Marktplätzen zählen weiterhin zu den häufigsten Betrugsformen im E-Commerce.
- Manipulation von Zahlungsterminals: Betrüger:innen verändern die Hardware oder Software von Kartenterminals, um Kartendaten zu stehlen oder Transaktionen zu manipulieren (z. B. werden falsche Beträge angezeigt). Solche Angriffe können sowohl physisch (durch Aufsetzen von Skimming-Geräten) als auch digital (durch Schadsoftware in Terminals) erfolgen und führen oft zu unbefugten Abbuchungen oder Datendiebstahl.
- Betrug durch missbräuchliche Rückbuchungen (Chargebacks): Betrüger:innen veranlassen unberechtigte Rückbuchungen (Chargebacks), obwohl kein berechtigter Reklamationsgrund vorliegt. Sie behaupten z. B. wahrheitswidrig, die Ware nicht erhalten zu haben oder die Zahlung nicht autorisiert zu haben. Händler:innen verlieren dadurch häufig sowohl den Kaufbetrag als auch die bereits gelieferte Ware und müssen zusätzlich Chargeback-Gebühren sowie Bearbeitungskosten tragen.
- Cash Trapping: Betrüger:innen manipulieren den Ausgabeschacht eines Geldausgabeautomaten, sodass das ausgegebene Bargeld zunächst im Ausgabefach hängen bleibt. Nachdem der Kunde bzw. die Kundin den Geldausgabeautomaten verlassen hat, entnehmen die Täter:innen das zurückgehaltene Bargeld.
- Phishing (siehe Infobox 1)

Betrug am Geldausgabeautomaten kommt in Österreich sehr selten vor. Diese Betrugsform trat 2025 nur rund 1.000-mal pro Jahr auf. Der Gesamtschaden bei dieser Kategorie lag (über die letzten Jahre relativ konstant) bei rund 400.000 EUR. Die Betrugsrate lag bei der Anzahl der Kartenbehebungen bei 0,0005 % bzw. 0,0008 % beim Wert der Kartenbehebungen.

In rund 80 % der Fälle wurde die Karte entwendet bzw. gefälscht. Um an Kartendaten zu gelangen, kommt oft die Man-in-the-Middle-Manipulation zum Einsatz, bei der die Kommunikation zwischen Karte und Geldausgabeautomat abgefangen wird, um PINs und Transaktionsdaten zu stehlen. Dazu installieren Betrüger:innen entsprechende Vorrichtungen am Geldausgabeautomaten. In rund 3 % aller Fälle werden Kartenhalter:innen von Betrüger:innen manipuliert, um Geld zu beheben.

Die Analyse der Länderverteilung zeigt, dass 2025 die Hälfte aller betrügerischen Kartenbehebungen am Geldausgabeautomaten in Österreich erfolgten. 13,1 % wurden außerhalb der EU registriert.

7 Betrügerische Transaktionen bei anderen Zahlungsarten

Gemäß EZB-Leitlinie 1998/NP28 müssen veröffentlichte Daten mindestens drei Wirtschaftssubjekte betreffen. Für den Fall, dass ein oder zwei Wirtschaftssubjekt(e) einen ausreichend großen Anteil darstellen, um sie indirekt identifizieren zu können, werden veröffentlichte Daten so dargestellt, dass ihre indirekte Identifikation verhindert wird. Aufgrund dieser Vertraulichkeitskriterien wird der Betrug bei Lastschriften, Schecks, E-Geld (Prepaid-Karten) bzw. bei Finanztransfers gesammelt dargestellt. Bei diesen vier Kategorien trat Betrug 2025 nur rund 3.600-mal auf und der Gesamtschaden lag bei 1,7 Mio EUR.

Infobox 3

Die gängigsten Betrugsmethoden bei anderen unbaren Zahlungsmethoden

- Unautorisierte Lastschriften: Betrüger:innen nutzen gestohlene Mandatsdaten (z. B. durch Phishing oder Datenlecks) oder gefälschte Mandate für betrügerische Lastschriften.
- Scheckbetrug: Schecks werden gefälscht (mit manipulierten Beträgen oder Unterschriften) oder gestohlene Schecks werden mit gefälschten Begünstigten eingereicht.
- Betrugsmethoden bei E-Geld: wie bei Kartenzahlungen (siehe Infobox 2).

