

TRADING ODER TRADING-BETRUG?

Die 250-Euro-Masche, virtuelle Gewinne, blockierte Auszahlungen und der zweite Angriff durch angebliche „Recovery“-Retter

Verbraucherbroschüre 2026

Die wichtigste Warnung

Wenn eine Plattform Ihnen hohe Gewinne zeigt, heißt das noch lange nicht, dass dieses Geld existiert. Bei betrügerischen Plattformen sind Kontostand, Kurse und Gewinne häufig nur Zahlen auf einem Bildschirm. Wer die Auszahlung verlangt, erlebt dann den eigentlichen Betrug.

Zwei völlig verschiedene Risiken

Fake-Trading: Es findet oft überhaupt kein echter Handel statt - die Gewinnchance ist faktisch null. Legales, hochspekulatives CFD-Trading: Es findet echter Handel statt, aber laut ESMA verlieren typischerweise 74 bis 89 Prozent der Kleinanlegerkonten Geld.

Diese Broschüre erklärt die typische Betrugschance und zeigt, wie Betroffene reagieren sollten. Sie ersetzt keine individuelle Rechts-, Anlage- oder Steuerberatung.

Das Wichtigste in 90 Sekunden

Trading-Betrug ist heute professionell organisiert. Die Webseiten sehen seriös aus, die „Broker“ sprechen gutes Deutsch, die Charts bewegen sich, und auf dem Bildschirm wächst das Guthaben. Genau darin liegt die Gefahr: Die technische Oberfläche kann vollkommen überzeugend wirken, obwohl im Hintergrund gar kein echter Handel stattfindet.

- 250 Euro sind häufig nur der Türöffner. Der Betrag ist bewusst niedrig, damit die Hemmschwelle fällt.
- Nach der ersten Einzahlung meldet sich ein „persönlicher Berater“ und baut Vertrauen auf.
- Das angebliche Handelskonto zeigt schnell Gewinne. Diese können frei erfunden oder manipuliert sein.
- Danach soll mehr Geld folgen - oft 5.000, 20.000, 50.000 Euro oder mehr.
- Bei der Auszahlung erscheinen plötzlich „Steuern“, „Versicherungen“, „Liquiditätsnachweise“, „AML-Gebühren“ oder andere Fantasieposten.
- Wer nicht weiterzahlt, wird unter Druck gesetzt oder verliert den Kontakt zur Plattform.
- Später meldet sich häufig ein angeblicher Anwalt, Ermittler, Blockchain-Experte oder „Recovery Service“, der das verlorene Geld gegen Vorkasse zurückholen will. Das kann der zweite Betrug sein.

Faustregel

Eine seriöse Auszahlung wird nicht dadurch freigeschaltet, dass Sie vorher immer neue Gelder auf fremde Konten oder Krypto-Wallets überweisen. Wer Ihnen sagt, Sie müssten erst „Steuern“, „Gebühren“ oder eine „Sicherheitsleistung“ zahlen, damit Ihr angebliches Guthaben freikommt, liefert ein massives Warnsignal.

1. Trading ist nicht gleich Trading

Der Begriff „Trading“ wird für sehr unterschiedliche Dinge verwendet. Wer die Risiken verstehen will, muss zuerst drei Welten auseinanderhalten.

Form	Was passiert tatsächlich?	Typisches Risiko

Langfristiges Investieren	Kauf realer Wertpapiere, z. B. breit gestreuter Fonds oder ETFs, mit langem Zeithorizont.	Marktschwankungen und Verluste sind möglich, aber der Ansatz unterscheidet sich grundlegend vom kurzfristigen Spekulieren.
Spekulatives Trading	Kurzfristige Wetten auf Kursbewegungen, häufig mit Hebel, CFDs, Forex, Optionen oder Kryptowerten.	Hohe Schwankungen, Kosten, Hebelwirkung und emotionaler Entscheidungsdruck. Ein großer Teil der Kleinanleger verliert Geld.
Fake-Trading / Cybertrading-Betrug	Die Plattform täuscht Handel nur vor. Zahlen, Charts und Gewinne können vollständig manipuliert sein.	Das eingezahlte Geld wird nicht wie behauptet investiert. Die „Rendite“ existiert nur auf dem Bildschirm.

