Verbraucherzentrale
Bayern

Gemeinsam stark gegen Anlagebetrug im Internet

Auswertung: Fast 2.000 Verbraucher nutzten neues Tool der Verbraucherzentrale

7. April 2026

1. Verbraucherrelevanz

Mit dem „**Fake-Check Geldanlage**" können Verbraucherinnen und Verbrauchern verdächtige Geldanlageangebote anhand konkreter Warnsignale online selbst überprüfen. Im Zeitraum vom 25.01.2026 bis 31.3.2026 wurden insgesamt **1.964 Checks** durchgeführt. Das Tool wird durchgehend und mit wechselnder Frequenz genutzt. Die Datenlage zeigt wöchentliche Schwankungen, aber einen stabilen Basistrend.

Der Fake-Check Geldanlage wird stark nachgefragt und zeigt auf, wo die größten Betrugsrisiken liegen. Besonders Kryptowährungen, Copy-Trading, CFDs und Forex prägen die Beschwerdelage; klassische Produkte wie Festgeld, Tagesgeld oder ETF tauchen ebenfalls auf und dienen Betrügern in etlichen Fällen als seriös wirkende Tarnung. Zugleich zeigt die Auswertung, dass ein erheblicher Teil der Betroffenen bereits Geld eingezahlt hat. Der Fake-Check erreicht Menschen sowohl präventiv, als auch mitten im Schadensprozess.

Die Auswertung der Daten zeichnet ein besorgniserregendes Bild: Kryptobetrug dominiert, angebliche Testimonials wie Prominente oder TV-Formate werden systematisch für Produktwerbung missbraucht und jede vierte Person, die den Check gemacht hat, hat bereits Geld verloren. Typische Warnzeichen sind schnelle Gewinne, Zeitdruck, Promi-Werbung und der Missbrauch bekannter Medien oder Behörden.