8 Wer trägt den Schaden?

Im Jahr 2025 trugen Zahlungsdienstnutzer:innen 97 % der Verluste, die bei Überweisungen entstanden. Der hohe Wert ist auf den hohen Anteil an sozialer Manipulation zurückzuführen, bei der das Opfer dazu gebracht wird, betrügerische Zahlungen zu autorisieren und freizugeben. Bei Bargeldabhebungen trugen die Kund:innen 55 % der entstandenen Verluste. Demgegenüber lag ihr Verlustanteil bei Kartenzahlungen bei lediglich 32 %. Bei E-Geld-Transaktionen wurden die Betrugsverluste hingegen vollständig von den Zahlungsinstituten getragen.

Die Rechte eines Betrugsopfers hängen davon ab, ob eine betrügerische Zahlung vom Opfer autorisiert wurde oder nicht. Generell trägt den Schaden bei einer nicht autorisierten Zahlung die Bank des Opfers. Bei autorisierten Zahlungen trägt in der Regel das Opfer den Schaden. Die konkrete Haftung hängt allerdings vom jeweiligen Einzelfall ab. Dabei können auch die Schutz- und Sorgfaltspflichten der Bank sowie eine mögliche grobe Fahrlässigkeit des Opfers eine Rolle spielen.

Eine Zahlung gilt dann als autorisiert, wenn der bzw. die Zahler:in seine Zustimmung erteilt hat. Die Zustimmung wird z. B. bei einer Überweisung mit Freigabe im Online-Banking (TAN, App-Freigabe) gegeben. Bei Kartenzahlungen erfolgt die Zustimmung mittels Eingabe der PIN oder der Unterschrift. Ohne diese Zustimmung gilt die Zahlung als nicht autorisiert.

Bei nicht autorisierten Zahlungen muss das Konto des Opfers von der Bank sofort berichtigt werden. Die Bank muss allfällige Schadensersatzansprüche gegen Kund:innen gesondert geltend machen, wenn eine grobe Fahrlässigkeit des Opfers vermutet wird. Die Pflicht einer sofortigen Erstattung durch die Bank entfällt nur dann, wenn berechtigte Gründe einen Betrug oder Betrugsversuchs des vermeintlichen Opfers nahelegen und die Bank diese Gründe der FMA schriftlich mitteilt.

Grobe Fahrlässigkeit bedeutet einen besonders schweren Sorgfaltsverstoß, der einem vernünftigen Menschen normalerweise nicht unterlaufen würde. Grobe Fahrlässigkeit liegt nur dann vor, wenn es für den Kunden bzw. die Kundin erkennbar war, dass sein bzw. ihr Verhalten eine missbräuchliche Verwendung des Zahlungsinstruments wahrscheinlich macht. Das ist unter Berücksichtigung der persönlichen Lebensgewohnheiten zu beurteilen. Werden Sicherheitswarnungen nicht beachtet, ist das allein noch keine grobe Fahrlässigkeit.

Aber selbst, wenn grobe Fahrlässigkeit bei nicht autorisierten Zahlungen vorliegt, haftet das Betrugsopfer nicht, wenn der Zahlungsdienstleister keine starke Kund:innenauthentifizierung verlangt hat. Muss sich der Zahlungsdienstleister eigene Sorgfaltsverletzungen vorwerfen lassen, kann es zu einer Schadensteilung bzw. Haftungsminderung für den Kunden bzw. die Kundin kommen.

Bei autorisierten Zahlungen trägt prinzipiell der Kunde bzw. die Kundin den Schaden, auch wenn die Autorisierung durch einen Betrug erreicht wurde. Wenn die Bank die Zahlung fehlerhaft ausgeführt oder ihre Schutz- und Sorgfaltspflichten verletzt hat, kann der Kunde bzw. die Kundin Schadensersatzansprüche gegen die Bank geltend machen. Selbst bei Mitverschulden des Kunden bzw. der Kundin kann es zu einer Teilung des Schadens kommen.