Die Verbraucherzentrale beschreibt bei betrügerischen Plattformen ausdrücklich, dass Kurse und Gewinne vollständig gefälscht sein können und der Kontakt typischerweise abbricht, sobald keine weiteren Einzahlungen erfolgen oder eine Auszahlung verlangt wird.

Quelle: Verbraucherzentrale, „Online-Trading: So entlarven Sie Betrüger“, Stand 2. Dezember 2025.

2. Die 250-Euro-Masche: Warum der Einstieg so billig wirkt

Die ersten 250 Euro sind psychologisch clever gewählt. Der Betrag ist für viele Menschen schmerzhaft, aber noch nicht existenzbedrohend. Genau deshalb eignet er sich als Vertrauensprobe. Wer einmal gezahlt hat, ist emotional und organisatorisch im System.

Kein Zufall

Die Verbraucherzentralen nennen 250 Euro ausdrücklich als typischen Einstiegsbetrag. Auch die BaFin warnte vor hunderten nahezu identischen „Investieren mit KI“-Webseiten, die mit einem Mindesteinsatz von 250 Euro warben.

1. Werbung: Eine Anzeige verspricht „KI-Trading“, Krypto-Gewinne, automatisierte Systeme oder geheime Strategien. Häufig werden Prominente, Nachrichtensendungen oder bekannte Marken missbraucht.

2. Datensammlung: Interessenten hinterlassen Name, Telefonnummer, E-Mail-Adresse und oft weitere persönliche Angaben.
3. Sofortiger Anruf: Ein angeblicher Broker oder Account Manager meldet sich schnell. Freundlich, professionell, verbindlich.
4. Erste Einzahlung: 250 Euro sollen „zum Test“ reichen. Das senkt die Angst und schafft einen ersten finanziellen Anker.
5. Schneller Erfolg: Auf dem Dashboard werden schon nach kurzer Zeit Gewinne angezeigt. Das Opfer soll denken: Es funktioniert wirklich.
6. Eskalation: Nun heißt es, mit 250 Euro sei das Potenzial zu klein. Für „echte Gewinne“ brauche es 5.000, 10.000 oder 25.000 Euro.

Warum Menschen danach immer weiter einzahlen

Der Betrug arbeitet nicht nur mit Technik, sondern mit Psychologie. Wer bereits Geld überwiesen hat und scheinbare Gewinne sieht, will die gute Entscheidung bestätigen. Gleichzeitig entsteht Angst, eine angeblich einmalige Chance zu verpassen. Hinzu kommt persönlicher Kontakt: Der „Berater“ kennt Beruf, Familie, Pläne und finanzielle Situation. Aus einem anonymen Investment wird eine Beziehung - und genau diese Beziehung wird ausgenutzt.

- Autorität: „Ich mache das seit 15 Jahren.“
- Knappheit: „Dieses Fenster schließt heute.“
- Sozialer Beweis: „Meine anderen Kunden verdienen bereits.“
- Verlustangst: „Wenn Sie jetzt nicht nachschießen, verlieren Sie die Position.“
- Schuld und Druck: „Ich habe für Sie einen Bonus freigeschaltet - jetzt müssen Sie mitziehen.“
- Isolation: „Sprechen Sie mit niemandem darüber, Banken verstehen Krypto nicht.“

3. Virtuelles Guthaben: Wenn 83.420 Euro nur eine Zahl sind

Einer der wirksamsten Tricks ist das gefälschte Handelskonto. Das Opfer sieht Charts, offene Positionen, Gewinne, Kontostände und manchmal sogar scheinbar echte Transaktionslisten. Das Problem: Eine professionell aussehende Benutzeroberfläche beweist weder, dass ein Broker reguliert ist, noch dass die gezeigten Trades tatsächlich an einem Markt ausgeführt wurden.

Der entscheidende Denkfehler

„Ich sehe das Geld auf meinem Konto“ ist bei einer Fake-Plattform keine Sicherheit. Ein Betrüger kontrolliert die Anzeige. Aus 10.000 Euro kann er per Mausklick 27.000 Euro machen - ohne dass auch nur ein Cent real erwirtschaftet wurde.