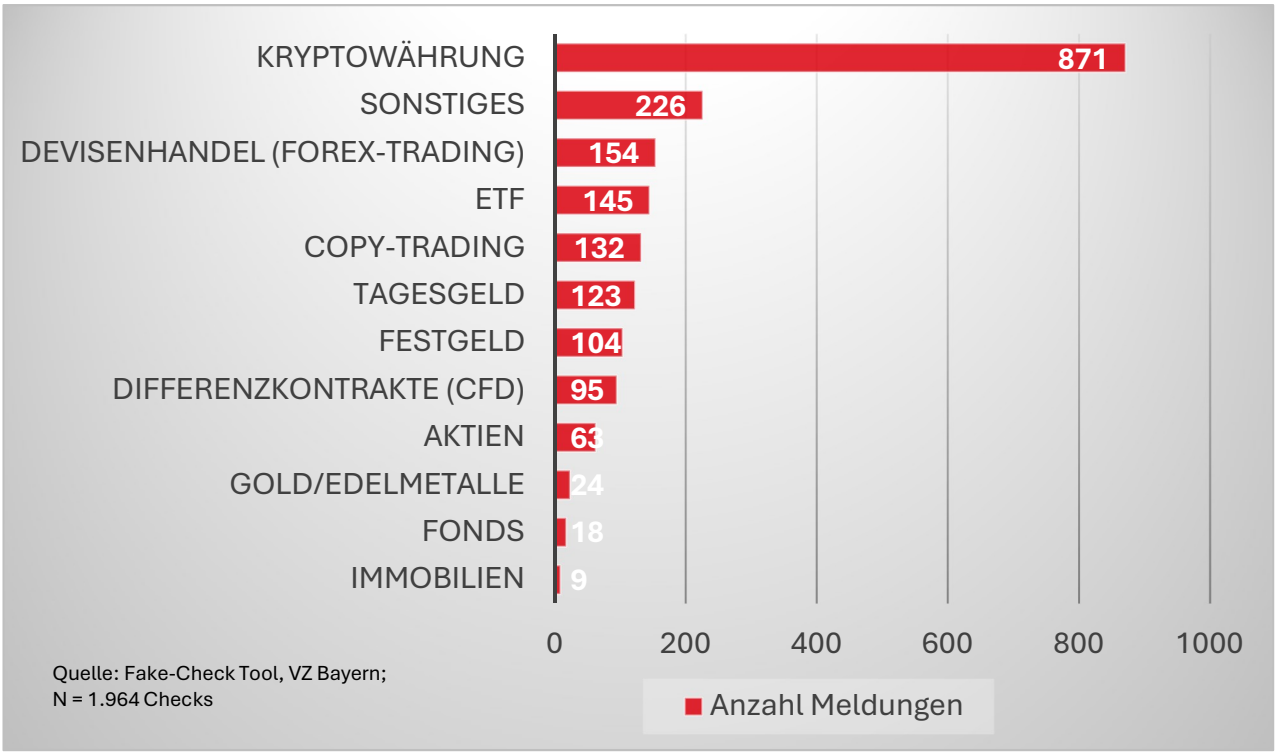
2. Funktionsweise des Online-Tools

Das Tool funktioniert anonym und ohne Registrierung. Nutzerinnen und Nutzer beantworten einige gezielte Fragen zu dem Angebot und erhalten anschließend eine Einschätzung, ob Warnzeichen für Betrug vorliegen. Je mehr Risikosignale (Red Flags) erkennbar sind, desto deutlicher fällt der Hinweis aus, dass es sich um ein unseriöses Angebot handeln könnte.

Wichtig: Das Tool ersetzt keine persönliche Rechtsberatung, gibt aber einen klaren Hinweis, wann es sinnvoll ist, sich individuell beraten zu lassen.

