Studie

Analyse des Betrugsökosystems Online-Werbung auf Meta-Plattformen

Dezember 2025

Österreichisches Institut für angewandte Telekommunikation

Impressum

Österreichisches Institut für angewandte Telekommunikation (ÖIAT)a
Ungargasse 64-66/3/404
1030 Wien

Projektleitung: Valentine Auer
Autorinnen: Valentine Auer, Lena Müller-Naendrup, Natalie Trell

Executive Summary

Online fraud is a growing global challenge, with social media platforms and search engines becoming key gateways for cybercriminals. This study, commissioned by the Austrian Digital Services Coordinator KommAustria and conducted by the Austrian Institute for Applied Telecommunications (ÖIAT), examines the scale and tactics of fraudulent and problematic online advertising shown to Austrian users on Meta's Facebook and Instagram platforms.

The study aims to: (1) **identify the main fraud schemes** actively advertised on Meta's platforms; (2) **estimate the scale of the problem**; and (3) gain insight into **scammers' strategies**, circulating **narratives**, and the specific **targeting of potential victim groups**. In doing so, the study makes an empirical contribution to the assessment of systemic risks as defined in the Digital Services Act (DSA).

Key findings

(1) Extent & Reach: Within just three months, the study identified 634,000 fraudulent or problematic advertisements across eight fraud schemes. Together, these ads generated more than 1 billion impressions across the EU, including approximately 123 million impressions in Austria alone.

Fraud Scheme	Number of Ads	EU Reach	Austria Reach
Online Gambling	448,699	620,572,304	64,790,612
Investment Fraud	83,216	126,665,013	21,961,476
Fake Shops (Brand Imitation)	28,276	65,931,501	2,024,487
Dubious Dietary Supplements	27,171	53,837,455	10,927,574
Job Fraud	18,140	17,265,387	15,757,809
Subscription Scams	17,779	102,402,859	2,891,621
Ghost Stores	9,955	21,407,495	4,751,404
Loan Fraud	805	236,180	121,344
Total	**634,041**	**1,008,318,194**	**123,226,327**

Figures are conservative lower-bound based only on ads identified through keyword searches.

(2) Deletion Rates & Ad Lifespan: 62.4% of all identified ads had already been removed by Meta at the time of data collection, indicating that the platform does detect and take action against some fraudulent content. At the same time, the identified ads tended to remain active only for very short periods, often just a few days or even hours, while new ads continued to appear.

(3) Manipulation Strategies: Across all eight fraud schemes, the qualitative analysis identified recurring manipulation strategies employed to lure victims, such as those outlined below:

DECEPTIVE DESIGN

Fraudulent ads systematically employ manipulative design patterns, including artificial scarcity (e.g. 'Only 2 items left'), manufactured urgency (e.g. 'Today only'), confirmshaming (e.g. framing inaction as a personal failure), and interface interference (e.g. prominent call-to-action buttons alongside barely visible exit options or links to terms-and-conditions).

CURIOSITY GAP

Ads deliberately create knowledge gaps designed to trigger irresistible impulses to click, for example through claims such as 'Are you smarter than the average?' (subscription scams), supposed insider knowledge about financial markets (investment fraud), or 'He carried a secret no one should know' (dietary supplements).

ABUSE OF ESTABLISHED TRUST ANCHORS

Well-known individuals (politicians, celebrities, entrepreneurs), media brands, and established institutions are systematically impersonated. In some cases, AI-generated deepfakes are used to fabricate video endorsements purportedly made by public figures.

EXPLOITATION OF SITUATIONAL VULNERABILITY

While fraudulent advertisers rarely apply explicit demographic targeting filters based on age or gender, the qualitative analysis reveals that fraudulent ads are designed to reach people in specific, often vulnerable, life situations. These include, for example, individuals experiencing financial distress (credit fraud), those with health concerns or chronic illnesses (dietary supplements), job seekers (job fraud), or people looking for passive income opportunities (investment fraud).

Compliance gaps on Meta

The DSA requires Very Large Online Platforms (VLOPs) such as Meta to provide transparency instruments that enable the independent verification of advertising. The Meta Ad Library is the central instrument intended to fulfil this obligation. The study documented structural deficits that limit the traceability and auditability of fraudulent ads.

(1) Opaque Advertiser Identity: Article 39 of the DSA requires the paying party behind each ad to be disclosed in the Ad Library. In practice, however, the 'payer' field is a free-text entry that Meta does not verify and that fraudsters systematically misuse. The dataset contains entries such as random digit strings, arbitrary character sequences, misappropriated brand names, and even 'facebook' itself listed as the payer for fraudulent ads.

(2) Disappearing Ads: Article 39 of the DSA requires VLOPs to retain ad records in the public repository for at least one year, even after an ad is no longer active. The study found that previously documented ads could no longer be found in later searches.

(3) Continued Ad Activity on Supposedly Disabled Accounts: Many identified ads were already marked as removed by Meta ('This ad was run by an account or Page we later disabled for not following our Advertising Standards'). However, our observation revealed that new ads were later placed under the same Page ID, despite the supposed deactivation of the account. This goes beyond the common practice of fraudsters creating new accounts under slightly modified names.

(4) Ads Not Retrievable via Text Search: Relevant fraudulent ads were found to be unsearchable by their text content, despite being present in the Ad Library when accessed via the account name. As a result, several well-known celebrity names had to be removed from the study's keyword lists, as text-based queries produced no results even though the research team knew that relevant ads existed.

Systemic Risk under the DSA

The study shows that the transparency mechanisms provided under the Digital Services Act offer important entry points for regulatory oversight. The ability to systematically collect and analyze advertisements enables evidence-based documentation of the problem, which can serve as a basis for enforcement action.

At the same time, the findings demonstrate that merely providing an Ad Library is not sufficient to effectively address fraudulent advertising. The study highlights that fraudulent and problematic advertising on Meta's platforms is not a marginal phenomenon, but constitutes a systemic risk under the DSA, as it spans eight thematically distinct fraud schemes involving large numbers of ads.

The DSA requires VLOPs not only to identify systemic risks, but also to mitigate them through appropriate measures. The compliance gaps documented in this study indicate that current measures against fraudulent advertising fall short of this obligation.

Inhalt

Einleitung

Der durch Online-Betrug verursachte Schaden nimmt international seit Jahren zu. Die Global Anti-Scam Alliance (GASA) dokumentiert für 2025 weltweite Scam-Verluste von rund 442 Milliarden US-Dollar (Abraham, 2025), schätzt die tatsächlichen Verluste jedoch zwischen 442 Mrd. bis zu einer Billion ein (Vorster, 2026). Auch in Österreich stellt Online-Betrug ein zentrales Problem dar: Laut Cybercrime-Report wurden 2024 62.328 Cybercrime-Delikte angezeigt. Zwar ist diese Zahl erstmals seit einem Jahrzehnt leicht rückläufig, die Straftaten im Bereich Internetbetrug bleiben jedoch auf hohem Niveau und machen mit 31.768 Fällen rund die Hälfte aller Cybercrime-Straftaten aus (Bundesministerium für Inneres, 2025).

Die zunehmende Verlagerung von Betrugsdelikten in den digitalen Raum ist dabei nicht nur auf die potenzielle Anonymisierung von Identitäten und Finanzflüssen zurückzuführen. Ein wesentlicher Faktor ist auch die Möglichkeit, mit geringem Ressourceneinsatz eine große Zahl potenzieller Opfer zu erreichen. Täter:innen stehen zudem vor der Herausforderung, ihre betrügerischen Angebote zu bewerben und an potenzielle Opfer heranzutragen. Hierfür bedienen sie sich zunehmend der **Werbemöglichkeiten großer Online-Plattformen**. Expert:innen aus dem Bereich der Betrugsprävention und -detektion berichten, dass Werbeanzeigen sich zu einem wesentlichen Einfallstor für Online-Betrug entwickelt haben (vgl. Federal Trade Commission, 2023; OCCRP, 2025).

Insbesondere auf vom Digital Services Act (DSA) regulierten großen Online-Plattformen (VLOPs) und sehr großen Online-Suchmaschinen (VLOSEs) können betrügerische Inhalte nicht nur massenhaft verbreitet, sondern auch anhand demografischer Merkmale, Interessen oder Verhaltensdaten auf Zielgruppen zugeschnitten werden. Beworben wird dabei eine **Vielzahl unterschiedlicher Online-Fallen** – von klar rechtswidrigen Betrugsmaschen wie unseriösen Investmentangeboten oder Fake-Shops bis hin zu problematischen Praktiken wie irreführenden Abo-Fallen oder Ghost Stores, die Nutzer:innen gezielt über Herkunft, Qualität oder rechtliche Rahmenbedingungen in die Irre führen.

Während der Einsatz von Online-Werbung für betrügerische Zwecke grundsätzlich bekannt ist, geben jüngste investigative Recherchen erstmals einen Einblick in das Ausmaß und die **strukturelle Verankerung dieses Problems im Werbeökosystem großer Plattformen**. Enthüllungen aus internen Dokumenten von Meta legen nahe, dass betrügerische Werbeanzeigen auf Meta-Diensten nicht nur ein Randphänomen sind, sondern einen signifikanten Bestandteil des Werbeökosystems darstellen. Laut internen Meta-Dokumenten, die Reuters zugespielt wurden,

projizierte Meta allein im Jahr 2024 rund 16 Milliarden US-Dollar mit Werbeanzeigen, die zu Betrugsmaschen oder zum Verkauf illegaler Waren führen – was etwa 10% des gesamten Werbeumsatzes entspricht. Meta reagierte auf die Zahlen zwar mit dem Hinweis, dass es sich dabei um Schätzungen gehandelt habe, um Planungen, inkl. jener zur Betrugsbekämpfung, durchzuführen (Horwitz, 2025a). Doch nur kurze Zeit später zeigen weitere Reuters-Recherchen von Meta geplante Strategien, um die Identifizierung betrügerischer Anzeigen durch Aufsichtsbehörden zu erschweren (Horwitz, 2025b).

Damit kommt der **Online-Werbung eine Schlüsselrolle im Kontext Online-Betrug** zu – nicht nur bei der Ermöglichung dessen, sondern auch bei der Bekämpfung. Denn die Plattformen, auf denen diese Werbung geschaltet wird, sind – im Gegensatz zu vielen anderen Akteuren in der Betrugswertschöpfungskette – identifizierbar und regulatorisch greifbar.

Vor diesem Hintergrund untersucht die vorliegende Studie im Auftrag der KommAustria als Koordinator für Digitale Dienste (DSC) **betrügerische und problematische Online-Werbung**, die an österreichische Nutzer:innen auf den **Meta-Diensten Facebook und Instagram** ausgespielt wird. Ziel der Studie ist es, zentrale Betrugsschemata zu identifizieren, das Ausmaß des Problems näherungsweise zu quantifizieren und Einblicke in Täterstrategien, vorherrschende Narrative sowie Formen der Zielgruppenansprache zu gewinnen. Damit leistet die Studie einen empirischen Beitrag zur Bewertung systemischer Risiken im Sinne des Digital Services Act und liefert eine evidenzbasierte Grundlage für regulatorische, politische und präventive Maßnahmen.

1. Hintergrund und Forschungsfragen

1.1. Systemisches Risiko unter dem Digital Services Act

Der seit Februar 2024 für alle digitalen Dienste unmittelbar anwendbare **Digital Services Act (DSA)** verpflichtet sehr große Online-Plattformen (VLOPs) und Online-Suchmaschinen (VLOSEs), gegen illegale Inhalte vorzugehen und Risiken zu adressieren, die sich aus dem Betrieb ihrer Dienste ergeben. Nach Artikel 34 DSA (EU 2022/2065) sind VLOPs und VLOSEs verpflichtet, Risiken, die sich aus der Nutzung der jeweiligen Dienste ergeben, regelmäßig zu ermitteln, zu analysieren und zu bewerten. Artikel 35 DSA (EU 2022/2065) verpflichtet sie dazu angemessene, verhältnismäßige und wirksame Maßnahmen zu ergreifen, um die ermittelten Risiken zu minimieren.

Systemische Risiken im Sinne des DSA zeichnen sich dadurch aus, dass sie nicht auf Einzelfälle beschränkt sind, sondern sich aus strukturellen Merkmalen der Konzeption und des Betriebs von VLOPs und VLOSEs ergeben. Dazu zählen laut Artikel 34 DSA (EU 2022/2065) unter anderem Risiken, die durch algorithmische Empfehlungssysteme, durch Systeme der Content-Moderation oder durch die datenbezogene Praxis der Anbieter verstärkt werden. Hervorgehoben werden zudem die „Systeme zur Auswahl und Anzeige von Werbung“, womit das Werbeökosystem selbst als potenzieller Träger systemischer Risiken anerkannt wird.

Als zentraler Bestandteil des Geschäftsmodells großer Plattformen, der aktiv gesteuert und monetarisiert wird, profitiert die Täterschaft im Betrugsökosystem durch Werbungen von denselben Mechanismen, die legitime Werbung effizient machen: hohe Reichweiten, personalisiertes Targeting sowie automatisierte Ausspielungen.

Zur Stärkung von Transparenz und Rechenschaftspflichten insbesondere im Bereich der Werbeanzeigen sieht der DSA in Artikel 39 (EU 2022/2065) vor, dass VLOPs und VLOSEs **öffentlich zugängliche Werbebibliotheken** zur Verfügung stellen müssen. Für jede auf der Plattform geschalteten Anzeige müssen unter anderem der Werbeinhalt, die juristische oder natürliche Person, die die Werbung geschaltet bzw. finanziert hat, der Zeitraum der Schaltung sowie Kennzahlen zum Targeting offengelegt werden. Damit ermöglichen die Werbebibliotheken Dritten, Werbeanzeigen systematisch zu analysieren und zu dokumentieren und stellen einen zentralen Ansatzpunkt dar, um die Größenordnung und die Struktur betrügerischer Werbung auf großen Plattformen empirisch zu untersuchen.

Erste Erhebungen des Österreichischen Instituts für angewandte Telekommunikation (ÖIAT) sowie der ÖIAT-Initiative Watchlist Internet[1] zeigen auf, dass in Österreich in erheblichem Umfang Werbung für unterschiedliche Betrugsformen und problematische Angebote geschaltet wird:

- **Investmentbetrug:** Zwischen Januar bis April 2024 wurden auf Meta-Plattformen 9.000 Werbeanzeigen mit einer täglichen Reichweite von rund 200.000 (Österreich) ermittelt, in denen die Namen und Bilder 25 österreichischer Prominente missbraucht werden (Watchlist Internet, 2024).
- **Ghost Stores:** Zwischen Januar und April 2025 wurden 36.000 Werbeanzeigen auf Meta-Plattformen ermittelt, die vorgeben ein lokales Familienunternehmen zu sein. Die Online-Shops verstoßen gegen geltende verbraucherschutz- und wettbewerbsrechtliche Bestimmungen, u.a. da ihr tatsächlicher Sitz im EU-Ausland ist und Konsument:innen gezielt irregeführt werden (Watchlist Internet, 2025b).
- **Dubiose Angebote für Nahrungsergänzungsmittel:** Zwischen Januar und Juli 2025 wurden 4.632 problematische Werbeanzeigen mit einer Reichweite von über 21,5 Millionen auf Meta-Plattformen dokumentiert, in denen insbesondere die Namen und Bilder bekannter Ärzt:innen und Gesundheits-Expert:innen missbraucht wurden. Besonders problematisch war dabei, dass im Zuge der Werbungen Desinformation verbreitet und das Vertrauen in evidenzbasierte Medizin und öffentliche Institutionen untergraben wurde (Auer et al., 2025).

Auch auf internationaler Ebene liegen vergleichbare Befunde vor: Bereits 2022 dokumentierte die britische Verbraucherorganisation Which? Werbeanzeigen für unseriöse und betrügerische Investmentplattformen (Which, 2022). Die europäische Non-Profit Organisation AI Forensics identifizierte EU-weit rund 46.000 Werbeanzeigen für nicht zugelassene Medikamente oder irreführende Gesundheitsversprechen, die insgesamt über 292 Millionen Mal an europäische Nutzer:innen ausgespielt wurden (Bouchand et al., 2025).

Diese Erhebungen liefern Hinweise darauf, dass betrügerische und problematische Online-Werbung **kein marginales Phänomen** darstellt, sondern potenziell ein systemisches Risiko im Sinne des Digital Services Act bildet. Die vorliegende Studie knüpft an diese Arbeiten an und zielt darauf ab, das Betrugsökosystem auf Meta-Plattformen exemplarisch zu analysieren und zu dokumentieren.