Nach Angaben der Polizei können eigens erstellte Fake-Anlageplattformen den Eindruck echten Tradings erzeugen. Der Handel wird vorgetäuscht; das eingezahlte Geld verschwindet stattdessen in kriminellen Netzwerken. Teilweise werden anfangs sogar kleine Beträge ausgezahlt, um Vertrauen aufzubauen.

Quelle: Polizeiliche Kriminalprävention, „Cybertrading-Betrug: Checkliste für den Ernstfall“, 2026.

Die kleine Auszahlung als Köder

Manchmal erhält ein Opfer tatsächlich 100 oder 200 Euro zurück. Das kann absichtlich geschehen. Die Auszahlung soll beweisen, dass das System funktioniert. Psychologisch ist sie extrem wirksam: Wer einmal Geld zurückbekommen hat, ist eher bereit, später 20.000 Euro zu überweisen. Die kleine Auszahlung ist dann kein Gewinn, sondern Marketingbudget des Betrugs.

4. Die Auszahlungsfalle: Plötzlich fehlen „Steuern“, „Gebühren“ oder „Sicherheiten“

Der Betrug wird meist erst sichtbar, wenn das Opfer sein Geld zurückhaben will. Dann beginnt eine neue Geschichte. Der angebliche Gewinn sei vorhanden - aber leider blockiert.

- „Kapitalertragsteuer“ müsse vorab direkt an die Plattform gezahlt werden.
- Eine „Geldwäsche-Sicherheitsleistung“ müsse hinterlegt werden.
- Es fehle eine „Liquiditätsbestätigung“ oder „Proof of Funds“.
- Für die „Blockchain-Freigabe“ sei eine Netzwerkgebühr nötig.
- Ein angeblicher Versicherer verlange eine Prämie vor Auszahlung.
- Das Konto müsse zunächst auf ein „Premium-Level“ hochgestuft werden.
- Eine Margin-Lücke müsse geschlossen werden, sonst verfalle das Guthaben.
- Eine ausländische Behörde habe das Geld eingefroren und verlange eine „Freigabegebühr“.

Wichtig

Bei einem seriösen Anbieter werden legitime Gebühren transparent vertraglich vereinbart und nicht spontan erfunden, sobald Sie Ihr Geld abziehen wollen. Steuern werden nicht dadurch „freigeschaltet“, dass Sie Geld auf ein privates Konto, ein fremdes IBAN-Konto oder eine Krypto-Wallet senden.

Warum die Betrüger immer neue Gründe erfinden

Weil der angezeigte Gewinn häufig gar nicht existiert. Es gibt nichts auszusahlen. Jede neue „Gebühr“ dient nur dazu, noch einmal Geld zu erhalten. Wer 10.000 Euro verloren hat, ist besonders anfällig für die Hoffnung, mit weiteren 2.000 Euro doch noch alles zu retten. Genau diese Hoffnung wird monetarisiert.

5. Fernzugriff: Wenn der „Broker“ plötzlich auf Ihrem Computer sitzt

Eine besonders gefährliche Stufe beginnt, wenn der angebliche Berater Software für Fernzugriff installieren lassen will. Begründungen klingen harmlos: Er wolle das Trading-Programm einrichten, bei der Banküberweisung helfen oder die Krypto-Wallet konfigurieren.

Tatsächlich kann Fernzugriff Kriminellen ermöglichen, Bildschirminhalte mitzulesen, Onlinebanking zu beobachten, Zugangsdaten abzugreifen oder Überweisungen vorzubereiten. Wer eine solche Software installiert hat, sollte nach einem Betrugsverdacht nicht einfach weiterarbeiten, sondern Bankzugänge sichern und das Gerät technisch überprüfen lassen.

- Keine TAN, PIN oder vollständigen Zugangsdaten am Telefon nennen.
- Keine Fernwartungssoftware auf Anweisung eines Anlagevermittlers installieren.
- Keine Überweisung ausführen, nur weil der „Berater“ den Bildschirm mitverfolgt.
- Wenn Fernzugriff bereits bestand: Verbindung trennen, Bank informieren, Passwörter von einem sauberen Gerät ändern und Gerät prüfen lassen.