Diese Ausführungen beziehen sich auf die aktuelle Rechtslage[6] bzw. Rechtsprechung. Mit den voraussichtlich im Herbst 2026 veröffentlichten neuen Regelungen (Zahlungsdienste-Verordnung und Zahlungsdienste-Richtlinie) werden Ende 2028 oder Anfang 2029 neue Haftungsregelungen und Sicherheitsvorkehrungen eingeführt, die Konsument:innen besser vor Betrug im unbaren Zahlungsverkehr schützen sollen.

Infobox 4

Handlungsempfehlungen im Betrugsfall

Bei Verdacht auf einen Betrugsfall oder nach einer bereits erfolgten betrügerischen Transaktion sollten Betroffene rasch handeln. Je schneller Maßnahmen gesetzt werden, desto größer sind die Chancen, Schäden zu begrenzen oder weitere missbräuchliche Transaktionen zu verhindern.

- **Sofortige Kontaktaufnahme mit der Bank:** Verdächtige Transaktionen unverzüglich melden und gegebenenfalls Rückruf oder Sperrmaßnahmen veranlassen.
- **Sperre von Karten und Zugängen:** Zahlungskarten, Online-Banking-Zugänge oder andere betroffene Zahlungsmittel umgehend sperren lassen.
- **Passwörter ändern:** Zugangsdaten zu Online-Banking, E-Mail-Konten und weiteren betroffenen Diensten unverzüglich ändern.
- **Mobilfunkanbieter informieren:** Besteht der Verdacht, dass auch Ihre Telefonnummer kompromittiert wurde (z. B. durch SIM-Swapping), sollten Sie umgehend Ihren Mobilfunkanbieter informieren und gegebenenfalls Ihre SIM-Karte sperren oder austauschen lassen.
- **Vorfall dokumentieren:** Nachrichten, E-Mails, SMS, Screenshots oder Zahlungsbelege als Beweismittel sichern.

[6] ZaDiG (2018).

- **Anzeige bei der Polizei:** Betrugsfälle möglichst rasch bei der Polizei melden.
- **Meldung an relevante Stellen:** Betrügerische Internetseiten, Fake-Shops oder Phishing-Nachrichten z. B. an die Watchlist Internet[7] oder andere zuständige Meldestellen weiterleiten.
- **Unterstützungsangebote nutzen:** Bei Bedarf Beratungs- und Informationsstellen in Anspruch nehmen (siehe Infobox 7).

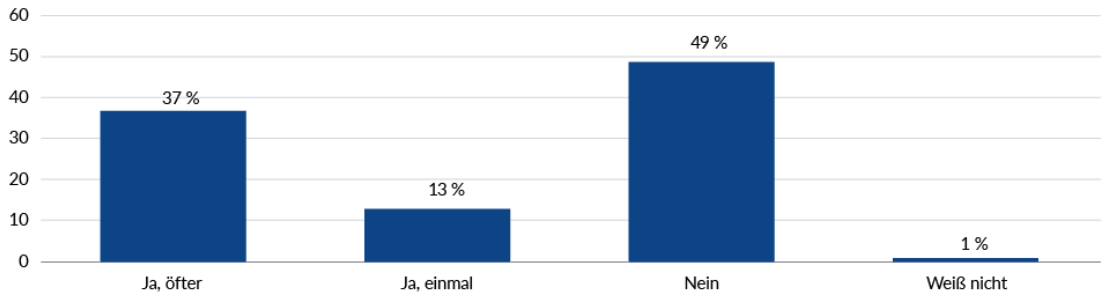
9 Betrugsprävention und -verhinderung benötigen ein Bündel an Maßnahmen

Die Zahlen des OeNB-Barometers 2025 zeigen, dass 50 % der Befragten (n = 2.054) angeben, in den letzten zwölf Monaten zumindest einmal mit einem Betrugsversuch konfrontiert gewesen zu sein.

Grafik 8

Ziel eines Betrugsversuchs in den letzten 12 Monaten

in Prozent der Befragten, n=2.054



Quelle: OeNB.