[1] Die Watchlist Internet ist die im deutschsprachigen Raum größte Online-Plattform zu Internetbetrug.

1.2. Fragestellungen

Vor diesem Hintergrund ist das Ziel der Studie, das Betrugsökosystem exemplarisch auf Plattformen des Unternehmens Meta (Facebook, Instagram) zu untersuchen und zu dokumentieren, um die systemischen Risiken betrügerischer Werbung aufzuzeigen. Konkret soll die Studie evidenzbasierte Einblicke in die folgenden Themenbereiche und Fragestellungen geben:

Identifikation von Betrugsschemata und Keywords

(1) Bei welchen Betrugsschemata kommen Werbeanzeigen zum Einsatz?

(2) Welche Keywords eignen sich zur Identifikation betrügerischer Anzeigen?

Quantitative Erfassung von Werbeanzeigen

(3) Wie viele betrügerische Anzeigen lassen sich je Betrugsschema mit den identifizierten Keywords finden?

(4) Wann und wie lange sind die Anzeigen aktiv?

(5) Wie hoch ist die Reichweite der Anzeigen je Betrugsschema?

(6) An welche Personengruppen werden die Anzeigen ausgespielt?

(7) Wer sind Werbetreibende, Begünstigte und Zahlende? Welche Muster lassen sich dabei erkennen?

(8) Welche Betrugsarten erzielen die höchsten Reichweiten?

Qualitative Erfassung von Werbeanzeigen

(9) Mit welchen Strategien und Narrativen werden die Betrugsfallen beworben?

(10) Welche Zielgruppen werden auf einer inhaltlichen Ebene angesprochen?

(11) Welche Rolle spielen KI bzw. Deepfakes bei der Bewerbung der Betrugsfallen?

(12) Welche weitere Infrastruktur wird bei der Weiterleitung von den Anzeigen verwendet?

(13) Welche Täterstrategien zur Umgehung von Sicherheitsmaßnahmen und Content-Moderation sind beobachtbar?

(14) Welche Sicherheitslücken auf den Plattformen-Diensten von Meta wurden beobachtet?

1.3. Limitierungen

Trotz der systematischen Vorgehensweise zur Erfassung und Analyse betrügerischer und problematischer Online-Werbung auf Meta-Plattformen weist die vorliegende Studie limitierende Aspekte auf, die bei der nachfolgenden Interpretation der Ergebnisse zu berücksichtigen sind.

Keine vollständige Erfassungsgesamtheit

Die Studie strebt nicht an, Werbeanzeigen in einzelnen Betrugsschemata vollständig zu erfassen. Eine solche **Vollerhebung** wäre **methodisch nicht realisierbar**, da ein Überblick über die Grundgesamtheit aller Werbeanzeigen fehlt. Die Methode des iterativen Testens bestimmter Keywords erfasst insbesondere Anzeigen mit erkennbaren Mustern. Betrugsanzeigen ohne auffällige Keywords bleiben unentdeckt, was bedeutet, dass die tatsächlichen Zahlen deutlich höher liegen werden.

Auch innerhalb eines Keywords kann es aus unterschiedlichen Gründen zu *False Negatives* kommen: Werbeanzeigen können unentdeckt bleiben, einerseits da betrügerische Akteur:innen Taktiken und Strategien entwickeln, um Erkennungs- und Detektionssysteme zu umgehen. Andererseits soll Meta laut internen Dokumenten selbst Methoden anwenden, die betrügerische Werbung schwerer auffindbar machen (Horwitz, 2025b). Hinzu kommt, dass teilweise sowohl die Anzahl der Suchbegriffe als auch der Berichtszeitraum reduziert werden mussten, um nicht das von Meta zur Verfügung gestellte Abfragen-Limit zu überschreiten. Ziel der Studie ist es daher, einen Einblick in die Größenordnung und die strukturellen Merkmale des Problems zu geben.

Fokus auf deutschsprachigen Raum

Ein Großteil der für die Studie verwendeten Keywords ist **deutschsprachig** oder auf den **regionalen Kontext des deutschsprachigen Raums** zugeschnitten (z. B. Namen bekannter Persönlichkeiten aus Deutschland oder Österreich). Zwar gibt Meta die Reichweiten für die gesamte EU an, in den meisten Fällen beziehen sich diese Angaben jedoch überwiegend auf den deutschsprachigen Raum. Für andere EU-Länder sind die Ergebnisse daher nicht aussagekräftig.

Einschränkung durch Datenlage

Obwohl der DSA Transparenz- und Werbebibliothekspflichten für VLOPs wie Meta vorsieht, bestehen strukturelle Einschränkungen, auf die die Studien-Autor:innen keinen Einfluss haben. Die **Richtigkeit, Genauigkeit und Vollständigkeit** der erhobenen Daten ist von den von Meta bereitgestellten Informationen abhängig, und Unvollständigkeiten oder Ungenauigkeiten in diesen Daten können die Analyse beeinflussen. Die in dieser Studie identifizierten Zahlen sind daher als

Näherungswerte zu verstehen, die auf den durch die Meta Ad Library verfügbar gemachten Daten beruhen und deren Genauigkeit nicht unabhängig überprüft werden kann.

Berücksichtigung von Grauzonen und problematischen Inhalten

Die Studie erfasst neben Werbeanzeigen für eindeutig strafrechtlich relevanten Betrug, auch unseriöse und irreführende Anzeigen, die mit dem Ziel veröffentlicht werden, Nutzer:innen zu täuschen und zu einer für sie nicht vorteilhaften Entscheidung zu bewegen. Da sich der DSA nicht nur gegen klar illegale Inhalte, sondern auch gegen manipulative Techniken sowie gegen Risiken für Verbraucherrechte auf Plattformen richtet, sind auch diese **inhaltlichen Grauzonen** relevant. Dieser erweiterte Fokus vertieft den analytischen Horizont, bedeutet aber zugleich, dass nicht jeder erfasste Fall eindeutig strafrechtlich relevant ist, sondern die Erhebung vielmehr ein breites Spektrum problematischer Angebote umfasst.

2. Identifikation der Betrugsschemata und Keywords

2.1. Methodisches Vorgehen

Die **Identifikation relevanter Betrugsschemata** bildet die Grundlage der Untersuchung und erfolgte auf Basis von zwei Ansätzen:

(1) Konsument:innen-Meldungen an die Watchlist Internet:

Betrugsschemata wie Investmentbetrug oder die Bewerbung von unseriösen Nahrungsergänzungsmittelangeboten werden regelmäßig von Konsument:innen an die Watchlist Internet gemeldet und sind daher als relevante Phänomene, in manchen Fällen inkl. Keywords, bekannt. Diese Meldungen bilden eine zentrale Grundlage für die Auswahl der zu untersuchenden Schemata.

(2) Exploratives Testen möglicher weiterer Betrugsschemata

Bei Themen, die noch nicht durch Meldungen oder Medienberichte bekannt waren, wurden mögliche passende Suchbegriffe in der Meta-Werbebibliothek auf relevante Ergebnisse explorativ getestet. Dieser Ansatz ermöglichte die Identifikation zusätzlicher Betrugsschemata.

Je identifiziertes Betrugsschema wurden **relevante Keywords identifiziert.** Keywords entsprechen dabei Textphrasen, die typischerweise in betrügerischen Werbeanzeigen verwendet werden – etwa Produktnamen, Versprechen oder Namen von Prominenten – und über die sich

entsprechende Anzeigen in der Werbebibliothek auffinden lassen. Für die Identifizierung der Keywords wurde ein iterativer Prozess angewandt:

- Initiale Keywords wurden basierend auf bekannten bzw. neu identifizierten Betrugsmustern in die Meta-Werbebibliothek eingegeben.
- Erste Suchergebnisse wurden hinsichtlich deren betrügerischer Absicht analysiert sowie dazugehörige Werbetreibende identifiziert.
- Durch die Suchergebnisse, aber auch durch die Werbetreibenden und deren weitere Anzeigen wurden zusätzliche Keywords identifiziert.
- Dieser Prozess wurde wiederholt, bis eine Sättigung erreicht wurde.

2.2. Identifizierte Betrugsschemata & Keywords

Im Rahmen der Studie wurden acht Betrugsschemata identifiziert, bei denen Werbeanzeigen über Meta-Plattformen im großen Ausmaß zum Einsatz kommen. Für jedes Schema wurde eine Detailanalyse durchgeführt, die insbesondere quantitative Einblicke in das jeweilige Betrugsökosystem liefert. Im Folgenden werden die identifizierten Betrugsschemata und Keywords[2] skizziert.

2.2.1. Abo-Fallen

Abo-Fallen sind ein etabliertes Betrugsschema, bei der Websites oder Online-Dienste vermeintlich kostenlose oder sehr günstige Leistungen anbieten. Verschleiert wird, dass Betroffene – meist unbemerkt – ein **kostenpflichtiges Abonnement abschließen**. Die Entgeltpflicht und die Laufzeit des Abos „sind dabei entweder gar nicht, nur unzureichend oder bewusst irreführend dargestellt (ÖIAT, 2025). Die beworbenen Leistungen umfassen typischerweise digitale Dienstleistungen mit niedrigem wahrgenommenem Risiko wie IQ-Tests.

Keywords
„ADHD is Not Laziness“
„Bist du schlauer als der durchschnittliche Deutsche“
„How high is your IQ score”
„if you can solve these 15 questions”

[2] Keywords in Anführungszeichen werden als exakte Wortfolge gesucht, Keywords ohne Anführungszeichen als freie Suche. Die Schreibweise der Keywords in dieser Tabelle folgt entsprechend der jeweils verwendeten Suchmethode.

„stop wasting time on 10,000 steps a day"
„Think you're smarter than the average American"
„Trainieren Sie Ihren Hund wie ein Profi"
„Verändere deinen Körper, deine Energie, dein Leben."
„Was ist Ihre Intelligenztyp"

2.2.2. Investmentbetrug

Investmentbetrug bezeichnet eine Form des Finanzbetrugs, bei der **vermeintlich lukrative Investitionsmöglichkeiten** beworben werden, um Betroffene zur Einzahlung von Geld zu verleiten. Tatsächlich dienen die Angebote jedoch ausschließlich dazu, Gelder von den Betroffenen zu erlangen. Eine tatsächliche Investition findet nicht statt. (Watchlist Internet, 2022b).

Keywords
„Hoss & Hopf"
„Wir nehmen kein Geld – du bekommst die besten Tipps völlig kostenlos."
„AI-Trading"
„ChatGPT Aktien"
„Gerald Hörhan"
Viele Leute wissen nicht, wie man Aktien auswählt
„Verdoppeln Sie Ihr Vermögen an der Börse"
„Österreicher verdienen"
Herbert Kickl
„Nur für Österreichische Staatsbürger"
„Die stärksten deutschen Aktien für 2026"
„Digitale Trends gewinnen immer mehr an Bedeutung"
„Deine Top-3 Aktien-Picks für bis zu +60% Potenzial"
„Hans Jörg Schelling"
„Die neue Plattform hat bereits die Effizienz des Bankensystems gefährdet"
„Armin Wolf"
„Expertenberatung bei schwierigen Investments"

2.2.3. Kreditbetrug

Kreditbetrug liegt vor, wenn vermeintlich günstige Kredit-, Darlehens- oder Finanzierungsangebote beworben werden, ohne dass jemals eine tatsächliche Kreditvergabe beabsichtigt ist. Ziel der Täter:innen ist es, Betroffene zur **Leistung von Vorauszahlungen** zu bewegen (Watchlist Internet, 2022a).

Keywords
„Privatkredite ohne Papierkram"
„trotz Schufa"
„Kreditstatus online prüfen"
„Erfahren Sie sofort, welche Kreditmöglichkeiten Sie haben."
„Jetzt Kredit online beantragen und sofort auszahlen lassen!"
„Karte anfordern"
„Brauchen Sie schnell Bargeld?"

„Sind sie kreditfähig?“
„Selbst hochverschuldete Menschen können Kredite erhalten!“
„Sofortkredit ohne Einkommensnachweis in Österreich“
„Finanzielle Entlastung gesucht?“
„Sie können auch mit Schulden einen Kredit erhalten!“

2.2.4. Jobbetrug

Über Werbeanzeigen werden **vermeintliche Jobangebote beworben**, die in Wirklichkeit keinen legalen Erwerbszweck verfolgen. Statt einer regulären Beschäftigung besteht das Ziel dieses Betrugsschemas darin, Personen in kriminelle Aktivitäten einzubinden (z. B. als Money-Mule), sensible Daten zu erlangen oder sie zu Vorauszahlungen zu bewegen. Eine Entlohnung für die beworbene Tätigkeit erfolgt nicht (Watchlist Internet, 2025a). Besonders häufig werden einfache, ortsunabhängige Tätigkeiten ohne erforderliche Vorkenntnisse und mit flexiblen Arbeitszeiten beworben.

Keywords
„Keine Erfahrung erforderlich“
talentway-at.com
„dass die von Ihnen angegebene WhatsApp-Nummer korrekt ist”
„Der Teilzeitjob, den ich über diese Website gefunden habe”
„Keine Erfahrung notwendig”
„Wir stellen ein – Starten Sie noch heute Ihre Remote-Karriere!“
„Hohes Gehalt und flexible Arbeitszeiten!“
„Machen Sie Ihre Leidenschaft zum Beruf und gestalten Sie Ihren eigenen Karriereweg!“
„Zzx0“
Wir suchen neue Kollegen - starte jetzt
„Weihnachtsjob gesucht?“
WorkAnchor Austria
„Bewirb dich jetzt und feiere Weihnachten“
„Join us and celebrate the warmest Weihnachten together“
Erfahrung ist nicht erforderlich, jeder ist willkommen!

2.2.5. Unseriöse Nahrungsergänzungsmittelangebote

Unseriöse Nahrungsergänzungsmittel werden oft mit **nicht zugelassenen Wirkversprechen** beworben, die gegen die Health Claims Verordnung (EG 1924/2006) verstoßen. Um die Produkte über Social Media zu vermarkten, werden häufig Namen und Gesichter bekannter Ärzt:innen, Gesundheitsexpert:innen oder etablierter Markennamen (z. B. dm oder Die Höhle der Löwen) missbräuchlich verwendet. Die gelieferten Produkte sind dabei oft wirkungslos, überteuert oder sogar gesundheitsgefährdend – oder es wird gar nichts geliefert (Auer et al., 2025).

Keywords
„Die Höhle der Löwen“
„Ihre Fettleber los“
Prostataprobleme
Wir garantieren Ihnen, dass Sie in 3 Wochen 10 kg abnehmen werden.
Ozempil
Hirschhausen
Reinigt die Blutgefäße
Meryn
Drosten
Tobias Weigl
„Probieren Sie dieses Abendritual aus“
Thomas Binder
Klaus Richter
„Müller Wohlfahrt“

2.2.6. Ghost Stores

Ghost Stores bezeichnen problematische Online-Shops, die meist vorgeben lokale, familiengeführte Shops mit Sitz in Österreich oder Deutschland zu sein und hochqualitative Ware verkaufen. Tatsächlich handelt es sich um Online-Shops, die **minderwertige Ware aus dem EU-Ausland** versenden – oder gar nichts liefern. Konsumentenschutzrechtliche Vorgaben werden dabei häufig nicht eingehalten.

Keywords
Lena boutique
Elle Weber
Modehaus Berfeld
Moser Wien
Muller Graz
Mirella Modehaus
Wien Modehaus
Schneider Salzburg
Thera Boutique
Weber Atelier
Greta Helene
Velser Wien
Werner & Martha

2.2.7. Fake-Shops (Markenimitation)

Fake-Shops geben sich als legitime Online-Shops aus. Wer dort bestellt, erhält entweder gar keine oder eine völlig andere als die bestellte Ware. Der Fokus dieser Recherche lag auf **Fake-Shops, die bekannte Marken imitieren**, indem sie deren Namen und Logos missbrauchen und den Webauftritt nachahmen.