6. Krypto als Geldschleuder: Warum Wallets bei Betrügern beliebt sind

Viele Fake-Trading-Netzwerke wechseln nach der ersten Zahlung zu Kryptowerten. Das Opfer soll Bitcoin, USDT oder andere Kryptowerte kaufen und an eine Wallet senden. Für Betrüger hat das Vorteile: Transaktionen lassen sich grenzüberschreitend schnell weiterleiten, und Rückbuchungen sind anders als bei Kartenzahlungen oder manchen Banktransfers meist nicht einfach möglich.

Achtung vor der Formulierung „Ihr Geld liegt auf der Blockchain“

Die Blockchain ist kein Tresor, in dem ein Kundenkonto auf Freigabe wartet. Wenn jemand behauptet, Sie müssten erst eine „Blockchain-Steuer“ oder „Wallet-Aktivierungsgebühr“ zahlen, ist äußerste Vorsicht geboten.

7. Der große „Recovery“-Retter: Der Betrug nach dem Betrug

Viele Opfer werden Wochen oder Monate später ein zweites Mal kontaktiert. Diesmal klingt die Geschichte völlig anders: Eine Kanzlei, eine Ermittlungsfirma,

ein Blockchain-Forensiker, ein „Asset Recovery Team“, eine Behörde oder ein angeblicher Insolvenzverwalter habe das verlorene Geld gefunden.

Warum trifft der zweite Betrug so genau?

Weil die Täter Ihre Daten bereits kennen. Entweder steckt dasselbe Netzwerk dahinter oder Opferdaten wurden an andere Kriminelle weiterverkauft. Der neue Anrufer kennt oft Plattformname, Verlusthöhe, Telefonnummer und sogar frühere Zahlungen. Genau dieses Wissen soll Seriosität vortäuschen.

Typischer Ablauf eines Recovery-Scams

1. Kontakt aus dem Nichts: „Wir haben Ihre Akte übernommen.“
2. Gute Nachricht: „Ihr Geld wurde gefunden / eingefroren / auf einer Wallet identifiziert.“
3. Autorität: Der Anrufer nennt angebliche Aktenzeichen, Behörden, Kanzleien oder internationale Ermittler.
4. Zeitdruck: „Sie haben nur 48 Stunden, sonst fällt das Geld an den Staat.“
5. Vorkasse: Für Gericht, Versicherung, Steuer, Übersetzung, AML-Prüfung, Wallet-Freigabe oder Provision soll vorab gezahlt werden.
6. Neue Forderungen: Nach jeder Zahlung taucht das nächste Hindernis auf.
7. Ende: Geld kommt nicht zurück, der „Retter“ verschwindet ebenfalls.

Die britische Finanzaufsicht FCA warnt ausdrücklich vor solchen „Recovery Room Scams“: Betrugsoffer werden kontaktiert und sollen für die angebliche Rückholung ihres Geldes zunächst Gebühren zahlen. Die Täter des ursprünglichen Anlagebetrugs können selbst hinter dem Recovery-Angebot stehen oder Opferdaten weitergeben.

Quelle: Financial Conduct Authority (FCA), „Recovery room scams“, zuletzt aktualisiert 19. Januar 2026.

Auch die BaFin warnte bereits vor gefälschten Zahlungsaufforderungen in ihrem Namen, bei denen Opfer nicht lizenzierter Online-Handelsplattformen Geld überweisen sollten, um angeblich verlorene Gelder zurückzuerhalten.

Quelle: BaFin, „Betrug: BaFin warnt vor gefälschten Zahlungsaufforderungen“, 25. März 2022.

8. Und wenn die Plattform seriös ist? Warum echtes Trading trotzdem extrem schwer ist

Nicht jede Trading-Plattform ist Betrug. Aber auch bei einem regulierten Anbieter ist kurzfristiges, gehebeltes Trading keine einfache Einkommensquelle. Die

zentrale Unterscheidung lautet: Ein seriöser Broker kann korrekt arbeiten - und der Kunde kann trotzdem sehr viel Geld verlieren.