3. Verteilung der gemeldeten Anlagetypen

Kryptowährungen dominieren das Bild mit großem Abstand: Auf sie entfallen fast die Hälfte aller 1.964 Checks. Forex-Trading und CFD folgen auf den Plätzen. Klassische Produkte wie ETF, Tagesgeld und Festgeld sind zwar auch nennenswert vertreten, hier überwiegen aber die präventionsmotovierten Prüfdurchläufe, wie im Verlauf noch gezeigt wird.



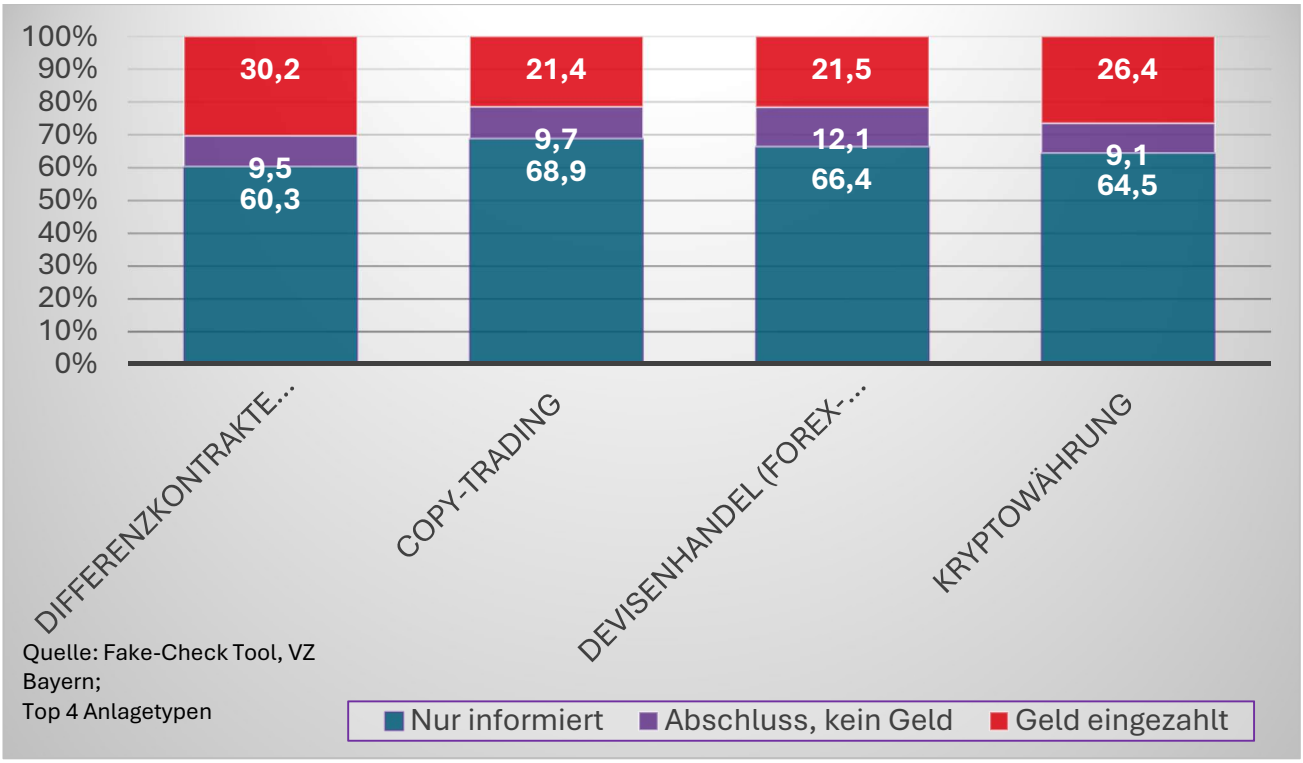
Quelle: Fake-Check Tool, VZ Bayern;
N = 1.964 Checks