Deshalb ist ein wichtiger Teil der Betrugsprävention die Information und Sensibilisierung der Bürger:innen, um Betrugsversuche bereits bei der Kontaktaufnahme durch Betrüger:innen zu erkennen und somit zu verhindern. Ziel ist es, Verbraucher:innen zu befähigen, Warnsignale richtig einzuordnen, Zahlungsentscheidungen kritisch zu hinterfragen und sich wirksam vor Betrug zu schützen.

Infobox 5

Typische Warnsignale bei Betrugsversuchen

Unabhängig von der jeweiligen Betrugsmasche treten häufig ähnliche Warnsignale auf. Besondere Vorsicht ist insbesondere bei folgenden Anzeichen geboten:

- unrealistische Gewinn- oder Renditeversprechen,
- hoher Zeitdruck oder Aufforderungen zu sofortigem Handeln,
- Aufforderungen zur Geheimhaltung,
- Bitte um Weitergabe von Passwörtern, TANs oder Zugangsdaten,
- ungewöhnliche Zahlungswege (z. B. Kryptowerte oder Gutscheinkarten),
- Kontaktaufnahmen über ungewohnte Kommunikationskanäle,
- emotionale Manipulation durch Angst, Hilfsbereitschaft oder Mitleid.

Wer eines oder mehrere dieser Warnsignale erkennt, sollte die Echtheit der Kontaktaufnahme über offizielle Kommunikationswege überprüfen, keine sensiblen Daten preisgeben und keine Zahlungen vorschnell freigeben.

[7] Internet-Falle melden

Ein erheblicher Teil der Betrugsfälle beruht auf der gezielten Manipulation von Menschen. Betrüger:innen setzen dabei auf Zeitdruck, Angst, Liebe, Hilfsbereitschaft, Gewinnstreben oder vermeintliche Autorität, um ihre Opfer zur Preisgabe vertraulicher Daten oder zur Durchführung einer Zahlung zu bewegen. Häufig geben sie sich als Bankmitarbeiter:innen, Behördenvertreter:innen, Unternehmen oder Angehörige aus und nutzen täuschend echte E-Mails, SMS, Webseiten oder Telefonanrufe, um Vertrauen aufzubauen.

In diesen Fällen werden technische Sicherheitsmechanismen wie die starke Kund:innenauthentifizierung oder der IBAN-Namensabgleich nicht von Betrüger:innen überwunden. Die Zahlung wird vom Opfer selbst freigegeben und gilt damit als autorisiert. Auch technisch versierte Personen können unter Zeitdruck oder in emotional belastenden Situationen Opfer solcher Manipulationen werden.

Ein zentrales Instrument zur rechtzeitigen Aufdeckung betrügerischer Zahlungsvorgänge ist die Echtzeit-Überwachung von Transaktionen durch die Bank (Transaktionsmonitoring), das zunehmend durch KI unterstützt wird. Zahlungsdienstleister nutzen Transaktionsmonitoringsysteme, um Betrug frühzeitig zu erkennen und zu verhindern. Dies erfolgt durch die Analyse verschiedener Risikoindikatoren und die Erkennung auffälliger Abweichungen vom üblichen Zahlungsverhalten, die auf einen betrügerischen Zahlungsvorgang hindeuten können. Hierbei werden neben aktuellen und historischen Transaktionsdaten Geräteinformationen, Verhaltensdaten, geografische Auffälligkeiten sowie bekannte Betrugsmuster berücksichtigt. Werden verdächtige Zahlungen überprüft und gegebenenfalls erst nach einer zusätzlichen Bestätigung durch den Kunden bzw. die Kundin freigegeben, können zahlreiche Betrugsfälle verhindert werden.

Eine weitere wichtige Maßnahme zur Betrugsprävention ist der laufende Informationsaustausch zwischen Zahlungsdienstleistern, Behörden, Telekommunikationsunternehmen, sozialen Netzwerke und großen Plattformen.