Keywords
lidl discount
hofer garmin
swarovski hofer
„Bosch sale“
„birkenstock outlet“
hofer gopro
Birkenstock sale
Hofer Black Friday Sale
Swarovski 130.
swarovski mega sale
swarovski billa

2.2.8. Online-Glücksspiele

Glücksspiel ist in Österreich streng reguliert: Nur Betreiber mit einer gültigen Konzession – die v.a. von den Österreichischen Lotterien und der Casino Austria AG gehalten werden[3] – dürfen Glücksspielangebote anbieten. Über Social Media werden jedoch massenhaft **betrügerische Casino-Apps und Mini-Glücksspiele** wie „Plinko" oder „Chicken Road" beworben – Fake-Apps, bei denen Gewinne von vornherein nicht auszahlbar sind, Kreditkartendaten gestohlen werden oder weitere Einzahlungen erpresst werden. Da in diesem Bereich teilweise mehrere zehntausend Anzeigen pro Woche geschaltet werden und Meta die Anzahl der Anfragen innerhalb eines Abfragezeitraums limitiert, wurde die Keyword-Auswahl hier bewusst klein gehalten.

Keywords
„Casino Austria“
„Casinos Austria“
Plinko
„Chicken Road“

[3] https://www.bmf.gv.at/themen/gluecksspiel-spielerschutz/gesetzliche-grundlagen-gluecksspiel/konzessionaere-ausspielbewilligte.html

3. Quantitative Erfassung von Werbeanzeigen

3.1. Methodisches Vorgehen

Für die Detailanalyse wurde ein an die API der Meta-Werbebibliothek angebundener Crawler eingesetzt. Der Erhebungszeitraum erstreckte sich von **September bis November 2025.**[4]

Die identifizierten Keywords je Betrugsschema wurden an den Crawler übergeben und die Ergebnisse bereinigt, indem zunächst doppelte Einträge, über die für jede Werbeanzeige einzigartige Ad ID entfernt. Anschließend wurden die Daten in einem manuellen Screening-Verfahren auf Legitimität geprüft, insbesondere durch das Screenen von Page Name, URL und Anzeigentext. Anzeigen, die eindeutig von legitimen Unternehmen stammten, wurden aus dem Datensatz entfernt. Aufgrund des manuellen Charakters dieses Prozesses können vereinzelte Fehlklassifikationen – sowohl falsch-positive als auch falsch-negative – nicht ausgeschlossen werden.

Die bereinigten Daten wurden analysiert, um eine deskriptive Statistik je Betrugsschema zu erstellen. Zur Beantwortung der oben skizzierten Fragestellungen wurden die Rohdaten in mehrdimensionale Pivot-Tabellen überführt, die eine systematische Aggregation der unterschiedlichen Kennzahlen ermöglichten.

Konkret wurden Analysen zu folgenden Kennzahlen durchgeführt:

- **Anzahl der Werbeanzeigen**; umfasst jene Anzeigen mit einzigartiger Ad ID
- **Anzeigendauer**; umfasst die Zeitdauer, in denen Werbetreibende eine Anzeige ausspielen
- **Löschrate**; umfasst den Anteil der Werbeanzeigen, die von Meta bereits gelöscht wurden – entweder weil der dahinterliegende Account (Werbetreibende) aufgrund von Verstößen gegen die Werberichtlinien deaktiviert wurde oder weil der Inhalt selbst gegen die Werberichtlinien verstößt
- **Targeting nach Alter, Geschlecht und Standort**; umfasst Angaben vonseiten der Werbetreibenden, ob bestimmte Zielgruppen beim Ausspielen von Anzeigen bewusst ein- oder ausgeschlossen werden
- **Reichweite**[5]; umfasst:

[4] Der Zeitraum bezieht sich darauf, ob in diesem Datumsbereich Impressionen der Werbeanzeige verzeichnet wurden.

[5] Reichweite bezeichnet in dieser Studie die von Meta ausgewiesene Anzahl erreichter Konten pro Werbeanzeige. Durch die Zusammenführung mehrerer Anzeigen ist es möglich, dass einzelne Konten mehrfach enthalten sind, sofern sie verschiedene Anzeigen gesehen haben. Die Kennzahl stellt einen Schätzwert dar.

  - die Reichweite innerhalb der EU (wobei aufgrund der Auswahl der Keywords hauptsächlich der deutschsprachige Raum relevant ist)
  - die Reichweite in Österreich gesamt sowie aufgeschlüsselt nach Geschlecht und Altersgruppen
- **Werbetreibende**; umfasst die Facebook-Seite oder den Account, der die Werbeanzeige geschaltet hat
- **Begünstigte und Zahlende**; umfasst eine Person, die von den Werbetreibenden als zahlende oder begünstigte Person angegeben wurde
- **Keywords**; umfasst den Anteil eines Keywords an allen identifizierten Werbeanzeigen

3.2. Gesamtüberblick: Reichweiten, Löschraten, Targeting

3.2.1. Anzahl der Werbeanzeigen & Reichweite

Über die acht Betrugsschemata hinweg wurden insgesamt **634.000 betrügerische sowie problematische Werbeanzeigen** innerhalb von 3 Monaten identifiziert, die 1 Milliarden Mal an Nutzer:innen innerhalb der EU und knapp 123 Millionen Mal an Nutzer:innen in Österreich ausgespielt wurden.

Betrachtet man die Zahlen nach Betrugsschemata, zeigen sich deutliche Unterschiede – sowohl die Anzahl der Anzeigen als auch die Reichweite betreffend. Die am deutlich höchsten Zahlen entfallen auf die Online-Glücksspiele, gefolgt von Investmentbetrug. Am unteren Ende mit den wiederum deutlich wenigsten Anzeigen befindet sich Kreditbetrug.

Betrugsschema	Anzahl Werbeanzeigen	Reichweite EU	Reichweite Ö
Online-Glücksspiele	448.699	620.572.304	64.790.612
Investmentbetrug	83.216	126.665.013	21.961.476
Nahrungsergänzungsmittel	27.171	53.837.455	10.927.574
Fake-Shops	28.276	65.931.501	2.024.487
Jobbetrug	18.140	17.265.387	15.757.809
Abo-Fallen	17.779	102.402.859	2.891.621
Ghost Stores	9.955	21.407.495	4.751.404
Kreditbetrug	805	236.180	121.344
Gesamt	**634.041**	**1.008.318.194**	**123.226.327**

Tabelle 1: Anzahl der Werbeanzeigen und Reichweiten je Betrugsschema

3.2.2. Hohe Löschraten

Auffällig ist dabei die hohe Dynamik der Werbeanzeigen: **62,4%** aller identifizierten Werbeanzeigen wurden zum Erhebungszeitraum bereits von Meta aufgrund eines Verstoßes **entfernt.** Erkennbar

ist das durch einen Hinweis, dass der dahinterstehende Account aufgrund von Verstößen gegen die Werberichtlinien gesperrt wurde (46,9% aller Werbeanzeigen) oder – seltener – der Content selbst gegen die Werberichtlinien verstieß (16,2%).

Gleichzeitig setzen auch die betrügerischen Akteur:innen auf **kurze Anzeigendauer** von nur wenigen Tagen oder gar Stunden (siehe 4.3.2 Kurze Anzeigenlaufzeiten). Stattdessen wird auf viele und schnell wechselnde Anzeigen gesetzt. Zu vermuten ist, dass dabei die Moderation vonseiten der Plattform umgangen werden soll bzw. neue noch nicht entdeckte Werbeanzeigen die moderierten und entfernten Anzeigen ablösen.

3.2.3. Breite demografische Zielgruppenansprachen

Wer Werbung auf Meta schaltet, kann diese gezielt an bestimmte Zielgruppen ausspielen. Dabei lassen sich unter anderem Demografien, Interessen, Verhaltensweisen oder *Lookalike Audiences* (also Nutzer:innen, die bestehenden Kund:innen ähneln) ein- oder ausschließen. Selbst wenn bei der Anzeigenerstellung keine spezifischen Targeting-Kennzahlen angegeben werden, können die datengestützten Algorithmen von Meta über *Advantage+ Audience* automatisch relevante Nutzer:innen finden.[6]

In der Werbebibliothek wird etwaiges Targeting nur nach **demografischen Kennzahlen (Alter, Geschlecht, Standort)** angezeigt. Die Analyse zeigt jedoch, dass betrügerische Akteur:innen kaum gezielt nach diesen Parametern vorgehen. Am ehesten wird noch der Standort genutzt: Bei 36% aller Werbeanzeigen wurden Deutschland und Österreich aktiv als Zielregion eingeschlossen. Hinsichtlich des Geschlechts wurden 93% an alle Geschlechter ausgespielt, die übrigen 7% gezielt an Männer, und 64% der Anzeigen verwendeten das Standard-Alter von 18–65 Jahren als Zielgruppe.

Die Auswertung der Reichweitendaten für Österreich liefert Einblicke darin, welche Zielgruppen die Anzeigen tatsächlich erreicht haben. Sie zeigt, dass betrügerische und problematische Werbeanzeigen insgesamt ein **breites demografisches Spektrum** adressieren. 53,5% der Reichweite entfielen auf männliche Nutzer, während 44,6% auf weibliche Nutzerinnen entfielen, was auf eine leichte Überrepräsentation von Männern hinweist.

Auch die Altersverteilung deutet auf eine breite Ansprache hin, einzig eine leichte **Tendenz zu einer kaufkräftigeren Zielgruppe** lässt sich erkennen, da den größten Anteil Nutzer:innen im

[6] https://www.facebook.com/business/help/744354708981227?id=2469097953376494

mittleren und höheren Erwerbsalter ausmachen: Die Altersgruppen 35-44 Jahre (22,9%) und 45-54 Jahre (22,0%) stellen gemeinsam fast die Hälfte der erreichten Personen. Jüngere Altersgruppen wurden seltener erreicht, nur 8,7% der 18-24-Jährigen und 11,7% der 25-34-Jährigen wurden erreicht. Die folgenden Detailanalysen je Betrugsschema zeigen in manchen Bereichen deutlichere Zielgruppenansprachen – sowohl das Geschlecht als auch das Alter betreffend.

3.3. Strukturelle Gemeinsamkeiten im Betrugsökosystem

Bei der Analyse der verschiedenen Betrugsschemata zeigen sich über alle Themen hinweg strukturelle Gemeinsamkeiten, die sowohl auf systematische Strategien der Werbetreibenden hindeuten als auch auf Compliance-Lücken bei Meta selbst.

3.3.1. Intransparenz bei zahlenden Personen

Artikel 39 DSA (EU 2022/2065) schreibt vor, dass in der Werbebibliothek „die natürliche oder juristische Person, die für die Werbung bezahlt hat" ersichtlich sein muss. Diese **Transparenzpflicht** soll Nachvollziehbarkeit hinsichtlich jener Personen sicherstellen, die für die Werbeanzeigen verantwortlich sind.

Die Detailanalysen zeigen jedoch, dass über Betrugsschemata hinweg weder Namen der Werbetreibenden noch jene der Zahlenden tatsächlich Aufschluss über die verantwortlichen Personen oder Organisationen geben. Das Feld für die zahlenden Personen ist ein Freifeld („Begünstigter und Zahlender") und kann entsprechend beliebig befüllt werden. Wie unsere Datensätze zeigen, wird das auch tatsächlich genutzt – unter den Zahlenden finden sich zum Beispiel:

- Zahlenreihen wie „369", „1" oder „222"
- Willkürliche Buchstabenreihen wie „SMB" oder „wsdggggg"
- Missbrauch von Markennamen wie „Die Höhle der Löwen" (v.a. bei Nahrungsergänzungsmittel), oft wird sogar „facebook" selbst als Zahlender angegeben
- Namen von Personen, die entweder erfunden sind oder ohne deren Wissen missbraucht werden
- Namen von Fake-Unternehmen (z. B. im Falle der Ghost Stores „Lena Boutique")

Besonders augenfällig ist das Beispiel aus der Analyse zum Betrugsschema Jobbetrug: Allein bei dieser Art des Betruges ist ein Zahlender mit dem Namen oder eher der Zahl „1" für 11.712 Werbeanzeigen mit einer EU-weiten Reichweite von knapp 600.000 verantwortlich.

Dies verdeutlicht, dass die im DSA vorgesehene **Transparenz in der Praxis nicht gewährleistet ist** und diese Compliance-Lücke strukturell von den Werbetreibenden genutzt wird, um die Nachvollziehbarkeit zu erschweren. Hinzu kommt eine hohe Fragmentierung mit zahllosen verschiedenen Zahlenden, die die Identifikation organisierter Strukturen erschwert.

3.3.2. Kurze Anzeigenlaufzeiten

Ein weiteres konsistentes Muster über alle untersuchten Betrugsschemata hinweg ist die extrem kurze Laufzeit der Werbeanzeigen. Ein Großteil der betrügerischen Anzeigen ist nur **für wenige Stunden bis höchstens wenige Tage aktiv**. Bei manchen Betrugsarten waren über zwei Drittel der Anzeigen weniger als einen Tag aktiv.

Es ist davon auszugehen, dass diese Strategie der gezielten Umgehung von Sicherheitsmaßnahmen und Content-Moderation dient. Durch die hohe Anzahl kurzlebiger Anzeigen wird es sowohl für automatisierte als auch für manuelle Überprüfungssysteme schwieriger, problematische Inhalte rechtzeitig zu identifizieren und zu entfernen. Die Werbetreibenden setzen auf **Masse statt auf Dauer** und erreichen durch die permanente Neuschaltung trotz kurzer Laufzeiten erhebliche Gesamtreichweiten.

3.4. Abo-Fallen

BASISDATEN

Werbeanzeigen: 17.779

Reichweite EU: 102.402.859

Reichweite Österreich: 2.891.621

HIGHLIGHTS

Niedrigste Löschrate aller Betrugsschemata

Lange Anzeigedauer

Hohe Keyword-Konzentration

Trotz der im Vergleich zu anderen Betrugsschemata moderaten Anzahl an Werbeanzeigen erreichten die identifizierten Werbeanzeigen, die zu Abo-Fallen führen, eine hohe Reichweite, auch in Österreich. Dies lässt sich vor allem durch die **niedrige Löschrate von Meta (4,5%)** und die

gleichzeitig **lange Anzeigendauer** erklären: Anzeigen, die länger unentdeckt ausgespielt werden, erreichen automatisch mehr Nutzer:innen. Die niedrige Löschrate deutet zudem darauf hin, dass diese Werbeformate häufig in einer **regulatorischen Grauzone** zwischen irreführender und eindeutig betrügerischer Werbung operieren.

Gleichzeitig zeigt die Analyse der Keywords eine hohe Konzentration von nur wenigen Keywords: Zwei Keywords decken über 80% aller identifizierten Anzeigen ab:

- „ADHD is Not Laziness“ (50,4%)
- “How high is your IQ score” (30,7%)

3.4.1. Targeting nach Geschlecht, Alter und Standort

Bei Abo-Fallen wurde von den Werbetreibenden kein gezieltes Targeting nach Geschlecht, Alter oder Standort vorgenommen. Die Reichweitenanalyse für Österreich zeigt, dass **männliche Nutzer leicht überrepräsentiert** sind (51,8% vs. 45,7% weiblich). Hinsichtlich Alter verteilt sich die Reichweite relativ gleichmäßig über alle Altersgruppen hinweg, mit den größten Anteilen bei 35–44 Jahren (29,6%) und 45–54 Jahren (26,8%), während jüngere (18–24 Jahre, 4,1%) und ältere Nutzer:innen (65+, 9,8%) weniger erreicht werden.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	1.320.781	45,7%
Männlich	1.498.763	51,8%
Unbekannt	72.077	2,5%
Altersgruppen		
18-24 Jahre	118.464	4,1%
25-34 Jahre	331.441	11,5%
35-44 Jahre	856.859	29,6%
45-54 Jahre	774.475	26,8%
55-64 Jahre	526.018	18,2%
65+ Jahre	284.324	9,8%
Unbekannt	40	0,0%

Tabelle 2: Abo-Fallen – Reichweite nach Geschlecht und Altersgruppen

3.4.2. Werbetreibende

Die Analyse der Werbetreibenden bei Abo-Fallen zeigt ein stark fragmentiertes Bild: Es existiert eine Vielzahl unterschiedlicher Accounts, die entweder **generische Namen**, **Verweise auf das beworbene Angebot** (z. B. IQ-Tests oder Hundetraining) oder **scheinbare Firmennamen**

verwenden. Ein Großteil der Anzeigen ist auf wenige Werbetreibende konzentriert: Rund 70% der Werbeanzeigen stammen von nur drei Accounts.