Bewertung: Die Krypto-Lastigkeit ist kein Zufall, sondern spiegelt ein aktives Täterfeld wider. Gleichzeitig zeigen die Aktien-,Tagesgeld- und ETF-Einträge, dass das Tool auch zur Angebotsverifikation klassischer Finanzprodukte genutzt wird.

4. Schadenstiefe nach Anlagetyp

Rund **25 Prozent** der Meldenden haben zum Zeitpunkt des Checks bereits Geld eingezahlt; sie sind potenziell direkt geschädigt. Weitere 10 Prozent haben das Angebot angenommen, aber noch nicht gezahlt. Nur gut 65 Prozent nutzen das Tool präventiv.

Besonders alarmierend: Bei Kryptowährungen und bei CFDs hat ein höherer Anteil der Melder bereits Geld eingezahlt. Copy Trading zeigte den größten Anteil an Personen, die noch im Recherchestadium sind, was auf eine präventive Wirkung des Tools hoffen lässt.

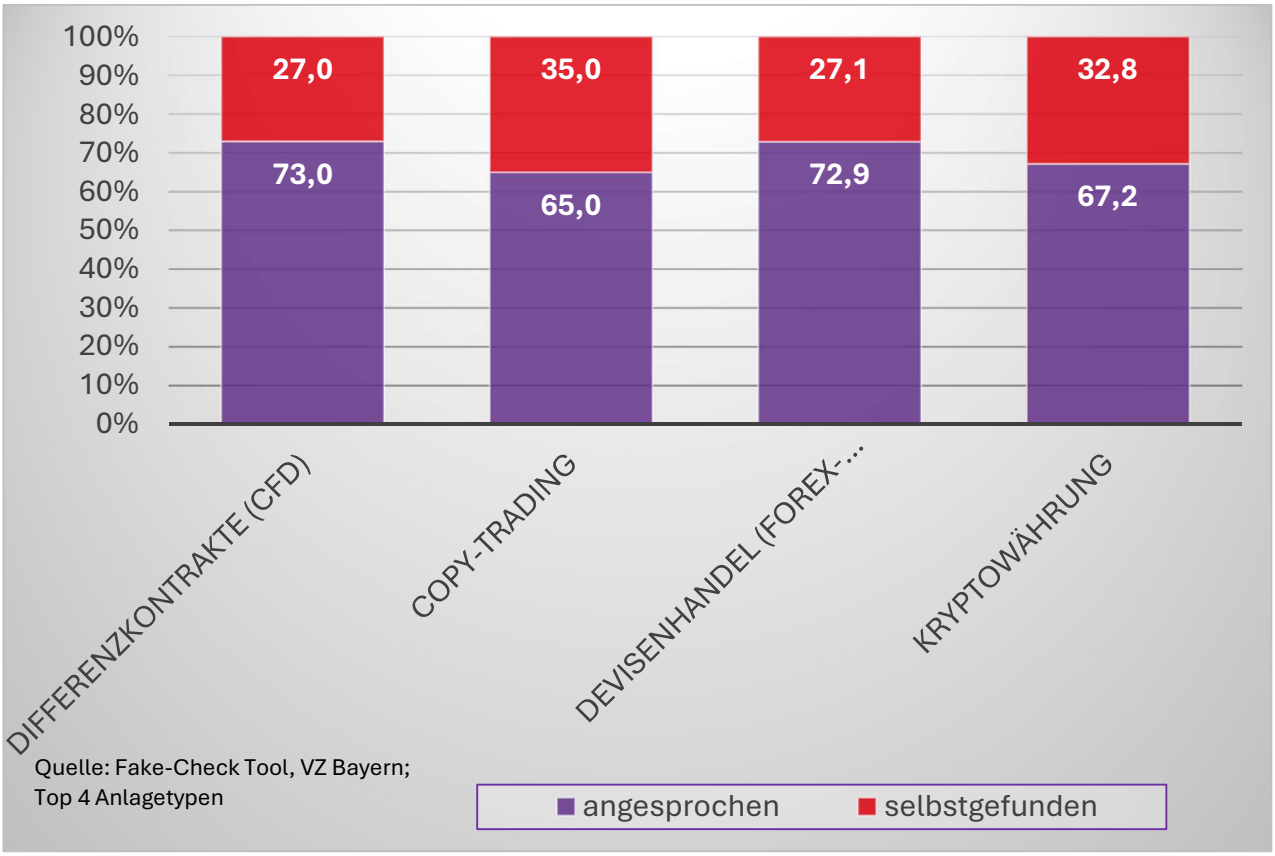


Quelle: Fake-Check Tool, VZ Bayern;
Top 4 Anlagetypen

Bewertung: Jede Person mit Status „Geld eingezahlt" ist potenziell geschädigt, diese Gruppe sollte bevorzugt in Beratungsangebote geleitet werden. Das Tool erfüllt seine Warnfunktion, erreicht aber einen signifikanten Teil der Betroffenen erst nach dem finanziellen Einstieg.

5. Erstkontaktweg: Selbst gefunden vs. aktiv angesprochen

Bei Kryptoangeboten und Copy-Trading wurden Betroffene etwas häufiger aktiv kontaktiert als bei Forex Trading und CFD, wo die meisten selbst auf das Angebot gestoßen sind. Insgesamt sind rund 30 % aller Meldenden proaktiv von Betrügern angesprochen worden.