Dieser breite Ansatz ist notwendig, da der Großteil der Betrugsanbahnung über Telekommunikationsdienste, das Internet und soziale Medien geschieht. Der Austausch von Daten und Erkenntnissen darf nicht an nationalen Grenzen Halt machen – denn auch Betrug kennt keine Ländergrenzen.

Darüber hinaus können Cooling-off-Perioden bei sicherheitsrelevanten Änderungen – z. B. bei der Registrierung neuer Geräte oder der Erhöhung von Zahlungslimits – einen zusätzlichen Schutz bieten, indem diese Änderungen nicht unmittelbar wirksam werden. Ergänzend leistet auch der IBAN-Namensabgleich („Verification of Payee“) einen wichtigen Beitrag zur Betrugsprävention (siehe Infobox 6). Eine wirksame Betrugsprävention erfordert das Zusammenspiel moderner Sicherheitstechnologien, leistungsfähiger Transaktionsmonitoringsysteme, eines effektiven Informationsaustauschs zwischen allen Teilnehmer:innen des Zahlungsökosystems sowie einer kontinuierlichen Sensibilisierung der Verbraucher:innen.

Infobox 6

IBAN-Namensabgleich (Überprüfung des Empfängers bzw. der Empfängerin)

Seit Oktober 2025 sind Banken dazu verpflichtet, vor der Freigabe einer Euro-Überweisung die Überprüfung des Empfängers bzw. der Empfängerin durchzuführen. Diese Prüfung soll über Unstimmigkeiten zwischen IBAN (früher: Kontonummer) und Name des hinterlegten Kontoinhabers bzw. der hinterlegten Kontoinhaberin informieren und damit fehlgeleitete Überweisungen und Betrug reduzieren.

Noch bevor eine Zahlung freigegeben wird, erhalten Nutzer:innen eine der folgenden Rückmeldungen:

- Vollständige Übereinstimmung: Der eingegebene Name stimmt mit dem Namen überein, der bei der IBAN als Kontoinhaber bzw. Kontoinhaberin hinterlegt ist.
- Teilweise Übereinstimmung: Der eingegebene Name stimmt mit dem Namen des Kontoinhabers bzw. der Kontoinhaberin nahezu überein. Bei kleinen Tippfehlern oder Namensvarianten kann diese Rückmeldung aufscheinen. Die Bank zeigt dann den vermuteten richtigen Kontoinhaber bzw. die richtige Kontoinhaberin zur Kontrolle an.
- Keine Übereinstimmung: Achtung! Der eingegebene Name stimmt nicht überein mit dem Namen des Kontoinhabers bzw. der Kontoinhaberin. Es wird eine Überprüfung der Daten dringend empfohlen, um Fehlüberweisungen und Betrugsversuche auszuschließen
- Durchführung der Überprüfung des Empfängers bzw. der Empfängerin nicht möglich: bei technischen Problemen oder bei einem Konto, das kein Zahlungskonto ist bzw. geografisch nicht durch die Überprüfung des Empfängers bzw. der Empfängerin abgedeckt ist.

Eine Überweisung kann vom Zahler bzw. von der Zahlerin unabhängig von der Rückmeldung freigegeben werden.

Bei welchen Betrugsarten kann der IBAN-Namensabgleich helfen, Betrug zu verringern?

1. **Von Zahler:innen autorisierter Überweisungsbetrug (APP-Betrug: „Authorized Push Payment Fraud"):** Betrüger:innen geben sich als Freund:in, Behörde oder Kund:innendienst aus und drängen zu schnellen Überweisungen. Der IBAN-Namensabgleich warnt, wenn Name und IBAN nicht zusammenpassen.
2. **Rechnungsbetrug:**
   Gefälschte Rechnungen mit manipulierten Kontodaten sehen täuschend echt aus. Besonders gefährlich: Oft basieren sie auf echter Kommunikation, z. B. aus entwendeten Rechnungen. Die Überprüfung des Empfängers bzw. der Empfängerin hilft, solche falschen Konten zu entlarven. Laut Finanzmarktaufsicht (FMA) war Rechnungsbetrug 2023 einer der häufigsten Betrugsfälle – mit durchschnittlich 56.000 EUR Schaden pro Fall.
3. **Identitätsbetrug durch Behördenvortäuschung:**
   Anrufe oder E-Mails angeblicher Behörden fordern zur sofortigen Zahlung auf. Der IBAN-Namensabgleich erkennt, wenn der eingegebene Name des Empfängers bzw. der Empfängerin nicht zu dem offiziellen Konto passt.