Werbetreibende	Anzahl der Werbeanzeigen
Betty Holland	5.110
International IQ Test	4.757
Alison Todd	2.600
My IQ	623
Innerly	426
Jacob Holland	412
Testora	409
Max – Your Dog Training Coach	240
Today Is The Day	154
Cerebrum IQ	153

Tabelle 3: Abo-Fallen – Anzeigen nach Werbetreibenden

3.5. Investmentbetrug

BASISDATEN

Werbeanzeigen: 83.216

Reichweite innerhalb der EU: 126.665.013

Reichweite in Österreich: 21.961.476

HIGHLIGHTS

Hohe Löschrate

Hohe Keyword-Konzentration

70% der Reichweite in Österreich entfiel auf Männer

Investmentbetrug nimmt nach den Online-Glücksspielen den zweiten Platz in Bezug auf die Anzahl der Werbeanzeigen und der Reichweite innerhalb der untersuchten Betrugsschemata ein. Gleichzeitig weist diese Kategorie eine **hohe Löschrate (78,2%)** auf. Die Keyword-Analyse zeigt eine starke Dominanz weniger Begriffe. Vier Keywords decken über 90% aller Anzeigen ab („Hoss & Hopf", „Wir nehmen kein Geld – du bekommst die besten Tipps völlig kostenlos", „AI-Trading", „ChatGPT Aktien").

3.5.1. Targeting nach Geschlecht, Alter und Standort

Im Bereich Investmentbetrug wurde von den Werbetreibenden kein spezifisches Targeting vorgenommen. Geografisch liegt der Fokus auf Deutschland und Österreich (40% der Anzeigen), in kleinerem Ausmaß wurden auch Belgien und Luxemburg als Zielregion eingeschlossen.

Die Analyse der Reichweite in Österreich zeigt einen deutlichen Fokus auf **männliche Nutzer (71%)** auf. Die Altersverteilung ist hingegen relativ ausgewogen, mit einem leichten Schwerpunkt auf mittleren bis älteren Altersgruppen.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	5.997.786	27%
Männlich	15.595.367	71%
Unbekannt	368.323	2%
Altersgruppen		
18-24 Jahre	2.066.159	9%
25-34 Jahre	3.102.779	14%
35-44 Jahre	4.790.038	22%
45-54 Jahre	4.608.649	21%
55-64 Jahre	4.265.388	19%
65+ Jahre	3.128.364	14%
Unbekannt	99	0%

Tabelle 4: Investmentbetrug – Reichweite nach Geschlecht und Altersgruppen

3.5.2. Werbetreibende

Die Werbetreibenden nutzen **Trendbegriffe, bekannte Firmennamen oder Prominentennamen**, um Seriosität zu vermitteln. Auffällig ist die Konzentration auf wenige Hauptakteure: „Trade-Republic Analysieren“ schaltete fast 16.000 Anzeigen, gefolgt von mehreren Accounts rund um „Hoss & Hopf“.

Werbetreibende	Anzahl der Werbeanzeigen
Trade-Republic Analysieren	15.999
Hoss & Hopf	3.836
T- R	3.030
Hoss	2.979
Philip Hopf	2.477
Chat gpt 5	1.608
Hoss & Hopf	1.462
Gerald Hörhan	1.282
Fxalgo Media	1.105
Cooper Phillip	929

Tabelle 5: Investmentbetrug – Anzeigen nach Werbetreibenden

3.6. Kreditbetrug

BASISDATEN

Werbeanzeigen: 805

Reichweite EU: 236.180

Reichweite Österreich: 121.344

HIGHLIGHTS

Vergleichsweise niedrige Löschrate

Großer Anteil der Reichweite entfällt auf Österreich

Österreichische Reichweite entfällt auf Personen über 55 Jahren

Kreditbetrug weist im Vergleich zu anderen Betrugsschemata die **geringste Anzahl an Werbeanzeigen** auf. Diese vergleichsweise niedrigen Zahlen können methodisch bedingt sein, da zu Beginn der Erhebung noch keine belastbaren Erkenntnisse darüber vorlagen, welche Keywords zur Identifikation geeignet sind und mit welchen Narrativen bzw. Begrifflichkeiten das Betrugsschema beworben wird. Dabei dominierte das Keyword „Privatkredite ohne Papierkram" mit 50,3%. Weitere typische Keywords wie „trotz Schufa" verdeutlichen, dass betrügerische Akteur:innen auf Personen in finanziellen Notlagen abzielen. Auffällig ist zudem eine im Vergleich zu den anderen Betrugsschemata **niedrige Löschrate von 11,8%**.

3.6.1. Targeting nach Geschlecht, Alter und Standort

Von den Werbetreibenden wurde kein spezifisches Targeting nach Geschlecht oder Alter vorgenommen. Das geografische Targeting zeigt eine starke Konzentration auf den deutschsprachigen Raum: Die überwiegende Mehrheit der Anzeigen (über 80%) zielt auf **Österreich, Deutschland und Luxemburg** ab, wobei manche Anzeigen auch Schweden einschließen.

Dennoch liegt der Anteil der in Österreich erreichten Nutzer:innen mit 51,4% deutlich über dem Durchschnitt von 12,2%. Die Reichweitenanalyse für Österreich zeigt außerdem, dass 67,4% der erreichten Nutzer:innen männlich sind. Bei der Altersverteilung liegt der Schwerpunkt auf älteren Zielgruppen: Die Altersgruppe 55-64 Jahre stellt mit 27,3% den größten Anteil dar, gefolgt von 65+ mit 25,7%. Zusammen entfallen **53% der Reichweite auf Personen über 55 Jahre.**

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	38.360	32%
Männlich	81.799	67%
Unbekannt	1.185	1%
Altersgruppen		
18-24 Jahre	13.496	11%
25-34 Jahre	2.518	2%
35-44 Jahre	15.873	13%
45-54 Jahre	25.194	21%
55-64 Jahre	33.072	27%
65+ Jahre	31.188	26%
Unbekannt	3	0%

Tabelle 6: Kreditbetrug – Reichweite nach Geschlecht und Altersgruppen

3.6.2. Werbetreibende

Die Analyse der Werbetreibenden zeigt ein stark fragmentiertes Bild mit einer Vielzahl verschiedener Accounts mit generischen Namen.

Werbetreibende	Anzahl der Werbeanzeigen
F&M GLOBAL BRANDS SERVICOS LTDA	323
Media Hub	147
BLOG DIGITAL	79
F & M GLOBAL BRANDS	30
OBMedia LLC	20
NewsTrends	18
AG MARKETING DIGITAL LTDA	16
RL Media Sp z oo Sp k	15
Eduarda Oliveira	14

Tabelle 7: Kreditbetrug – Anzeigen nach Werbetreibenden

3.7. Jobbetrug

BASISDATEN

Werbeanzeigen: 18.140

Reichweite EU: 17.265.387

Reichweite Österreich: 15.757.809

HIGHLIGHTS

Sehr starker Fokus auf Österreich mit 91,3% der gesamten EU-Reichweite

Hohe Löschrate & hohe Keyword-Dichte

Überwiegend Personen im erwerbsfähigen Alter erreicht

Jobbetrug zeigt den mit Abstand höchsten Österreich-Anteil aller Betrugsschemata: 91,3% der EU-weiten Reichweite entfallen auf österreichische Nutzer:innen. Dies deutet auf eine sehr gezielte Kampagnenausrichtung auf Österreich hin. Gleichzeitig sehen wir sowohl eine **hohe Löschrate mit 78%** als auch eine hohe Keyword-Dichte – 89% entfallen auf das Keyword „Keine Erfahrung erforderlich".

3.7.1. Targeting nach Geschlecht, Alter und Standort

Von den Werbetreibenden wurde kaum Targeting nach Alter oder Geschlecht durchgeführt. Anders als bei anderen Betrugsschemata zeigt sich jedoch ein deutlich stärkerer Fokus auf den **österreichischen Markt:** Von der EU-Gesamtreichweite von 17,3 Millionen entfallen 15,8 Millionen auf Österreich. Nur vereinzelt wurden Anzeigen mit sehr spezifischem lokalem Targeting (z. B. einzelne Städte) oder breitere geografische Regionen (EU, EWR) identifiziert.

Die Reichweitenanalyse für Österreich zeigt zudem eine Fokussierung auf **Personen im erwerbsfähigen Alter:** Die Altersgruppe 35-44 Jahre stellt mit 33,2% den größten Anteil, gefolgt von 45-54 Jahren mit 26,7%. Insgesamt entfallen 50,7% der Reichweite auf Personen ab 45 Jahren. Zudem sind 62% der erreichten Nutzer:innen weiblich.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	9.847.003	62%
Männlich	5.557.742	35%
Unbekannt	353.064	2%
Altersgruppen		
18-24 Jahre	344.286	2%
25-34 Jahre	2.186.612	14%
35-44 Jahre	5.236.441	33%
45-54 Jahre	4.213.032	27%
55-64 Jahre	2.579.193	16%
65+ Jahre	1.197.729	8%
Unbekannt	516	0%

Tabelle 8: Jobbetrug – Reichweite nach Geschlecht und Altersgruppen

3.7.2. Werbetreibende

Im Bereich des Jobbetrugs wird stark auf **unbekannte Namen** gesetzt. Da der Großteil dieser Seiten zum Erhebungszeitraum Ende Dezember nicht mehr online war, ist nicht nachvollziehbar, ob es sich um kompromittierte Nutzer:innen-Konten oder um eigens für die Betrugsmaschen erstellte Konten mit Fake-Personas handelt.

Werbetreibende	Anzahl der Werbeanzeigen
Natalia Scully Brady	1.119
Brandon Ryan McDaniel	434
Smith Roy Peffley	366
Grace Ruggeri Emily	363
Jr. Deanna Dolch	312
Manaayy Conomon Collazo	251
Tabitha Onions2	217
Miller Malik Mills	200
Elwell Certesio Karma	200
Katie Seelig Barbara	199

Tabelle 9: Jobbetrug – Anzeigen nach Werbetreibenden

3.8. Unseriöse Nahrungsergänzungsmittelangebote

BASISDATEN

Werbeanzeigen: 27.171

Reichweite EU: 53.837.455

Reichweite Österreich: 10.927.574

HIGHLIGHTS

Massiver Missbrauch der Sendung „Höhle der Löwen“

74% der erreichten Personen über 45 Jahre alt

Frauen in der Reichweite überrepräsentiert

Unseriöse Nahrungsergänzungsmittelangebote erreichen mit einer **EU-weiten Reichweite von über 53 Millionen** sehr viele Nutzer:innen. Die Löschrate von 52% zeigt, dass Meta etwa die Hälfte der Anzeigen zum Erhebungszeitpunkt als problematisch erkennt, während die andere Hälfte ungehindert ausgespielt wird – was insbesondere hinsichtlich der laut Meta-Werberichtlinien strengeren Regelungen im Kontext von Gesundheitswerbung problematisch ist. Auffällig ist zudem der systematische Missbrauch des Namens der TV-Sendung „Die Höhle der Löwen“ – auf dieses Keyword entfielen 78% aller Werbeanzeigen.

3.8.1. Targeting nach Geschlecht, Alter und Standort

Von den Werbetreibenden wurde bei 94% der Anzeigen kein Targeting nach Alter oder Geschlecht vorgenommen. Die Reichweitenanalyse für Österreich zeigt jedoch ein klares Muster: 74% der Reichweite entfallen auf **Personen ab 45 Jahren**, wobei die Gruppe 65+ mit knapp 30% den größten Anteil stellt. Auch Frauen sind mit 60% deutlich überrepräsentiert. Dies entspricht der typischen Zielgruppe für Gesundheitsprodukte.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	6.532.996	60%
Männlich	4.241.489	39%
Unbekannt	153.089	1%
Altersgruppen		
18-24 Jahre	1.848.431	17%
25-34 Jahre	167.250	2%
35-44 Jahre	859.146	8%
45-54 Jahre	1.917.918	18%
55-64 Jahre	2.890.556	26%
65+ Jahre	3.244.244	30%
Unbekannt	29	0%

Tabelle 10: Unseriöse Nahrungsergänzungsmittel – Reichweite nach Geschlecht und Altersgruppen

3.8.2. Werbetreibende

Die Benennung der Werbetreibenden gibt einen Einblick darin, wie die unseriösen Anbieter arbeiten: So zeigt sich eine starke Dominanz der Werbetreibenden-Namen von unterschiedlichen **Variationen des Namens „Die Höhle der Löwen“**. Dies zeigt, dass in diesem Bereich massiv die bekannte Investment-Sendung missbraucht wird, um den beworbenen Produkten Glaubwürdigkeit zu verleihen.

Werbetreibende	Anzahl der Werbeanzeigen
Die Höhle der Löwen	1.700
Höhle des Löwen	1.327
Die Höhle der Löwen	1.070
Höhle der Löwen	956
Klinik VitalLuft München	930
Die Höhle der Löwe	916
Fabuleux	686
Dr. Leon Schulte	626
Die Höhle der Löwen - VOX 2023	534
Vitales Leben	465

Tabelle 11: Unseriöse Nahrungsergänzungsmittel – Anzeigen nach Werbetreibenden

3.9. Ghost Stores

BASISDATEN

Werbeanzeigen: 9.955

Reichweite EU: 21.407.495

Reichweite Österreich: 4.751.404

HIGHLIGHTS

Niedrige Löschrate

Frauen und ältere Personen in der Reichweite überrepräsentiert

Ghost Stores weisen mit **26,9% die zweitniedrigste Löschrate** aller Betrugsschemata auf. Dies geht auch damit einher, dass die Angebote in einer Grauzone operieren und nicht strafrechtlich relevant sind. Stattdessen verstoßen sie aufgrund irreführender Werbepraktiken gegen das Gesetz gegen den unlauteren Wettbewerb sowie gegen weitere Konsumentenschutzgesetze.

3.9.1. Targeting nach Geschlecht, Alter und Standort

Bei der überwiegenden Mehrheit der Anzeigen wurde von den Werbetreibenden kein spezifisches Targeting nach Alter oder Geschlecht vorgenommen. Nur in **12,8% der Fälle** richteten sich die Anzeigen gezielt an **Männer** und in 3,2% an Frauen. Bei der Reichweitenanalyse für Österreich zeigt sich ein deutlicherer Fokus – jedoch weniger auf Männer als auf Frauen, gleichzeitig wird eine eher ältere Zielgruppe erreicht: Die Altersgruppe 65+ stellt mit 26% den größten Anteil, gefolgt von der Altersgruppe zwischen 55-64 Jahren mit 22%. Gleichzeitig entfielen 60% der Reichweite auf Frauen.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	2.851.510	60%
Männlich	1.819.518	38%
Unbekannt	80.376	2%
Altersgruppen		
18-24 Jahre	846.379	18%
25-34 Jahre	295.030	6%
35-44 Jahre	581.269	12%
45-54 Jahre	733.441	15%
55-64 Jahre	1.037.942	22%
65+ Jahre	1 257 283	26%
Unbekannt	60	0%

Tabelle 12: Ghost Stores – Reichweite nach Geschlecht und Altersgruppen

3.9.2. Werbetreibende

Die Analyse der Werbetreibenden zeigt eine hohe Übereinstimmung zwischen den Namen der werbenden Accounts und den beworbenen Shop-Namen (inkl. der tatsächlichen Shop-Domains). Werbetreibende wie „Elle Weber", „Modehaus Berfeld" oder „Lena-Boutique" entsprechen gleichzeitig den für Ghost Stores identifizierten Keywords.

Werbetreibende	Anzahl der Werbeanzeigen
Elle Weber	2.256
Modehaus Berfeld	1.887
Lena-Boutique	1.830
Lena Boutique Berlin	1.105
Moser Wien	1.074
Muller Graz	518
Mirella Modehaus	466
Alpina Modehaus Wien	183
Thera Boutique Graz	106
Weber Atelier	104

Tabelle 13: Ghost Stores – Anzeigen nach Werbetreibenden

3.10. Fake-Shops (Markenimitationen)

BASISDATEN

Werbeanzeigen: 28.276

Reichweite EU: 65.931.501

Reichweite Österreich: 2.024.487

HIGHLIGHTS

Dominanz von Lidl-Missbrauch

Überwiegend Männer erreicht

Breites EU-Targeting

Fake-Shops mit Markenimitationen zeigen eine starke inhaltliche Konzentration: **86,4%** aller Anzeigen entfallen auf das **Keyword 'Lidl Discount'**. Dies bestätigt Beobachtungen von Expert:innen der Watchlist Internet, die in den vergangenen Monaten eine Häufung von Fake-Shops dokumentierten, die den Namen des Diskonters missbrauchen. Die Löschrate liegt bei 41,6%.