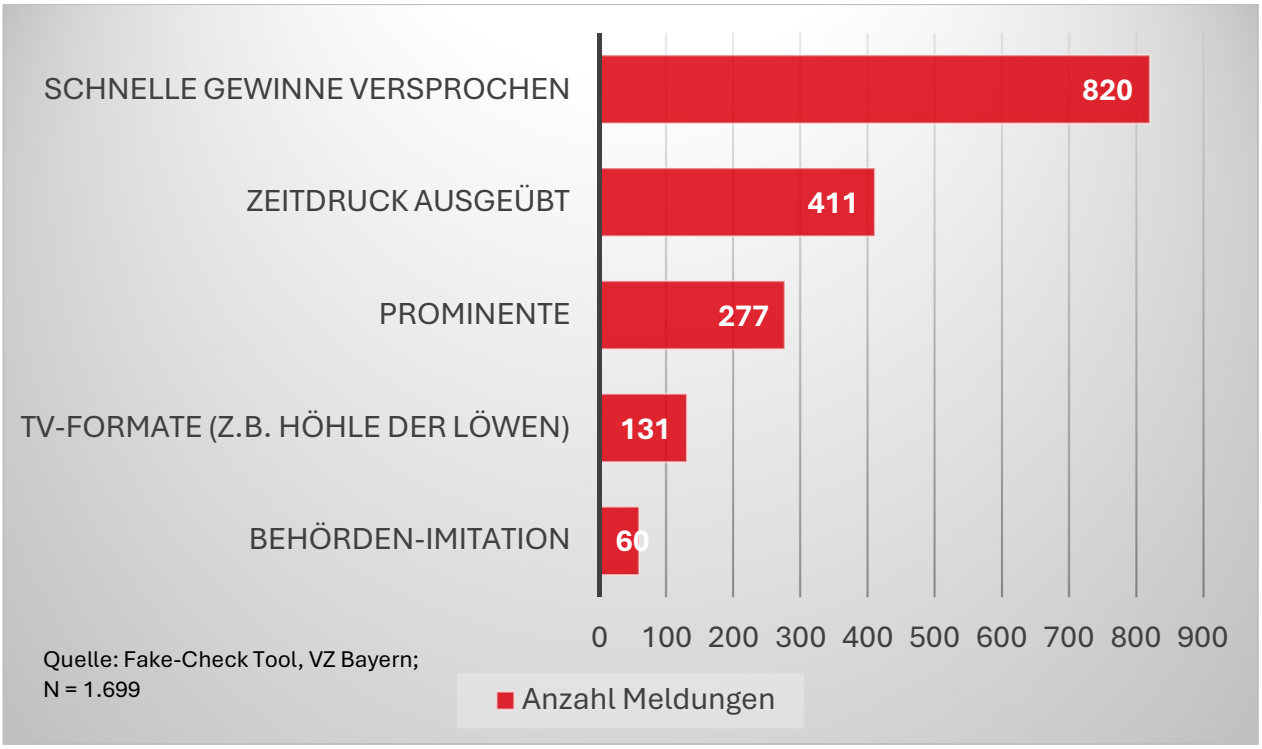


Quelle: Fake-Check Tool, VZ Bayern;
Top 4 Anlagetypen

Bewertung: Die aktive Ansprache ist ein klassisches Merkmal organisierter Betrugsstrukturen (Cold Calls, Social-Media-Direktnachrichten). Der hohe Anteil von „selbstgefunden“ bei Krypto zeigt aber auch, wie effektiv die passive Online-Werbung dieser Akteure ist.

6. Eingesetzte Manipulationstaktiken

Mit Abstand am häufigsten ist das Versprechen schneller Gewinne, gefolgt von hohem Zeitdruck. An dritter Stelle scheinen Prominente eine Anziehungswirkung zu haben, wobei TV-Formate wie die „Höhle der Löwen" als falsche Referenz und die Imitation von Behörden etwas weniger weit verbreitet sind.