Achtung: Der IBAN-Namensabgleich kann nur prüfen, ob der eingegebene Name mit dem der IBAN zugeordneten Namen des Kontoinhabers bzw. der Kontoinhaberin übereinstimmt. Es kann jedoch vorkommen, dass eine Zahlungsaufforderung insgesamt betrügerisch ist und der eingegebene Name mit dem der IBAN zugeordneten Namen des Kontoinhabers bzw. der Kontoinhaberin übereinstimmt.

10 Schutz vor Betrug durch Information und Sensibilisierung

Da ein erheblicher Teil der Betrugsfälle auf sozialer Manipulation beruht, kommt der Information und Sensibilisierung der Bevölkerung eine zentrale Rolle bei der Betrugsprävention zu. Ziel ist es, Verbraucher:innen zu befähigen, Betrugsversuche frühzeitig zu erkennen, Warnsignale richtig einzuordnen und Zahlungsentscheidungen kritisch zu hinterfragen.

Infobox 7

So schützen Sie sich vor Betrug

Verbraucher:innen können durch ein sicherheitsbewusstes Verhalten wesentlich dazu beitragen, das Risiko eines Betrugs zu reduzieren.

- **Zahlungsaufforderungen kritisch hinterfragen:** Lassen Sie sich insbesondere bei Zeitdruck, außergewöhnlichen Zahlungsaufforderungen oder unrealistischen Gewinn- bzw. Renditeversprechen nicht zu vorschnellen Entscheidungen verleiten.
- **Empfänger:innen sorgfältig prüfen:** Kontrollieren Sie vor jeder Überweisung die Angaben des Empfängers bzw. der Empfängerin und beachten Sie Warnhinweise aus dem IBAN-Namensabgleich.
- **Keine vertraulichen Daten weitergeben:** Geben Sie Passwörter, PINs, TANs oder Freigaben für Zahlungen niemals auf Aufforderung Dritter weiter. Banken, Behörden oder andere seriöse Institutionen fragen diese Informationen weder telefonisch noch per E-Mail oder SMS ab.
- **Zusätzliche Authentifizierungsverfahren nutzen:** Verwenden Sie zusätzliche Sicherheitsverfahren wie biometrische Verfahren oder Authenticator-Apps, sofern diese angeboten werden. Prüfen Sie jede Zahlungsfreigabe sorgfältig und geben Sie Freigaben niemals auf Aufforderung Dritter frei.
- **Geräte und Anwendungen aktuell halten:** Installieren Sie Sicherheitsupdates für Betriebssysteme und Apps zeitnah und laden Sie Anwendungen ausschließlich aus offiziellen App-Stores oder von vertrauenswürdigen Quellen herunter.
- **Kontobewegungen regelmäßig kontrollieren:** Überprüfen Sie Konto- und Kreditkartenumsätze regelmäßig und informieren Sie Ihre Bank unverzüglich über verdächtige Transaktionen.
- **Identität von Anrufer:innen überprüfen:** Betrüger:innen geben sich häufig als Bankmitarbeiter:innen, Behörden, Unternehmen oder Angehörige aus. Überprüfen Sie die Identität einer Person immer über offiziell bekannte bzw. Ihnen persönlich bekannte Kontaktdaten.
- **Offizielle Kontaktwege nutzen:** Beenden Sie verdächtige Telefonate oder Nachrichten und nehmen Sie Kontakt mit Banken, Unternehmen oder Behörden ausschließlich über offiziell veröffentlichte Kontaktdaten auf.
- **Passwortmanager nutzen:** Verwenden Sie für unterschiedliche Online-Dienste jeweils individuelle Passwörter und verwalten Sie diese möglichst mit einem Passwortmanager.
- **Datensicherungen erstellen:** Sichern Sie wichtige Daten regelmäßig, damit diese nach einem Schadsoftwareangriff oder im Falle eines kompromittierten Geräts wiederhergestellt werden können.