3.10.1. Targeting nach Geschlecht, Alter und Standort

Bei der überwiegenden Mehrheit der Anzeigen (94%) wurde von den Werbetreibenden kein spezifisches Targeting nach Alter oder Geschlecht vorgenommen. Nur 5,2% der Anzeigen richteten sich gezielt an Männer, weniger als ein Prozent an Frauen. Das geografische Targeting ist allerdings breiter gestreut als bei anderen Betrugsschemata und zielt häufig auf Gesamt-Europa bzw. den EU-Raum ab. Entsprechend entfallen auch **nur 3,1% der EU-Reichweite auf Österreich**. 71% der erreichten Nutzer:innen sind dabei männlich. Bei der Altersverteilung entfallen 48,5% auf Personen über 55 Jahre.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	547.436	27%
Männlich	1.444.321	71%
Unbekannt	32.730	2%
Altersgruppen		
18-24 Jahre	321.385	16%
25-34 Jahre	60.212	3%
35-44 Jahre	284.011	14%
45-54 Jahre	377.169	19%
55-64 Jahre	471.440	23%
65+ Jahre	510.262	25%
Unbekannt	60	0%

Tabelle 14: Fake-Shops - Reichweite nach Geschlecht und Altersgruppen

3.10.2. Werbetreibende

Die Top-Werbetreibenden nutzen Namen wie **„Discount Store“** oder **ahmen bekannte Supermärkte wie Lidl oder Hofer** nach, wobei die Namen leicht von den tatsächlichen Markennamen abweichen: Zum Beispiel wird bei „H0Fer“ das „O“ mit einer „Null (0)“ ersetzt.

Werbetreibende	Anzahl der Werbeanzeigen
Discount Store	2.328
Online Discount Stores	2.148
Discount Shop	1.556
Discount stores	1.288
L&i Wholesale Mall	913
LiDL Shop	848
Online Discount Shop	770
Online-Discount.Shop	596
Lidl discount mall	593
H0FER	591

Tabelle 15: Fake-Shops – Anzeigen der werbetreibenden Person

3.11. Online-Glücksspiele

BASISDATEN (hochgerechnet)

Werbeanzeigen: 448.699

Reichweite EU: 620.572.304

Reichweite Österreich: 64.790.612

HIGHLIGHTS

Höchste Anzahl der Werbeanzeigen und Reichweite trotz geringer Keyword-Anzahl

Höchste Löschrate (82%)

25% der Werbeanzeigen wurden gezielt an Männer ausgespielt

Online-Glücksspiele stellen mit Abstand das **größte Betrugsschema** dar – sowohl nach Anzahl der Anzeigen als auch nach Reichweite – und das, obwohl die Anzahl der Keywords auf vier Suchbegriffe limitiert wurde. Gleichzeitig musste für das Keyword „Chicken Road" der Erhebungszeitraum auf eine Woche (statt drei Monate) gekürzt werden. Grund für diese Limitierungen ist, dass die Suche nach betrügerischen Online-Glücksspielangeboten die Ratenbegrenzung der Meta-API deutlich überschritten hätte. Um dennoch eine Vergleichbarkeit mit den anderen Betrugsschemata zu gewährleisten, wurden alle wichtigen Kennzahlen hochgerechnet. Die ermittelten Anzeigenzahlen wurden dabei linear auf den gesamten Erhebungszeitraum von drei Monaten hochgerechnet (Faktor ×13).

Hochgerechnet wurden 448.699 Werbeanzeigen mit einer EU-weiten Reichweite von etwas über 620 Millionen innerhalb des Erhebungszeitraums ermittelt. Auffällig bei diesem Betrugsschema ist, dass Meta **82% der identifizierten Werbeanzeigen bereits entfernt** hat.

3.11.1. Targeting nach Geschlecht, Alter und Standort

Während bei 75% der Anzeigen von den Werbetreibenden kein spezifisches Targeting nach Alter oder Geschlecht vorgenommen wurde, richteten sich **25% gezielt an Männer.** Die Reichweitenanalyse zeigt ein ähnliches Bild: 70% der erreichten Nutzer:innen sind männlich, nur 28% weiblich. Bei der Altersverteilung zeigt sich ein Fokus auf Zielgruppen zwischen 25 und 55 Jahren, auf die insgesamt 80% der Reichweite entfällt.

Kategorie	Reichweite	Anteil
Geschlecht		
Weiblich	18.063.938	28%
Männlich	45.286.921	70%
Unbekannt	1.439.753	2%
Altersgruppen		
18-24 Jahre	842.189	1%
25-34 Jahre	13.497.856	21%
35-44 Jahre	21.762.612	34%
45-54 Jahre	16.423.450	25%
55-64 Jahre	8.751.400	14%
65+ Jahre	3.512.839	5%
Unbekannt	266	0%

Tabelle 16: Online-Glücksspiele – Reichweite nach Geschlecht und Altersgruppen

3.11.2. Werbetreibende

Insgesamt konnten 1.368 individuelle Werbetreibende identifiziert werden mit 7.558 Begünstigten/Zahlenden. Die Top-Werbetreibenden nutzen Namen wie „Chicken Road" oder Variationen davon. Oft werden auch generische Namen wie „Big Win", „Touch of Fortune" oder „Glücksspiel Österreich" verwendet. Teilweise werden auch Namen von bekannten Casinos nachgeahmt wie „Casino Austria" oder „Casino Wien".

Werbetreibende	Anzahl der Werbeanzeigen
Chicken Road	44.952
Chicken Road Slots	37.140
Chicken Road 2	22.404
Best Games	9.912
Ćhićken Røad Româŋiα	7.980
Chicken Game	7.812
Epic Adventure	7.620
Chicken Road2	5.892
Bonus Slot	5.388
Chicken Road X100	5.172

Tabelle 17: Online-Glücksspiele – Anzeigen der werbetreibenden Person

3.12. Fazit

Die quantitative Analyse dokumentiert die Größenordnung betrügerischer und problematischer Werbung auf Plattformen des Unternehmens Meta: **634.000 Werbeanzeigen** erreichten innerhalb von drei Monaten mehr als 1 Milliarde Impressionen EU-weit und 123 Millionen in Österreich. Wie in Kapitel 4.3 (Strukturelle Gemeinsamkeiten im Betrugsökosystem) dargestellt, lassen sich über alle Betrugsschemata hinweg strukturelle Gemeinsamkeiten erkennen –

insbesondere **kurze Anzeigenlaufzeiten** sowie fehlende Informationen über die werbetreibenden Personen bzw. jene Personen, die für eine Anzeige zahlen.

Die Daten zeigen gleichzeitig deutliche Unterschiede zwischen den Betrugsschemata – sowohl hinsichtlich der Größenordnung als auch der Zielgruppenansprache sowie der aktiven Entfernung der Anzeigen vonseiten Meta.

Online-Glücksspiele dominieren mit knapp 450.000 Anzeigen und einer Reichweite von über 620 Millionen sowohl in Volumen als auch in Reichweite – obwohl die Erhebung auf nur vier Keywords und einen verkürzten Zeitraum limitiert werden musste. Investmentbetrug folgt mit 83.000 Anzeigen und der zweithöchsten Reichweite, während im Bereich Kreditbetrug mit 805 Anzeigen die wenigsten Werbeanzeigen gefunden wurden.

Auch bei der **Zielgruppenansprache** zeigen sich schema-spezifische Profile: Nahrungsergänzungsmittel erreichen überproportional Frauen und Personen ab 45 Jahren, während Investmentbetrug und Kreditbetrug vor allem Männern über 55, Jobbetrug Frauen im erwerbsfähigen Alter und Online-Glücksspiele überwiegend Männer erreichen.

Die **Gesamtlöschrate liegt bei 62,4%**, variiert jedoch erheblich zwischen den Betrugsschemata: Während Werbeanzeigen für Online-Glücksspiele, Jobbetrug und Investmentbetrug hohe Löschraten aufweisen, werden Abo-Fallen, Ghost Stores und insbesondere Kreditbetrug kaum entfernt. Die Gründe für dieses Gefälle sind nicht eindeutig nachvollziehbar – es korreliert weder durchgehend mit der strafrechtlichen Relevanz der Inhalte noch mit deren Ausmaß. Deutlich wird jedoch, dass manche der Betrugsschemata von der bestehenden Content-Moderation weniger erfasst werden.

4. Qualitative Analyse

4.1. Methodisches Vorgehen

Für die qualitative Beschreibung der jeweiligen Betrugsschemata wurde eine **kriteriengeleitete Stichprobenziehung** durchgeführt, die darauf abzielt, jene Werbeanzeigen zu erfassen, die aufgrund ihrer Häufigkeit und Reichweite die größte Wirksamkeit auf Nutzer:innen entfalten.

Grundlage dieser Auswahl bildeten die Crawler-Ergebnisse der quantitativen Erhebung. Je Betrugsschema wurden die fünf Keywords mit der höchsten Anzahl von individuellen Werbeanzeigen herangezogen. Innerhalb dieser Keywords wurden wiederum die Anzeigenbeschreibungen nach Häufigkeit sortiert und zu den jeweils häufigsten Beschreibungen die Werbeanzeigen mit der höchsten EU-Reichweite ausgewählt.

In Fällen, in denen eine ausgewählte Anzeige bereits von Meta entfernt worden war oder die Landing Page nicht mehr erreichbar war, wurden durch eine erneute Suche in der Werbebibliothek ähnliche Anzeigen identifiziert. **Pro Betrugsschema** umfasst das Stichproben-Set **zehn exemplarische Werbeanzeigen**. Bei der Auswahl dieser wurde auch auf thematische Varianz je Betrugsschema geachtet, um unterschiedliche Narrative erheben zu können.

Die ausgewählten Werbeanzeigen wurden anschließend entlang folgender Analysedimensionen ausgewertet:

- Eingesetzte Narrative
- Visuelle Strategien, inkl. Einsatz von KI-basierter Bild- und Videogenerierung
- Inhaltliche Zielgruppenansprache
- Verwendete Weiterleitungs-Infrastruktur
- Beobachtbare Täterstrategien zur Umgehung von Content-Moderation

Die dabei identifizierten wiederkehrenden Muster wurden zu übergeordneten Strategien verdichtet.

4.2. Täterstrategien zur Umgehung von Sicherheitsmechanismen

Täter:innen wenden beim Schalten betrügerischer Werbeanzeigen verschiedene Methoden und Strategien an, um die Content-Moderation sowie Sicherheitsmechanismen der Plattformen zu umgehen. Diese Praktiken erschweren Forscher:innen, Regulierungsbehörden und auch der Content-Moderation der Plattformen die systematische Überprüfung und Dokumentation

problematischer und betrügerischer Werbeanzeigen – und stellen damit auch für die vorliegende Studie eine methodische Einschränkung dar. Im Folgenden werden die im Rahmen der Analyse identifizierten Umgehungsstrategien dargestellt und in den Kontext bestehender Forschungs- und Regulierungserkenntnisse eingebettet.

4.2.1. Cloaking

Beim Cloaking wird den **Überprüfungssystemen der Plattform** (dazu zählt auch das Suchen über die Werbebibliothek) eine andere Version der verlinkten Website angezeigt als den tatsächlichen Nutzer:innen, die z. B. während des Scrollens in ihrem Feed auf eine Werbeanzeige klicken. Während automatisierte Prüfsysteme und Personen, die über die Werbebibliothek auf eine Anzeige klicken, eine unauffällige und neutrale Website sehen (die sogenannte „White Page"), werden Nutzer:innen aus dem Feed heraus zu den tatsächlichen betrügerischen Inhalten und Verkaufsseiten weitergeleitet (die sogenannte „Black Page").

Diese Strategie ist schon länger bekannt: Bereits 2020 klagte Meta selbst gegen den Anbieter „LeadCloak", dessen Software unter anderem dafür genutzt wurde, um automatisierte Anzeigenprüfungssysteme zu umgehen (Sapra, 2020). Die Anbieter dieser Cloaking-Technologien professionalisieren sich dabei zunehmend. Sicherheitsforscher:innen sprechen von einem wachsenden Ökosystem von „Cloaking-as-a-Service"-Anbietern (Burt, 2025), die ihre Dienste mittlerweile offen anbieten. Diese erhöhte Verfügbarkeit und Zugänglichkeit senkt die technische Einstiegshürde und ermöglicht auch weniger technisch versierten betrügerischen Akteur:innen den Einsatz dieser Umgehungsstrategie.

4.2.2. Nutzung von kompromittierten Accounts

Eine weitere Umgehungsstrategie besteht in der Nutzung kompromittierter Accounts. Dabei werden kompromittierte Nutzer:innen-Konten – häufig **verifizierte Profile von Prominenten** – verwendet, um betrügerische Werbeanzeigen zu schalten. Auch dieses Phänomen ist nicht neu und wird von unterschiedlichen Sicherheitsforscher:innen dokumentiert. 2023 wurden zum Beispiel mehrere verifizierte und kompromittierte Konten bekannt, die sich nach offiziellen Unternehmen wie „Meta Ads", „Meta Ads Manager" oder „Google AI" umbenannten und als solche über das Schalten von Werbeanzeigen Malware verbreiteten (Hatmaker, 2023). Durch die Nutzung solcher kompromittierter Konten wird den Werbeanzeigen zusätzliche Glaubwürdigkeit verliehen, zugleich sorgen bereits große Follower-Zahlen für eine erhöhte Sichtbarkeit von organischen Inhalten.

4.2.3. Multiple Anzeigenversionen & „Chameleon ads“

Das Ausspielen mehrerer Anzeigenversionen innerhalb einer einzigen Kampagne stellt eine weitere identifizierte Umgehungsstrategie dar. Möglich wird dies durch die von Meta bereitgestellte Funktion der **dynamischen Anzeigengestaltung**, bei der je nach Zielgruppe unterschiedliche Versionen ausgespielt werden. Während die meisten dieser Anzeigenversionen harmlos erscheinen, enthält zumindest eine Anzeige problematische oder betrügerische Inhalte. Dabei kann sich nicht nur das Anzeigenbild oder Video sowie der Anzeigentext von Version zu Version unterscheiden, sondern auch der Link, zu dem weitergeleitet wird.

Diese Strategie erschwert sowohl die automatisierte Erkennung als auch die manuelle Überprüfung, da die betrügerischen Inhalte hinter auf den ersten Blick unverdächtigem Material verborgen werden. Dazu kommt, dass Sicherheitsforscher:innen zusätzlich vermuten, dass dabei eine weitere Taktik namens **„Chameleon ads“** zum Einsatz kommt. Dabei laden Betrüger:innen beim Erstellen der Werbeanzeige zunächst nur die harmlos aussehenden Anzeigen hoch. Sobald die Anzeige genehmigt wurde, werden Bilder, Texte und Links durch betrügerische Inhalte ersetzt (Social MediaLab, 2025).

4.3. Narrative, Zielgruppenansprache & genutzte Infrastrukturen

Die qualitative Analyse der einzelnen Betrugsschemata zeigt trotz thematischer Unterschiede deutliche Gemeinsamkeiten. Diese betreffen die eingesetzten Narrative und Strategien, die Zielgruppenansprache sowie teilweise auch die genutzten Infrastrukturen im weiteren Verlauf des Betrugs. Im Folgenden werden drei Muster dargestellt, die in vielen der untersuchten Betrugsschemata in variierender Ausprägung beobachtet werden konnten: (1) der Einsatz von Deceptive Design, (2) die gezielte Erzeugung von Wissenslücken („curiosity gap“) und (3) der Missbrauch etablierter Vertrauensanker.

4.3.1. Deceptive Design

Als Deceptive Design – ursprünglich von Harry Brignull geprägt und unter dem Begriff „Dark Patterns“ bekannt – werden Benutzeroberflächen bezeichnet, die durch den **gezielten Einsatz von manipulativen Gestaltungselementen** Nutzer:innen dazu verleiten, gegen ihre eigenen Interessen zu handeln, wie z. B. durch überstürzte Kaufentscheidungen (Brignull, 2023). Im digitalen Raum begegnen uns solche Muster in vielfältigen Formen, oftmals auch in Kombination: Online-Shops arbeiten zum Beispiel mit künstlichen Verknappungen („Nur noch 2 Artikel verfügbar!“) und

erzeugen so einen Kaufdruck. Mit dem Lockvogeltrick (Bait-and-Switch) werden scheinbar „kostenlose“ Angebote beworben, die sich später als teure Abonnements herausstellen. Und mit Sätzen wie „386 Personen haben dieses Produkt heute schon gekauft“ wird sozialer Druck vorgetäuscht, der zum Kauf animieren soll (Beltzung et al., 2024).