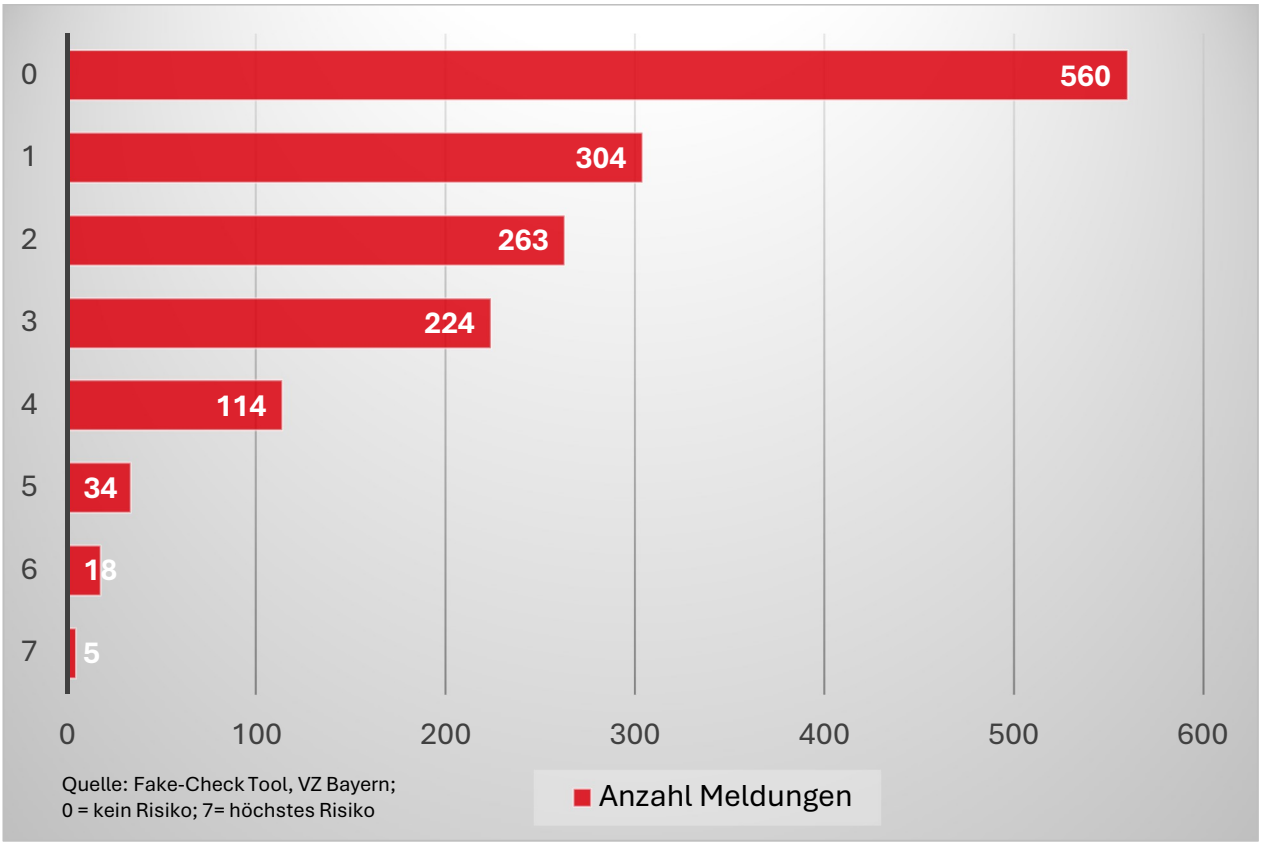


Quelle: Fake-Check Tool, VZ Bayern;
N = 1.699

Bewertung: Diese Taktiken sind bekannte Social-Engineering-Muster. FOMO *(die Angst etwas zu verpassen*) scheint eine tragende Rolle beim Abschluss zuspielen, während Testimonials wie Prominente oder TV-Formate zwar eine geringere Bedeutung haben, jedoch immer noch viele Menschen zu falschen Entscheidungen bewegen.

7. Verteilung der Warnsignal-Scores

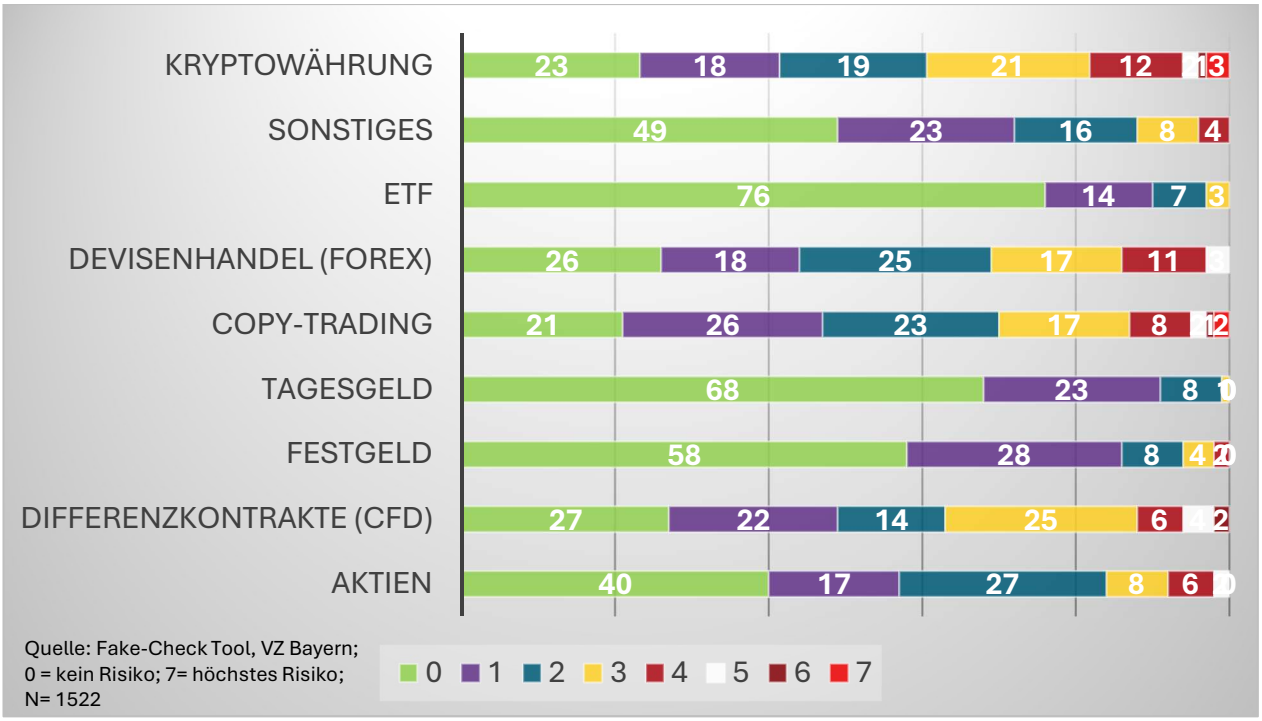
Je mehr Warnsignale (Red Flags) beim Check auftauchen desto höher die Wahrscheinlichkeit eines unseriösen Angebotes. Eine hohe Anzahl der Checks weist 0 Warnsignale auf. Diese Nutzer haben das Tool vermutlich zur Vorprüfung eines Angebots genutzt, das sich als unkritisch herausstellte. Jedoch zeigt ein substanzieller Anteil der Fälle 3 bis 7 Warnsignale gleichzeitig, was auf klassische Betrugsprofile hindeutet.