Die nüchterne Statistik

Bei CFDs zeigen Auswertungen europäischer Aufsichtsbehörden, dass typischerweise 74 bis 89 Prozent der Kleinanlegerkonten Geld verlieren. Die ESMA nennt durchschnittliche Verluste von etwa 1.600 bis 29.000 Euro je Anleger in den untersuchten Märkten.

Quelle: ESMA, Product Intervention Measures zu CFDs und binären Optionen; Analysen nationaler Aufsichtsbehörden in mehreren EU-Staaten.

Warum verlieren so viele?

- Hebel: Kleine Kursbewegungen können große Verluste verursachen. Ein Hebel von 20 verstärkt nicht nur Gewinne, sondern auch Verluste.
- Spread und Gebühren: Jeder Trade startet häufig mit Kosten. Viele kurzfristige Trades summieren diese Belastung.
- Finanzierungskosten: Über Nacht gehaltene gehebelte Positionen können laufende Kosten verursachen.
- Volatilität: Kurse können schneller springen, als ein unerfahrener Trader reagiert.
- Psychologie: Angst, Gier, Verlustaversion und „Rache-Trades“ zerstören selbst vernünftige Strategien.
- Informationsnachteil: Privatanleger konkurrieren mit professionellen Marktteilnehmern, schnellen Systemen und großen Datenmengen.
- Overtrading: Ständiges Handeln fühlt sich produktiv an, erhöht aber häufig nur Kosten und Fehlerquote.
- Keine belastbare Strategie: Einzelne Gewinne werden mit Können verwechselt, obwohl Zufall eine große Rolle spielen kann.

Ein einfaches Hebel-Beispiel

Sie setzen 1.000 Euro eigenes Kapital ein und bewegen mit Hebel 20 eine Position von 20.000 Euro. Bewegt sich der Markt nur 5 Prozent gegen Sie, entspricht das rechnerisch 1.000 Euro Verlust - Ihr eingesetztes Kapital kann damit praktisch aufgebraucht sein. Schutzmechanismen können das Risiko begrenzen, ändern aber nichts daran, dass Hebel Verluste massiv beschleunigt.

Trading ist kein Sparplan

Wer Vermögen langfristig aufbauen will, verfolgt meist ein anderes Ziel als ein Daytrader. Langfristiges, breit gestreutes Investieren und kurzfristiges Spekulieren sollten gedanklich und finanziell strikt getrennt werden.

9. Die 25 Warnsignale, bei denen Sie sofort bremsen sollten

- | | |
|---|---|
| 1. Unaufgeforderter Anruf oder WhatsApp-Kontakt nach einer Online-Anzeige. | 2. „Schon ab 250 Euro“ kombiniert mit außergewöhnlich hohen Gewinnen. |
| 3. Werbung mit Prominenten, TV-Shows oder Nachrichtenseiten, die Sie nicht unabhängig bestätigen können. | 4. Garantierte Gewinne oder angeblich „risikofreie“ Strategien. |
| 5. Ein „persönlicher Broker“ drängt auf schnelle Einzahlungen. | 6. Zeitdruck: „Nur heute“, „letzte Chance“, „Position läuft aus“. |
| 7. Der Anbieter sitzt in einem Offshore-Staat oder nennt wechselnde Firmenanschriften. | 8. Kein überprüfbares Impressum oder widersprüchliche Firmendaten. |
| 9. Lizenznummer lässt sich im Register der genannten Behörde nicht finden. | 10. Der Name der Firma passt nicht zum Kontoinhaber der Überweisung. |
| 11. Zahlung auf Privatkonten oder ständig wechselnde IBANs. | 12. Zahlung in Kryptowerten an unbekannte Wallet-Adressen. |
| 13. Installation von Fernzugriffssoftware wird verlangt. | 14. Der „Berater“ will Zugang zu Ihrem Onlinebanking sehen. |
| 15. Das Dashboard zeigt ungewöhnlich gleichmäßige Gewinne. | 16. Schon wenige Tage nach Einstieg wird massiver Profit angezeigt. |
| 17. Für eine Auszahlung müssen Sie erst weiteres Geld einzahlen. | 18. „Steuern“ sollen direkt an den Broker oder auf eine Krypto-Wallet gezahlt werden. |
| 19. Es wird eine „Anti-Geldwäsche-Gebühr“ oder „Freigabesicherheit“ verlangt. | 20. Der Ansprechpartner wechselt ständig oder Telefonnummern funktionieren nicht mehr. |
| 21. Sie sollen gegenüber Ihrer Bank einen falschen Verwendungszweck nennen. | 22. Sie sollen Ihre Bank oder Familie nicht über das Investment informieren. |
| 23. Nach Verlust meldet sich ungefragt ein „Recovery“-Dienst. | 24. Der Recovery-Dienst kennt erstaunlich viele Details Ihres alten Falls. |
| 25. Auch der Recovery-Dienst verlangt Vorkasse, bevor angeblich Geld freigegeben wird. | |