Deceptive Design ist aus mehreren Gründen problematisch: Es untergräbt die informierte Entscheidungsfreiheit der Nutzer:innen, schafft ein strukturelles Machtungleichgewicht zugunsten der Unternehmen oder Werbetreibenden und kann zu messbaren Schäden führen – etwa durch ungewollte Vertragsabschlüsse, unbeabsichtigte Datenweitergabe oder finanzielle Verluste (Brignull, 2023). Angesichts dieser Risiken gerät Deceptive Design zunehmend in den Fokus von Verbraucherschutzbehörden.

In den untersuchten Betrugsschemata bilden solche Design-Elemente eine zentrale Grundlage der von den Werbetreibenden verwendeten Narrative, um Konsument:innen zu schnellen und unüberlegten Handlungen zu verleiten. Besonders verbreitet sind dabei **künstliche Verknappung** sowie eine ebenso **künstlich erzeugte Dringlichkeit** – von zeitlich begrenzten Kreditangeboten („Nur noch heute!“) über limitierte Plätze in vermeintlichen Investment-Communities („Nur für die ersten 1000 Anmeldenden“) bis hin zu ablaufenden Rabattaktionen bei Ghost Stores und Fake-Shops.

Starke Verwendung findet zudem das „**Confirmshaming“**: Dabei soll die Entscheidungsfindung der Nutzer:innen durch das Auslösen von unangenehmen Emotionen beeinflusst werden. Etwa indem das Nicht-Teilnehmen an IQ-Tests oder ADHS-Screenings (siehe Abo-Fallen) implizit als Eingeständnis von Unwissenheit oder Passivität gerahmt werden oder das Nicht-Beitreten zu vermeintlichen Insider-Gruppen (Investmentbetrug) als verpasste Chance inszeniert wird.

Ein weiteres Deceptive Design-Element ist **Interface Interference**, also Manipulationen der Benutzeroberfläche, die bestimmte Aktionen gegenüber anderen hervorheben, um so die Handlungsoptionen zumindest visuell einzuschränken (Gray et al., 2018). Dieses Element wird insbesondere auf den Landing Pages, zu denen die Werbeanzeigen weiterleiten, verwendet. Auf manchen der Landing Pages dominieren großflächige, farblich hervorgehobene Call-to-Action-Buttons (z. B. „Jetzt kaufen“, „Kostenlos testen“) die visuelle Hierarchie, während Optionen zum Abbrechen oder zu den Vertragsbedingungen durch kleinere Schriftgrößen, geringeren Kontrast oder Platzierungen am Rand kaum sichtbar sind.

4.3.2. Curiosity Gap

In mehreren Betrugsschemata wird systematisch der sogenannte Curiosity Gap genutzt – also das **gezielte Konstruieren einer Wissenslücke**, die bei den Konsument:innen einen starken Handlungsimpuls erzeugen sollen. Wird einer Person bewusst gemacht, dass ihr eine bestimmte Information fehlt, entsteht ein gefühlter Spannungszustand, der erst durch das Schließen der Wissenslücke gelöst werden kann. Im Kontext von Online-Werbung – und zwar nicht nur betrügerischer – wird dieser Mechanismus gezielt eingesetzt. Ein prominentes Beispiel sind Clickbait-Überschriften, die mit Formulierungen wie „Diese neue Methode wird dich staunen lassen" oder „Diesen Trick kennt niemand" zum Klicken verleiten sollen. Die gleichzeitige Verwendung von Superlativen oder anderen intensivierenden Wörtern erhöht die wahrgenommene Relevanz der fehlenden Information und so auch den Impuls, die Wissenslücke schließen zu müssen (Scott, 2021).

Wenig überraschend wird der Curiosity Gap auch im Kontext betrügerischer und problematischer Werbeanzeigen gezielt genutzt: Angefangen bei Abo-Fallen die **selbstbezogene Wissenslücken** erzeugen („Wie hoch ist dein IQ wirklich?" oder „Bist du schlauer als der durchschnittliche Deutsche?") über das **Referenzieren von angeblichem Insider-Wissen** im Bereich Investmentbetrug („Die neue Plattform hat bereits die Effizienz des Bankensystems gefährdet" oder „Viele Leute wissen nicht, wie man Aktien auswählt") bis hin zu Bewerbungen unseriöser Nahrungsergänzungsmittel, die häufig mit **angstauslösenden Elementen** kombiniert werden („Er trug ein Geheiminis in sich, das niemand erfahren sollte."). Letzteres zeigt zudem, dass der Curiosity Gap häufig mit emotionaler Aktivierung kombiniert wird und so verstärkt wirkt. Auch durch Aussagen wie „Dein IQ ist vermutlich niedriger als du denkst" oder „Nur für Österreichische Staatsbürger" kann die kritische Bewertung von Informationen beeinträchtigt werden. Dabei werden gezielt innere Einflüsse (*visceral influence*) angesprochen, wie zum Beispiel Selbstzweifel, Dringlichkeit und Exklusivitätsempfinden (Langenderfer & Shimp, 2001).

4.3.3. Missbrauch etablierter Vertrauensanker

Ein weiteres übergreifendes Muster ist der systematische Missbrauch von Bekanntem – seien es Personen, Marken, Institutionen oder der Bezug auf Regionalität. Die analysierten Werbetreibenden nutzen diese Strategie, da Menschen Informationen und Aufforderungen eher als glaubwürdig bewerten und folgen, wenn sie von einer als autoritativ wahrgenommenen Quelle stammen (Stajano & Wilson, 2011). Das bereits 1986 entwickelte Elaboration Likelihood Model (ELM) findet mittlerweile auch im Kontext von Online-Betrug Anwendung (Norris et al., 2019). Laut dieses

Models greifen Personen bei der Konfrontation mit einer Botschaft – wenn ihnen Motivation oder Fähigkeiten zur Überprüfung fehlen – auf Hinweisreize wie bekannte Namen, Logos oder prominente Gesichter als Bewertungsgrundlage zurück. Dieses Verhalten wird insbesondere auf Sozialen Netzwerken relevant, da sie oftmals mit geringen Aufmerksamkeitsspannen und zeitgleicher hohen Informationsflut einhergehen.

In den analysierten Werbeanzeigen werden etablierte Vertrauensanker durch unterschiedliche Strategien missbraucht:

(1) In mehreren Betrugsschemata werden gezielt **Namen, Bilder sowie KI-generierte Deepfake-Videos bekannter Persönlichkeiten missbraucht**, um den beworbenen Angeboten Glaubwürdigkeit zu verleihen. Im Bereich des Investmentbetrugs werden etwa Personen wie der ehemalige österreichische Finanzminister Hans Jörg Schelling oder der Finfluencer Philip Hopf zur Bewerbung genutzt. Im Bereich der unseriösen Nahrungsergänzungsmittel sind es hingegen medizinische Autoritäten, wie der Arzt und Kabarettist Eckhart von Hirschhausen oder der ORF-Arzt Siegfried Meryn.

(2) Neben der Nutzung der Autorität von bestimmten Personen wird außerdem auf die **Bekanntheit und das Vertrauen kommerzieller und medialer Marken** gesetzt. Bei unseriösen Angeboten von Nahrungsergänzungsmittel dominiert zum Beispiel der systematische Missbrauch der TV-Sendung „Die Höhle der Löwen“ (Name, Logo, Investoren). Fake-Shops imitieren gezielt Marken bzw. Lebensmittelketten wie Lidl, Hofer, Swarovski oder Birkenstock; Online-Casinos schmücken sich mit Namen wie „Casino Austria“ oder „Casino Baden“ und Investmentbetrüger nutzen Namen und Logos von Medien wie oe24, ORF oder Kronen Zeitung.

(3) Eine dritte Ausprägung beruht weniger auf Autorität im engen Sinne, sondern auf der Annahme, dass **regionale Angebote als plausibel und vertrauenswürdig** gelten. Diese Konstruktion lokaler Zugehörigkeit machen sich insbesondere Akteur:innen des Betrugsschemas Ghost Stores zu Nutze, indem Geschäftsnamen wie „Schneider Salzburg“ oder „Muller Graz“ einen lokalen – zumeist auch noch familiengeführten – Betrieb suggerieren.

4.3.4. Ausnutzung situativer Vulnerabilitäten

In der Zielgruppenansprache der analysierten Werbeanzeigen werden bewusst Personen adressiert, die in ihren **spezifischen Lebenssituationen** anfälliger für Betrug sind. Dabei muss davon ausgegangen werden, dass nicht vordergründig demografische Kennzahlen Vulnerabilität kennzeichnen, sondern vielmehr spezifische Lebenssituationen (Europäische Kommission et al., 2016), wie zum Beispiel finanzielle Belastungen oder akute Stresserfahrungen sowie die damit

einhergehenden situationsgebundenen körperlichen oder emotionalen Zustände wie Angst, Gier oder Verzweiflung.

Greifbar wird dies zum Beispiel im Bereich Kreditbetrug durch das gezielte Ansprechen von Personen, die sich in **finanziellen Notlagen** befinden und auf anderen Wegen kaum Zugang zu Krediten hätten („trotz Schufa“ oder „Kredit ohne Einkommensnachweise“). Im Bereich Jobbetrug werden **Arbeitssuchende** mit geringer formaler Qualifikation oder brüchigen Erwerbsbiografien angesprochen, die auf niederschwellige Berufseinstiege hoffen („keine Erfahrung notwendig“). Auch beim Bewerben von unseriösen Nahrungsergänzungsmitteln wird gekonnt auf Vulnerabilitäten gesetzt – etwa indem **Personen mit chronischen Krankheiten** angesprochen werden und ihre Hoffnung auf die beworbenen Wundermittel ausgenutzt wird.

4.3.5. Genutzte Infrastrukturen

Eine Analyse ausgewählter Weiterleitungsziele (Landing Pages), die über die Werbeanzeigen erreichbar sind, zeigt, dass hinter dem Betrugsökosystem eine **professionalisierte und teils geteilte technische Infrastruktur** steht. Ein wiederkehrendes Merkmal ist zum Beispiel der Einsatz von Cloudflare als sogenannter Reverse Proxy: Dabei wird der gesamte Datenverkehr einer Website über Cloudflare-Server geleitet, bevor der eigentliche Zielserver erreicht wird. Für Außenstehende ist dadurch nicht erkennbar, wo eine Website gehostet wird. Nahezu alle untersuchten Domains nutzen diesen Mechanismus und erschweren damit die Rückverfolgung. Ghost Stores wiederum nutzen vielfach Shopify als Plattformbasis.

Darüber hinaus setzen die Websites in großem Umfang auf **etablierte Tracking- und Analysedienste** (vor allem von Facebook, aber auch Google Tag Manager, TikTok Pixel und Klaviyo). Diese Dienste ermöglichen es, das Verhalten von Nutzer:innen auf einer Website detailliert zu verfolgen – und analysieren zu können, welche Seiten aufgerufen werden, wo geklickt wird und wer tatsächlich kauft. Die dabei gesammelten Daten fließen zurück in die Werbeplattformen und erlauben eine präzise Aussteuerung der Anzeigen – ein Mechanismus, den auch legitime Werbetreibende nutzen, der im Kontext betrügerischer Anzeigen jedoch das gezielte Erreichen vulnerabler Zielgruppen begünstigt.

Darüber hinaus lassen sich auf Basis einer Ähnlichkeitsanalyse des HTML-Quellcodes mehrere **Cluster von Websites** identifizieren, die mutmaßlich von denselben Akteur:innen betrieben werden. Websites für dubiose Nahrungsergänzungsmittel setzen einheitlich auf den Dienst Funnelish – ein auf Conversion-Optimierung spezialisiertes Tool, das ähnlich wie Shopify funktioniert. Gleichzeitig nutzen diese Websites identische Bilder, die auf Funnelish gehostet

werden und zumindest teilweise mittels generativer KI erstellt wurden. Auch der Quellcode dieser Landing Pages ähnelt sich stark. Die HTML-Quellen der ausgewählten Landing Pages der Fake-Shops sind wiederum fast identisch, enthalten Code-Kommentare auf Chinesisch und beziehen ihre Bilder von einem auf Chinesisch konfigurierten Webserver, der bei Alibaba registriert ist. Trotz Cloudflare-Verschleierung weisen sie eine mutmaßlich gemeinsame Serveradresse auf, der auf einen in China ansässigen Akteur hindeutet. Auch im Bereich der problematischer Nahrungsergänzungsmittel zeigen sich geteilte Merkmale: Mehrere Domains teilen denselben E-Mail-Server, der bei Hetzner in Deutschland gehostet wird und mutmaßlich auch als Webserver für die eigentlichen Landing Pages dient. Eine Suche nach diesem Server förderte **mehr als 300 weitere vergleichbare betrügerische Websites** zutage – ein Hinweis auf ein deutlich größeres, koordiniertes Netzwerk.

4.4. Abo-Fallen

Für das Betrugsschema Abo-Fallen lassen sich betrügerische Werbeanzeigen in verschiedensten Themenbereichen finden: von Intelligenztests, Selbsttests für neurodivergente Ausprägungen (z. B. ADHS) bis hin zu Produktivitätsanalysen oder Hundetrainingsprogrammen. Während sich die konkreten Inhalte je nach Zielgruppe und beworbenem Abonnement unterscheiden, zeigen sich übergreifende Gemeinsamkeiten in der visuellen Gestaltung, der Ansprache sowie in den zugrunde liegenden strategischen Mustern.

Ansprache von Selbstzweifel und Optimierungsbedürfnissen

Eine häufig verwendete Strategie liegt in der gezielten Ansprache von alltagsnahen Unsicherheiten und des **gesellschaftlich verbreiteten Selbstoptimierungsdrucks.** Die Werbeanzeigen greifen Themen auf, mit denen sich viele Nutzer:innen identifizieren können, wie etwa Konzentrationsschwierigkeiten, Prokrastination, vermutete ADHS-Ausprägungen oder die Frage nach der eigenen Intelligenz. Einerseits finden sich Aussagen wie „Dein IQ ist vermutlich niedriger als du denkst." oder „ADHS ist Not Laziness", die bestehende Selbstzweifel verstärken oder alltägliche Schwierigkeiten problematisieren. Andererseits wird mit aufwertenden Formulierungen gearbeitet, etwa „Nur sehr intelligente Menschen lösen diese Fragen" oder „Du bist klüger als du denkst". Diese Kombination nutzt den **Curiosity-Gap** (siehe Narrative, Zielgruppenansprache & genutzte Infrastrukturen): Die Verunsicherung spricht eine selbstbezogene Wissenslücke an und erzeugt ein Bedürfnis diese zu schließen, während das Schmeicheln als Anreiz wirkt, diesem Bedürfnis durch einen Klick nachzugeben. Adressiert werden damit insbesondere Personen, die

bereits Unsicherheiten in Bezug auf ihre kognitiven Fähigkeiten, ihre Produktivität oder ihre mentale Gesundheit empfinden.

Alltagsprobleme werden dabei entweder pathologisiert oder als unentdecktes Potenzial gerahmt. Konzentrationsschwierigkeiten erscheinen als mögliches Anzeichen für ADHS und durchschnittliche Testergebnisse als Hinweise auf unterschätze Hochbegabung. Begleitet werden diese Narrative häufig durch pseudowissenschaftlich anmutende Erklärungen zu ADHS, Neurodivergenz, Produktivität oder Gehirnleistung. Begriffe wie „Studien zeigen“, „wissenschaftlich bewiesen“ oder „PhD-level questions“ werden eingesetzt, um die Seriosität und Wissenschaftlichkeit der Anzeigen weiter zu untermalen.