Ergänzend zu den Informationsangeboten der OeNB auf ihrer Webseite sowie über ihre Social-Media-Kanäle stehen der Bevölkerung weitere vertrauenswürdige Informations- und Beratungsstellen zur Verfügung. Sie informieren über aktuelle Betrugsmaschen, veröffentlichen Warnhinweise und unterstützen Betroffene mit Beratung und konkreten Hilfestellungen. Um die Bevölkerung frühzeitig über neue Betrugsformen zu informieren, initiiert die OeNB zudem auch gemeinsam mit dem Bundesministerium für Inneres (BMI) Presseaussendungen zu aktuellen Betrugsmaschen und gibt konkrete Empfehlungen zum sicheren Bezahlen bzw. zum Schutz vor Betrug.[8]

Infobox 8

Informations- und Beratungsstellen

- **Oesterreichische Nationalbank (OeNB):** Informationen zum sicheren Zahlungsverkehr, aktuelle Betrugswarnungen und Prävention.[9]
- **Finanzmarktaufsicht (FMA):** Informationen zu Betrugsrisiken im Finanzbereich und Warnungen vor unseriösen Anbietern.[10,11]
- **Bundeskriminalamt (BK):** Informationen zu Cyberkriminalität und Prävention sowie Hinweise zur Anzeige von Betrugsfällen.[12]
- **Watchlist Internet:** Aktuelle Warnungen vor Phishing, Fake-Shops und weiteren Betrugsmaschen.[13]
- **onlinesicherheit.gv.at:** Informationsplattform der Republik Österreich zu den Themen Cybersicherheit, Internetkriminalität und digitale Sicherheit, einschließlich eines Überblicks über relevante Beratungs- und Meldestellen.[14]
- **Internet Ombudsstelle:** Beratung bei Problemen im Online-Handel sowie Unterstützung bei Internetbetrug.[15]
- **Arbeiterkammer (AK):** Informationen zu Konsumentenschutz, Online-Betrug, Fake-Shops und Unterstützung bei Verbraucher:innenfragen.[16]
- **Rundfunk und Telekom Regulierungs-GmbH (RTR):** Meldestelle für Rufnummernmissbrauch sowie unerwünschte elektronische Kommunikation.[17]

[8] Bundeskriminalamt und Nationalbank warnen vor Quishing - Oesterreichische Nationalbank (OeNB)

[9] Warnung – Betrugsversuche - Oesterreichische Nationalbank (OeNB)

[10] Startseite - Reden wir über Geld

[11] Warnungen - FMA Österreich

[12] Ansprechstellen zum Thema Cybersicherheit - Bundeskanzleramt Österreich

[13] Watchlist Internet – Online-Betrug, -Fallen & -Fakes im Blick

[14] Onlinesicherheit

[15] Internet Ombudsstelle | Kostenlose Streitschlichtung & Beratung in Österreich

[16] Achtung Falle | Arbeiterkammer Wien

[17] Meldestelle Rufnummernmissbrauch | RTR

© Oesterreichische Nationalbank, 2026. Alle Rechte vorbehalten.
Adresse: Otto-Wagner-Platz 3, 1090 Wien
Postfach 61, 1011 Wien
Website: www.oenb.at

Reproduktionen für nicht kommerzielle Verwendung, wissenschaftliche Zwecke und Lehrtätigkeit sind unter Nennung der Quelle freigegeben.

Die in dieser Studie zum Ausdruck gebrachte Meinung gibt nicht notwendigerweise die Meinung der Oesterreichischen Nationalbank oder des Eurosystems wieder.

Die Autor:innen der OeNB verwenden grundsätzlich inklusive Sprache. Bei etablierten Fachwörtern und Wendungen, die (auch) juristische Personen bezeichnen, kann es jedoch fallweise vorkommen, dass aus Gründen der Klarheit und Lesbarkeit darauf verzichtet wird.

Datenschutzinformationen: www.oenb.at/datenschutz
ISSN 2960-5075 (online)