10. So prüfen Sie einen Anbieter, bevor auch nur 1 Euro fließt

1. Unternehmensname exakt notieren - nicht nur Markenname oder Webseitenname.
2. Impressum, Handelsregisterdaten, Geschäftsanschrift und Geschäftsführung prüfen.
3. Bei Finanzdienstleistungen in Deutschland die BaFin-Unternehmensdatenbank und aktuelle Warnmeldungen prüfen.
4. Bei angeblich ausländischer Regulierung direkt im Register der genannten Aufsicht suchen - nicht auf einen Screenshot oder Link des Anbieters vertrauen.
5. Domainalter und Domaininhaber prüfen, soweit verfügbar. Eine „20 Jahre alte Investmentfirma“ mit einer drei Wochen alten Webseite ist verdächtig.
6. Telefonnummern, E-Mail-Domains und Kontoinhaber vergleichen. Abweichungen hinterfragen.
7. Geschäftsmodell erklären lassen: Was wird konkret gekauft? Wo wird es verwahrt? Wer ist Vertragspartner? Welche Kosten entstehen?
8. Auszahlungsbedingungen vor Einzahlung lesen. Formulierungen zu Bonus, Mindestumsatz, Margin oder Freigabe kritisch prüfen.
9. Eine unabhängige zweite Person einbeziehen. Betrug funktioniert besonders gut in Isolation.
10. Nie Geld investieren, dessen Verlust Miete, Lebenshaltung, Altersvorsorge oder Notfallreserve gefährden würde.

BaFin-Warnhinweis

Wer in Deutschland erlaubnispflichtige Finanz-, Wertpapier- oder Kryptowerte-Dienstleistungen anbietet, benötigt grundsätzlich eine entsprechende Erlaubnis. Die BaFin rät bei Internet-Geldanlagen zu besonderer Vorsicht und dazu, Anbieter vorab zu prüfen.

11. Schon eingezahlt? Jetzt zählt Geschwindigkeit

Scham ist in dieser Situation fehl am Platz. Professionelle Betrugsnetzwerke leben davon, glaubwürdig zu wirken. Entscheidend ist jetzt nicht, warum Sie gezahlt haben, sondern wie schnell Sie weitere Schäden begrenzen.

1. Sofort keine weiteren Zahlungen leisten - auch nicht für angebliche Steuern, Freigaben oder Recovery.
2. Bank, Kreditkartenanbieter oder Zahlungsdienst unverzüglich kontaktieren. Prüfen lassen, ob Überweisungsrückruf, Chargeback oder Sperrmaßnahmen noch möglich sind.
3. Bei Krypto-Zahlungen die verwendete Börse oder den Zahlungsdienst informieren und Transaktions-IDs sowie Empfänger-Wallets sichern.

4. Onlinebanking, E-Mail und wichtige Konten absichern. Passwörter von einem vertrauenswürdigen, sauberen Gerät ändern; Zwei-Faktor-Authentifizierung aktivieren.
5. Wenn Fernzugriff installiert wurde: Verbindung trennen, Software entfernen beziehungsweise Gerät fachkundig prüfen lassen. Bank über möglichen Fremdzugriff informieren.
6. Beweise sichern: Screenshots, Webseiten, Chatverläufe, E-Mails, Telefonnummern, Namen, IBANs, Wallet-Adressen, Zahlungsbelege, Transaktions-Hashes, Verträge.
7. Strafanzeige bei Polizei oder Staatsanwaltschaft erstatten. Möglichst strukturiert alle Zahlungswege und Kontaktpersonen dokumentieren.
8. Bei Verdacht auf unerlaubte Finanzdienstleistungen die BaFin informieren und Warnlisten prüfen.
9. Kredit- und Identitätsmissbrauch beobachten, wenn Ausweiskopien oder Bankdaten übermittelt wurden.
10. Bei größeren Schäden fachkundige anwaltliche Beratung erwägen - aber auch dort Identität, Kanzleisitz und Zulassung unabhängig prüfen.