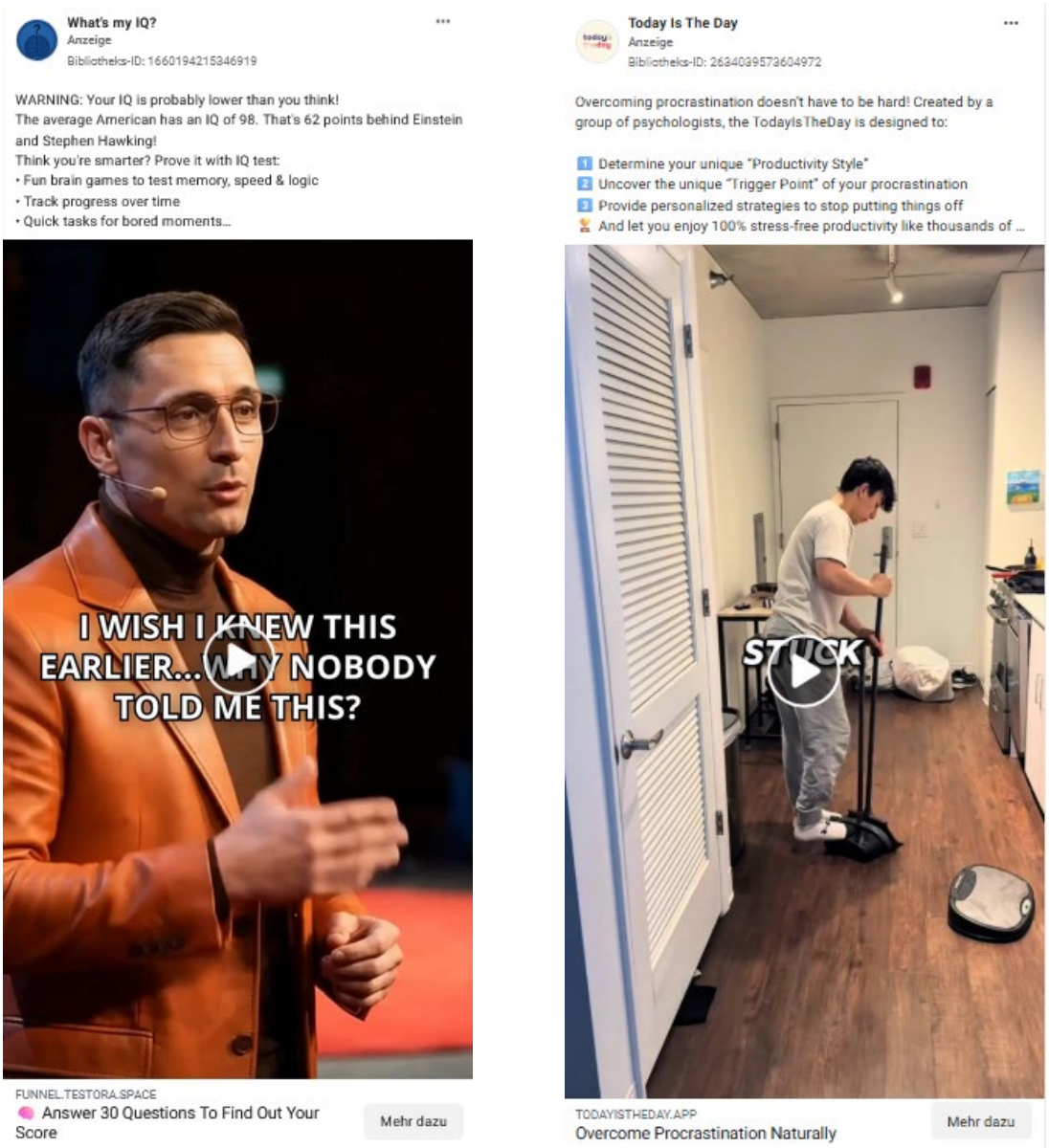

Abbildung 1: Betrügerische Werbeanzeige zu IQ Test und ADHS-Test

Visuell werden diese Botschaften zusätzlich mit vermeintlichen Expert:innen-Videos ergänzt, die teilweise KI-generiert sind. In diesen Videos erklären Personen in einem sachlichen, ruhigen Tonfall, warum die eigene Selbsteinschätzung vermutlich unzutreffend sei und weshalb ein kurzer Test innerhalb weniger Minuten verlässliche Erkenntnisse liefern könnte. Ergänzt werden diese Darstellungen durch Grafiken von IQ-Skalen oder plakativen Gehirndarstellungen.

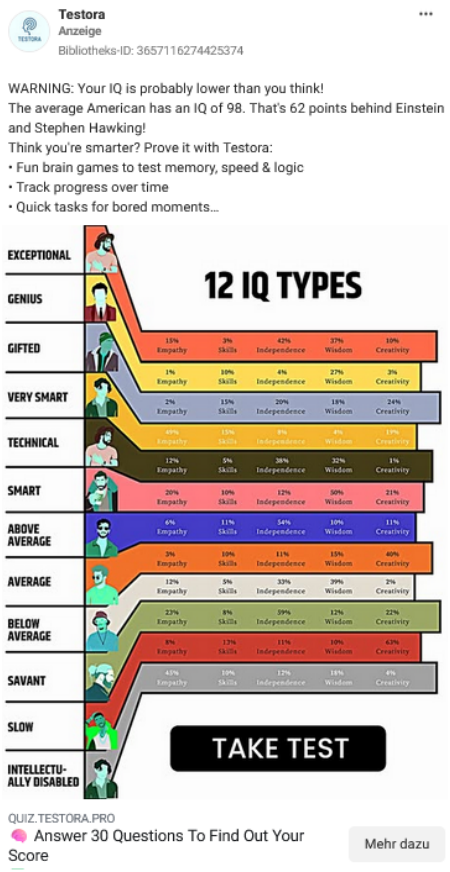

Abbildung 2: Betrügerische Werbeanzeige mit IQ-Skala

Niederschwellige Interaktion

Eine weitere identifizierte Strategie ist das Werben von möglichst niederschwelligen Interaktionen. Der Einstieg in das Angebot wird bewusst **einfach und unverbindlich** beschrieben. Formulierungen wie „1-Minute-Test", „Nur 30 Fragen" oder „Jetzt sofort starten" vermitteln den Eindruck eines schnellen, simplen Erkenntnisgewinns ohne größeren Aufwand. Die Hemmschwelle zur Teilnahme wird dadurch erheblich reduziert.

Weiterer Verlauf: Click-Through-Tests & vermeintliche Individualisierung

Ein Klick auf den Anzeigenlink führt zu visuell und strukturell ähnlichen „Click-Through"-Tests, bei denen Nutzer:innen schrittweise Fragen beantworten. Fortschrittsbalken und personalisierte Ansprache verstärken den Eindruck eines **individuellen Diagnoseprozesses.** Nutzer:innen beantworten Fragen zu Konzentration, Denkverhalten, Alltagsituationen oder zu spezifischen Verhaltensmustern ihres Tieres. Fortschrittanzeigen, personalisierte Anredeformen und Zwischenauswertungen verstärken den Eindruck eines personalisierten Diagnose- oder Analyseprozesses.

Am Ende wird die Möglichkeit angeboten, eine detaillierte Auswertung der Testergebnisse oder einen personalisierten Trainings-/Übungsplan per E-Mail zu erhalten. Erst an dieser Stelle tritt – häufig weniger prominent – die kostenpflichtige Abonnementstruktur in Erscheinung.

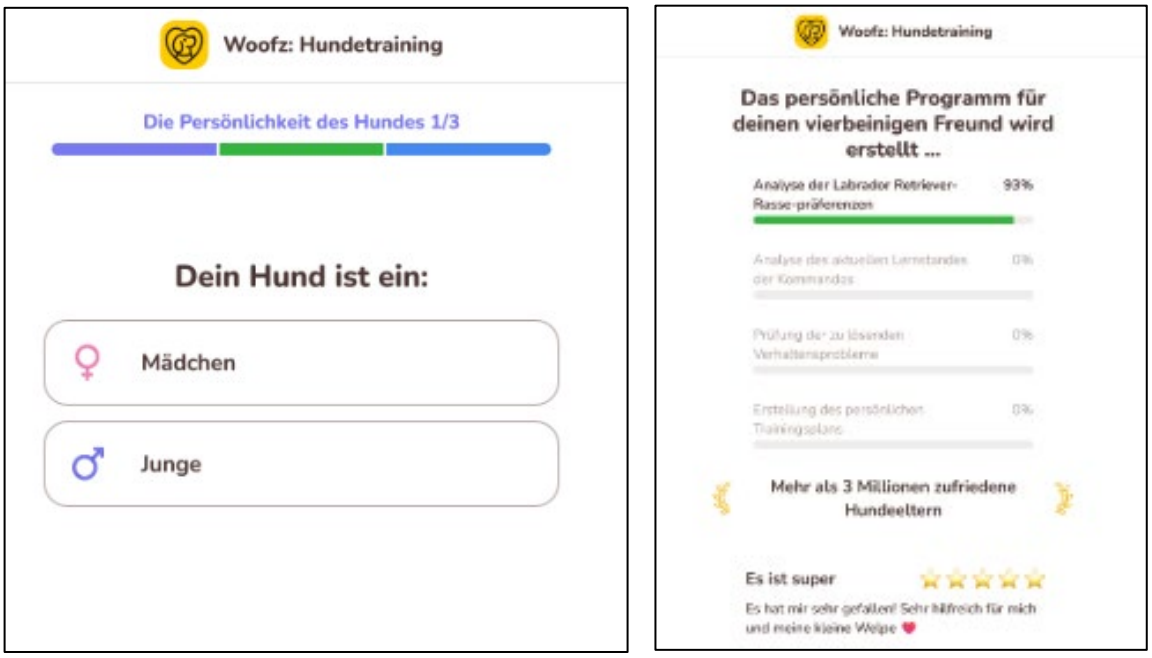

Abbildung 3: Landing Page Woofz Academy

Die Benutzeroberflächen der Landing Pages sind zudem oft so gestaltet, dass sie Nutzerinnen dazu verleiten, viel und schnell mit ihnen zu interagieren. Großflächige „Call-to-Action-Buttons", reduzierte Textmenge, emotionale Bestärkungen („Du bist fast am Ziel!") sowie Countdown-Elemente oder zeitlich begrenzte Angebote lassen sich klar den Methoden des Deceptive Designs zuordnen und erhöhen somit manipulativ den Interaktionsreiz. Vertragsdetails, Laufzeiten oder Hinweise auf automatische Verlängerungen sind zwar formal vorhanden, jedoch häufig erst in weiterführenden Links oder umfangreichen Nutzungsbedingungen ersichtlich.

4.5. Investmentbetrug

Unter den analysierten Werbeanzeigen im Bereich Investmentbetrug lassen sich mehrere übergeordnete Strategien erkennen, die trotz thematischer Variationen, wie z. B. KI-gestütztes Trading oder Insider-Trading Communities, strukturell ähnlich aufgebaut sind.

Technologische Innovation als Renditeversprechen

Eine zentrale Strategie liegt in der Instrumentalisierung **aktueller Technologie-Entwicklungen,** insbesondere Künstlicher Intelligenz, um einen vermeintlichen Wettbewerbsvorteil zu suggerieren. Anzeigen nutzen systematisch Buzzwords wie „AI-Trading", „ChatGPT Aktien" oder „KI-Strategie". Formulierungen wie „Künstliche Intelligenz analysiert täglich den Aktienmarkt, um hochwertige

Aktien für Sie zu finden“ oder „Wie ich mache 1000€ jeden Tag mit ChatGPT ohne Erfahrung“ suggerieren, dass komplexe Finanzmarktanalysen durch KI für Laien zugänglich gemacht werden.

Besonders perfide ist dabei die Verwendung von konkreten Treffsicherheitsquoten – etwa „KI-Treffsicherheit bis zu 98%“, die eine vermeintliche empirische Validierung der Methode vortäuschen. Diese Zahlen dienen nicht nur der Vertrauensbildung, sondern kommunizieren auch Pseudowissenschaftlichkeit. Die „Modernisierung“ des Finanzmarktzugangs wird dabei als technologischer Fortschritt dargestellt, der rationale Investmentbarrieren überwindet.

Abbildung 4: Betrügerische Werbeanzeigen mit Verweis auf ChatGPT

Exklusivität durch Community Modell

Eine zweite Strategie liegt in der **Konstruktion exklusiver Gemeinschaften** und der Verlagerung der Kommunikation auf **Messenger-Plattformen.** Dominierten vor noch etwa einem Jahr Werbeanzeigen, die im nächsten Schritt zu Fake-News-Seiten und von dort weiter zu den betrügerischen Plattformen führten, leiten die Anzeigen mittlerweile zu einem Großteil zu Messenger-Plattformen weiter: 87% aller von uns erhobenen und noch nicht entfernten Anzeigen leiteten nicht auf eine Landing Page, sondern auf „fb.me“ – also den Facebook-Messenger. Auszugehen ist davon, dass von dort wiederum in – wie in den Anzeigen beworben – WhatsApp Chat-Gruppen weitergeleitet wird.

Diese Verlagerung auf private Chat-Gruppen erschwert die Nachvollziehbarkeit für Behörden und Forscher:innen, nutzt gleichzeitig die vermeintliche Privatsphäre von Messenger-Diensten zur Vertrauensbildung und gibt den Nutzer:innen das Gefühl Teil einer exklusiven Community zu sein. Formulierungen wie „Exklusive Gewinnchancen – jetzt profitieren“, „Pre-market-Handelsstrategie“ oder „Aktienanalyse-VIP-Gruppe beitreten“ schaffen ein künstliches Gefühl von Privilegierung und suggerieren, dass „normale Anleger:innen“ keinen Zugang zu diesen Informationen haben.

Auffällig ist zudem eine strategische Verschiebung in der Zielgruppenansprache: So wurde noch vor einigen Monaten häufig die Telefonnummer auf Fake-News-Seiten oder direkt auf Investmentseiten

abgefragt und die Betroffenen telefonisch von einer „persönlichen Betreuerin“ oder einem „persönlichen Betreuer“ kontaktiert. Mit der Verlagerung in Chat-Gruppen wird stärker auf niederschwellige Interaktion, kontinuierliche Informationszufuhr sowie gruppendynamische Effekte gesetzt.

Deceptive Design Elemente

Besonders wirksam ist dabei die Kombination aus künstlicher Verknappung und Gratis-Angebot. Aussagen wie „nur für die ersten 1000 Anmeldenden“, „nur 100 Plätze verfügbar“ oder „limitierte Teilnahme“ erzeugen Dringlichkeit und Exklusivitätsdruck, während gleichzeitig betont wird „Wir nehmen kein Geld – du bekommst die besten Tipps völlig kostenlos“.

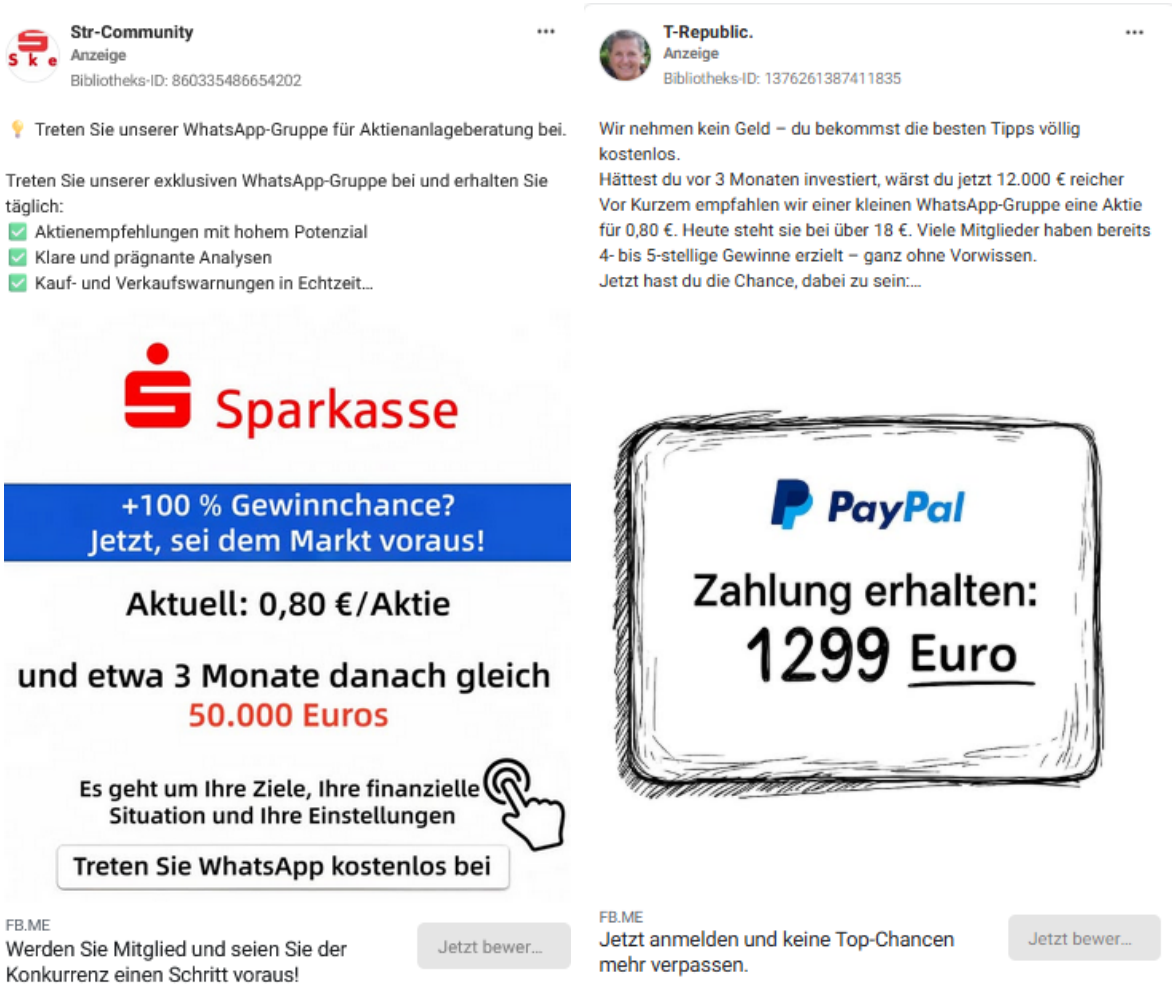

Abbildung 5: Betrügerische Werbeanzeigen mit Community Modell

Das Community-Modell arbeitet zudem mit dem **Prinzip der sozialen Bewährtheit**: Wenn angeblich zahlreiche „Mitglieder bereits dabei" sind, entsteht der Eindruck einer etablierten und legitimen Investorengemeinschaft.