Bewertung: Fälle mit 1+ Flags (29 %) sollten konsequent in persönliche Beratung übergeleitet werden, sie können Schadensrisiken beinhalten. Ab 3+ Flags (20 %) wird gleich vor einem Abschluss gewarnt, da man hier mit sehr hoher Wahrscheinlichkeit einem unseriösen Angebot aufgesessen ist.

8. Risikograd nach Anlageprodukt

Die Grafik zeigt auf einen Blick, welche Anlageprodukte wie riskant bewertet werden; farblich codiert von Grün (Flag 0 = kein Warnsignal) bis Rot (Flag 7 = höchstes Risiko).



Copy-Trading und Kryptowährungen weisen die bedrohlichsten Profile auf: Der grüne Anteil (Flag 0) ist hier relativ klein, während die Risikosegmente (Flag 2–7) deutlich dominieren. Das bedeutet: Wer ein Copy-Trading- oder Krypto-Angebot prüft, hat es mit hoher Wahrscheinlichkeit mit einem strukturierten Betrugsangebot zu tun.

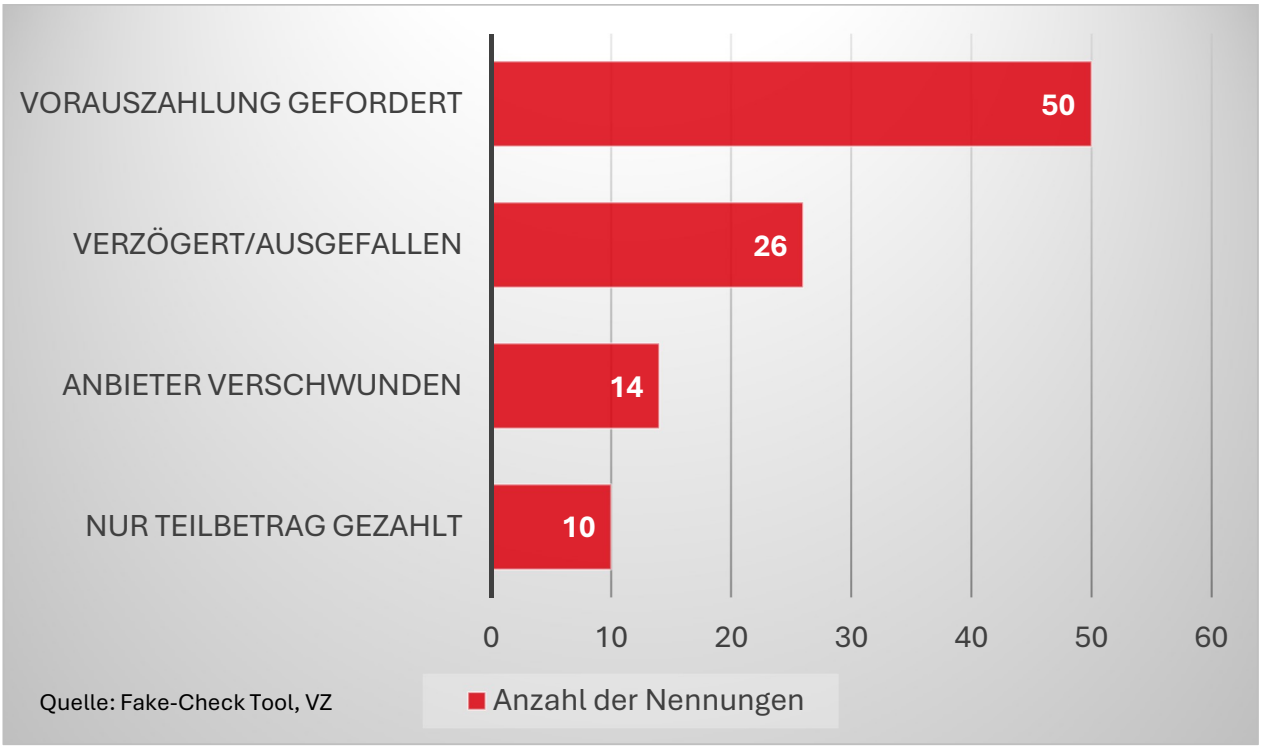
Forex-Trading und CFDs liegen im mittleren Risikobereich: Zwar gibt es einen nennenswerten Anteil niedriger Flags, aber auch ein klares Cluster bei 3–5 Warnsignalen, was auf professionell aufgesetzte Betrugsangebote hindeutet.