Nicht noch einmal zahlen

Der häufigste Folgefehler ist der Versuch, einen bereits hohen Verlust mit „nur noch einer letzten Zahlung“ zu retten. Genau diese letzte Zahlung gibt es bei Betrügern nicht. Nach der nächsten Forderung kommt meist die übernächste.

12. So prüfen Sie angebliche Geldretter

- Wer hat Sie beauftragt und woher besitzt die Person Ihre Daten?
- Wie lautet der vollständige Firmen- oder Kanzleiname?
- Ist die Kanzlei im offiziellen Anwaltsverzeichnis auffindbar?
- Existiert die behauptete Behörde wirklich und stimmt die Telefonnummer auf deren offizieller Website?
- Warum soll eine Gebühr im Voraus gezahlt werden?
- Warum kann die Gebühr nicht aus dem angeblich bereits sichergestellten Geld beglichen werden?
- Wohin soll gezahlt werden? Passt der Kontoinhaber zur Firma?
- Warum wird Krypto verlangt?
- Gibt es ein überprüfbares Aktenzeichen bei einer realen Behörde?
- Kann die Information unabhängig über die offizielle Telefonnummer der Behörde bestätigt werden?

Goldene Regel für Recovery

Wer ungefragt anruft, verspricht, verlorenes Trading-Geld sicher zurückzuholen, und dafür zunächst eine Gebühr verlangt, sollte wie ein potenzieller Betrüger behandelt werden - bis seine Identität und Berechtigung unabhängig bestätigt sind.

13. Beispiel: Wie aus 250 Euro ein Schaden von 48.000 Euro werden kann

Das folgende Beispiel ist fiktiv, entspricht aber typischen Mustern aus Verbraucherwarnungen.

Tag 1	Anzeige: „KI macht aus 250 Euro ein Zusatzeinkommen.“ Registrierung und erste Einzahlung.
Tag 3	Dashboard zeigt 312 Euro. Berater gratuliert und empfiehlt 2.500 Euro „Arbeitskapital“.
Woche 2	Kontostand angeblich 7.900 Euro. Eine kleine Auszahlung von 150 Euro funktioniert - Vertrauen steigt.
Woche 3	„Exklusive Position“: weitere 10.000 Euro. Auf dem Bildschirm wächst das Guthaben auf 31.000 Euro.
Woche 5	Berater behauptet, für eine größere Auszahlung müsse die Kontoklasse aufgewertet werden. Weitere 15.000 Euro.
Woche 6	Angebliches Guthaben: 78.000 Euro. Bei Auszahlungswunsch werden 6.800 Euro „Steuer“ verlangt.
Woche 7	Nach Zahlung fehlen plötzlich 4.500 Euro „AML-Sicherheit“. Danach ist der Broker nicht mehr erreichbar.
Monat 3	Ein „Recovery Lawyer“ meldet sich und behauptet, 65.000 Euro seien auf einer Wallet eingefroren. Für die Freigabe verlangt er 9.000 Euro. Zweiter Betrugsversuch.

Der entscheidende Punkt: Die 78.000 Euro auf dem Bildschirm waren nie ein Vermögen des Opfers. Real war nur das Geld, das tatsächlich überwiesen wurde.

14. Zehn eiserne Regeln gegen Trading-Betrug

1. Keine Geldanlage aufgrund eines unerwarteten Anrufs, einer Messenger-Nachricht oder einer Social-Media-Anzeige abschließen.
2. 250 Euro als „Testbetrag“ nicht verharmlosen - er ist oft der Einstieg in eine Eskalationsstrategie.
3. Garantierte oder fast sichere hohe Renditen als Alarmzeichen behandeln.