Festgeld, Tagesgeld, ETF und Aktien zeigen ein umgekehrtes Bild: Hier dominieren die grünen Segmente (Flag 0–1). Die meisten Nutzer, die klassische Produkte eingeben, erhalten die Rückmeldung „keine auffälligen Warnsignale". Das Tool wird für diese Kategorien also vorwiegend zur Beruhigung und Verifikation genutzt und erfüllt damit eine wichtige präventive Funktion.

Bewertung: Das Muster ist eindeutig: *Je spekulativer und komplexer das Produkt, desto höher der durchschnittliche Flag-Score.* Für Beratung und Kommunikation lässt sich daraus eine klare Botschaft ableiten: Angebote zu Copy-Trading und Krypto sollten generell mit maximaler Skepsis begegnet werden. Aber auch bei Forex und CFD ist das Gefahrenpotential recht hoch.

9. Art der Auszahlungsprobleme bei Geschädigten

Das häufigste Problem: Auszahlungen werden immer wieder verzögert und bleiben schließlich ganz aus, ein Klassiker bei Investment-Scams. An zweiter Stelle folgt die Forderung nach Vorauszahlungen (angebliche Steuerschulden oder Sicherheitsleistungen), gefolgt von Fällen, in denen der Anbieter plötzlich nicht mehr erreichbar ist.



Bewertung: Diese Muster entsprechen dem typischen Verlauf eines Pig-Butchering-Scams. Also das „Mästen“ eines Opfers durch emotionale Manipulation, bevor es um seine Ersparnisse gebracht wird.

Fazit:

1. Wer ungewöhnlich hohe Renditen, Zeitdruck oder prominente Empfehlungen sieht, sollte sehr vorsichtig sein.
2. Es reicht nicht, nur Verbraucherinnen und Verbraucher gegen Cyberbetrug zu sensibilisieren. Vielmehr muss die Betrugsinfrastruktur ausgeschaltet werden, indem diese Geschäftsmodelle unattraktiv und riskant gemacht werden. Werbung, Zahlungsflüsse, Plattformhaftung und Strafverfolgung müssen zusammen gedacht werden.
3. Der Fake-Check Geldanlage ist ein Instrument, um unseriöse Angebote früh zu erkennen und Schäden zu vermeiden.

Die Verbraucherzentrale Bayern sieht politischen Handlungsbedarf und fordert:

1. Gezielte Regulierung von Online-Finanzwerbung

Plattformen müssen stärker in die Pflicht genommen werden, betrügerische Werbung für Krypto, Trading- und Anlageprodukte schneller zu erkennen, zu löschen und zu verhindern.

2. Disruption statt nur Aufklärung

Fake-Websites und Scam-URLs müssen schnell und unbürokratisch durch Aufsichts- sowie Strafverfolgungsbehörden abgeschaltet werden können. Dazu müssen auch Barrieren beim behördlichen Informationsaustausch auf nationaler wie internationaler Ebene abgebaut werden.

3. Frühzeitige Bekämpfung von Auszahlungsbetrug und Fake-Brokern

Zahlungswege, auffällige Transaktionen, kompromittierte IBAN und ausländische Kontostrukturen müssen ständig und lückenlos überwacht werden, damit typische Betrugsmodelle früher gestoppt werden können. Kurze Geldtransaktionsverzögerungen bei Verdacht sind sinnvoll, damit Zahlungen noch gestoppt werden können. Banken und Finanzdienstleister müssten zu solchen Maßnahmen berechtigt und auch verpflichtet werden.

Impressum

Herausgegeben von:
Verbraucherzentrale Bayern e. V.
Mozartstraße 9, 80336 München

T +49 89 55 27 94-0
info@verbraucherzentrale.bayern
verbraucherzentrale.bayern

Stand:
April, 2026