4. Keinem Anlageberater Fernzugriff auf Computer oder Smartphone geben.
5. Keine TAN, PIN, Wallet-Seed-Phrase oder vollständigen Onlinebanking-Daten weitergeben.
6. Lizenz immer im offiziellen Register prüfen, nicht anhand von PDFs oder Screenshots des Anbieters.
7. Kontostand auf einer unbekannten Plattform niemals mit real verfügbarem Geld gleichsetzen.
8. Für eine Auszahlung keine spontanen „Steuern“, „Sicherheiten“ oder „Freigabengebühren“ nachschießen.
9. Nach einem Betrug besonders misstrauisch gegenüber Recovery-Angeboten sein.
10. Bei Verdacht sofort stoppen, dokumentieren, Bank informieren und Anzeige erstatten.

15. Quellen und weiterführende Hinweise

Die folgenden Quellen wurden für die Einordnung der typischen Betrugsmuster und der Trading-Risiken herangezogen. Abrufstand: 13. September 2026.

Verbraucherzentrale: Online-Trading: So entlarven Sie Betrüger

<https://www.verbraucherzentrale.de/wissen/geld-versicherungen/sparen-und-anlegen/onlinetrading-so-entlarven-sie-betrueger-104167>

Verbraucherzentrale: Vorsicht: Betrügerisches Online-Trading

<https://www.verbraucherzentrale.de/warnungen/vorsicht-betruegerisches-onlinetrading-54699>

Verbraucherzentrale: Investment-Angebote auf Social Media - schnelles Geld oder große Pleite?

<https://www.verbraucherzentrale.de/wissen/geld-versicherungen/sparen-und-anlegen/investmentangebote-auf-social-media-schnelles-geld-oder-grosse-pleite-63629>

BaFin: Warnung vor Plattformreihe „Investieren mit KI“ - mehr als 700 nahezu identische Websites, häufig 250 Euro Mindesteinsatz

https://bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/unerlaubte/2025/meldung_2025_06_03_Investieren_mit_KI_en.html

BaFin / BKA / Landeskriminalämter: Warnung vor Abzocke bei Geldanlagen im Internet

https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_schreiben_warnung_bafin_bka.pdf?__blob=publicationFile&v=2

Polizeiliche Kriminalprävention: Cybertrading-Betrug: Checkliste für den Ernstfall

<https://www.polizei-beratung.de/medienangebot/detail/download/35436/type-100015/>

ESMA: Product intervention measures relating to CFDs and binary options - 74-89 % der Retail-CFD-Konten verlieren typischerweise Geld

https://www.esma.europa.eu/sites/default/files/library/esma35-43-1000_additional_information_on_the_agreed_product_intervention_measures_relating_to_contracts_for_differences_and_binary_options.pdf

FCA: Recovery room scams

<https://www.fca.org.uk/consumers/recovery-room-scams>

BaFin: Betrug: Warnung vor gefälschten Zahlungsaufforderungen im Namen der BaFin

https://bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2022/meldung_2022_03_25_Warnung_gefaelschte_Zahlungsaufforderung.html

Hinweis zur Statistik

Die ESMA-Zahl von 74 bis 89 Prozent bezieht sich auf CFD-Konten von Kleinanlegern in den von europäischen Aufsichtsbehörden untersuchten Märkten. Sie ist keine pauschale Quote für jede Form des Wertpapierhandels. Sie zeigt aber, wie hoch das Verlustrisiko bei gehebeltem, kurzfristigem Retail-Trading sein kann.

Schlussgedanke

Die gefährlichste Illusion beim Trading-Betrug ist nicht der angebliche Gewinn. Es ist das Gefühl, die Situation noch mit einer letzten Zahlung retten zu können. Genau an diesem Punkt verdienen Betrüger häufig das meiste Geld. Wer den Mechanismus erkennt, kann die Kette unterbrechen: nicht weiterzahlen, Beweise sichern, Zahlungswege melden und jede spätere „Rettung“ unabhängig überprüfen.

Stand: 13. September 2026. Verbraucherinformation - keine individuelle Anlage-, Rechts- oder Steuerberatung.