Autoritäts- und Vertrauenskonstruktion u.a. durch Einsatz von Deepfakes

Die dritte Strategie basiert auf dem systematischen Missbrauch prominenter Namen und der Konstruktion vermeintlicher Expert:innen-Identitäten. Besonders häufig werden dabei Autoritäten aus der Finanzwelt missbraucht wie der ehemalige österreichischen Finanzminister Hans Jörg Schelling, dem Finfluencer Philip Hopf (bzw. dem stark kritisierten Podcast-Duo Hoss & Hopf) oder der „Investmentpunk" Gerald Hörhan.

Abbildung 6: Der Name des Finfluencers Philip Hopf wird für eine betrügerische Werbeanzeige missbraucht.

Technologisch unterstützt wird diese Strategie durch den **Einsatz von Deepfake-Videos**. Diese Videos zeigen scheinbar authentische Aufnahmen der Personen, die für betrügerische Investments werben oder zur Teilnahme an WhatsApp-Gruppen aufrufen. In einem Video tritt etwa Philip Hopf auf und kündigt einen exklusiven „Insider-Tipp" für eine wachstumsstarke Aktie an, verbunden mit der Aussicht auf schnelle und sichere Gewinne.

Auch hier ist eine Verschiebung in der Auswahl der missbrauchten Prominenz zu beobachten: Während noch vor etwa einem Jahr verstärkt ORF oder Puls4 Moderator:innen (z. B. Armin Assinger, Nadja Bernhard, Armin Wolf, Barbara Fleißner) verwendet wurden, liegt der Fokus inzwischen stärker auf Personen mit expliziter Finanzexpertise oder politischer Autorität. Statt auf breite Bekanntheit zu setzen, wird zunehmend **fachliche Glaubwürdigkeit** inszeniert**.** Zugleich spricht die Auswahl der Prominenten teilweise eine tendenziell jüngere Zielgruppe an.

Die Renditeversprechen sind dabei systematisch unrealistisch: Aussagen wie „0,80 € pro Aktie und etwa 3 Monate danach 50.000€" oder „+100% Gewinnchance?" versprechen außergewöhnlich hohe und zugleich risikofreie Gewinne. Ergänzt werden diese Versprechen durch Dringlichkeitsnarrative

– „nur noch wenige Plätze“, „sei dem Markt voraus“, typische Deceptive Design-Mechanismen der künstlichen Verknappung.

4.6. Kreditbetrug

Kern der Strategie im Bereich Kreditbetrug ist die gezielte Ansprache finanziell vulnerabler Personen durch eine Kombination aus (1) garantierter Kreditzugänglichkeit, (2) radikaler Vereinfachung des Kreditprozesses und (3) künstlich erzeugter Dringlichkeit. Das somit entstehende Narrativ suggeriert Hoffnung, Entlastung und unmittelbare Problemlösung und ist eine besondere Gefahr für Personen in finanziell vulnerablen Situationen.

Abbildung 7: Betrügerische Werbeanzeigen Kreditbetrug (links: Kredit trotz schlechter Bonität, rechts: vereinfachte Darstellung des Kreditprozesses)

Ausnutzung finanzieller Vulnerabilität durch Niederschwelligkeit und Dringlichkeit

Die Zielgruppe dieser Werbeanzeigen umfasst insbesondere **Personen in finanziell prekären Situationen,** die aufgrund ihrer Lebenssituation vom regulären Kreditmarkt ausgeschlossen sind oder sich so wahrnehmen. Der Zielgruppe wird dabei suggeriert, dass sie trotz Ausschlusskriterien

in Kreditvergabeprozessen in der Lage sind einen Kredit zu beantragen. Die klassische Selektionslogik seriöser Kreditvergabe – Bonitätsprüfung, Einkommensnachweise, Risikobewertungen – wird rhetorisch bewusst umgedreht: Inklusion statt Ausschluss. Formulierungen wie „Kredit trotz Schufa", „Kredite ohne Einkommensnachweise" oder „ohne Bonitätsprüfung" kommunizieren dieses Gegennarrativ zum formalen Bankensystem und sprechen aktiv das Bedürfnis nach einer „zweiten Chance" an.

Ein weiteres zentrales Element ist die Vereinfachung des Antragsprozesses. Aussagen wie „Nur wenige Klicks" oder „keine Dokumente nötig" stellen eine in der Regel komplexe, langwierige finanzielle Entscheidung als scheinbar **beiläufige, unkomplizierte digitale Interaktion** dar. Die Tragweite eines Kreditvertrags, von Zinsen und Laufzeiten über Vertragsbedingungen, bleibt in den Darstellungen verschleiert und unspezifisch. Stattdessen wird der Fokus auf Geschwindigkeit, Niedrigschwelligkeit und minimale Dateneingabe gelegt.

Deceptive Design Elemente

Visuell bedient sich die Anzeige verschiedener manipulativer Elemente: Formulierungen wie „nur noch heute", „nur noch wenige Plätze" oder „das Angebot endet bald" vermitteln ein Bild der Dringlichkeit, welches Nutzer:innen dazu verleiten soll schnelle Entscheidungen zu treffen. Insbesondere bei Personen in finanziellen Notlagen kann diese **inszenierte Verknappung** bestehende Stresssituationen verstärken und die Bereitschaft erhöhen außerhalb seriöser Institutionen und die damit einhergehenden Prüfungsmodalität zu handeln.

Weiterer Verlauf: Click-Through-Tests

Folgt man dem Ad Link, gelangt man häufig zu „Click-Through-Tests", die ähnliche Strategien verfolgen wie im Abschnitt Abo-Fallen dargestellt – personalisierte Kreditangebote, „Call-to-Action-Buttons" sowie emotionale Bestärkung.

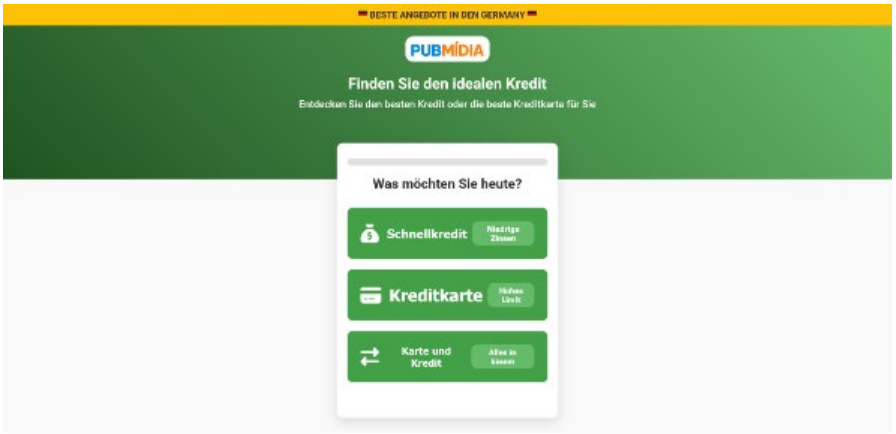

Abbildung 8: Unseriöse Kreditbetrug Website

4.7. Jobbetrug

Betrügerische Werbeanzeigen im Bereich Jobbetrug bedienen ein breites thematisches Feld und variieren ihre narrative Ausgestaltung teilweise saisonal oder ereignisbezogen. Zwei übergeordnete strategische Methoden lassen sich dabei durchgängig identifizieren: die Vermittlung niederschwelliger Erwerbsversprechen einerseits sowie die Vortäuschung von Legitimität und Plausibilität andererseits.

Abbildung 9: Betrügerische Werbeanzeigen für vermeintliche Jobanzeigen

Niederschwelliges Erwerbsversprechen

Im Zentrum vieler Anzeigen steht die Darstellung eines **mühelosen Berufseinstiegs**, der nahezu unabhängig von Qualifikation, Erfahrung oder formalen Anforderungen möglich sei. Formulierungen wie „keine Erfahrung erforderlich" oder „Keine Erfahrung? Kein Problem!" suggerieren, dass sich jede Person bewerben und sofort starten kann.

Diese niederschwellige Einladung wird durch weitere Elemente verstärkt: Tätigkeiten werden als „kleine Aufgaben“ beschrieben, Teamzusammenhalt und Unterstützung betont und kostenlose Schulungen in Aussicht gestellt.

Gleichzeitig wird der Bewerbungsprozess stark entformalisiert. Aussagen wie „Starten Sie noch heute“, „Unser professionelles Team meldet sich innerhalb von 24 Stunden“ oder „Sofort beantragen“ verkürzen den üblichen Bewerbungsprozess auf eine unmittelbare Handlung.

Häufig wird zu einer Kontaktaufnahme über Messenger-Dienste aufgerufen, wodurch die institutionelle Distanz weiter abgebaut wird. Dies bestätigt sich auch in den Daten, da 58% aller noch nicht entfernten Anzeigen auf „fb.me“ leiteten – also den Facebook-Messenger. Der komplexe und mehrstufige Auswahlprozess regulärer Beschäftigungsverhältnisse wird so als eine spontane, nahezu beiläufige Interaktion dargestellt.

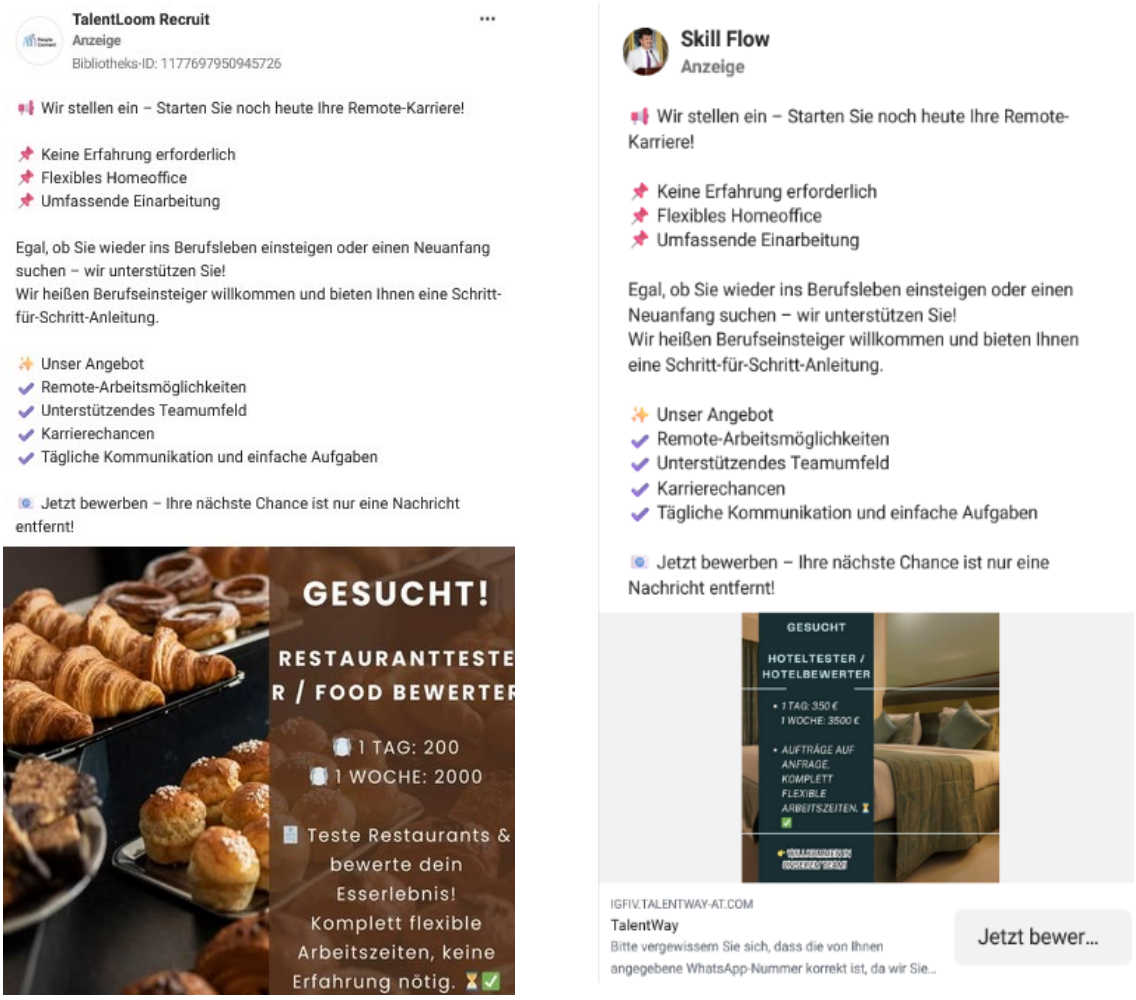

Abbildung 10: Betrügerische Werbeanzeigen zu angeblichen Traumberufen

Ein weiteres zentrales Element dieser Strategie sind unrealistische oder zumindest stark überhöhte Vergütungsversprechen. Aussagen wie „200 € pro Tag", „150-300 € pro Video" oder „bezahlt deine Miete bei 1-2 Stunden Arbeit täglich" erzeugen ein deutliches **Missverhältnis zwischen Leistung und Einkommen.** Die Tätigkeit selbst bleibt dabei oft vage oder unspezifisch, während finanzielle Belohnung klar und prominent kommuniziert wird. In Kombination mit „Traumberufen", wie etwa Hotel- oder Restaurant-Tester:innen, entsteht ein trügerisch-verlockendes Arbeitsbild, das Status, Flexibilität und finanzielle Sicherheit miteinander verbindet.

Vortäuschung von Legitimität und Plausibilität

Im Bereich Jobbetrug wird einerseits ein niedrigschwelliges, hochattraktives Erwerbsversprechen konstruiert, das zentrale Hürden des Arbeitsmarktes aufhebt und unrealistische Einkommensperspektiven eröffnet. Andererseits wird durch die Übernahme realer Stellenanzeigen, die Nutzung bekannter Markennamen sowie durch lokal- und ereignisbezogene Kontexte Legitimität simuliert. Parallel zur Konstruktion eines attraktiven Erwerbsangebots wird gezielt an der Reduktion potenzieller Skepsis gearbeitet. Dies geschieht durch die Vortäuschung von Seriosität sowie der Konstruktion vermeintlicher Legitimität – etwa durch die Übernahme realer oder realitätsnaher Stellenanzeigen bekannter Unternehmen. In einzelnen Fällen werden Jobinserate sogar im identischen Wortlaut kopiert und über Werbeanzeigen mit einem abweichenden, unseriösen Link erneut ausgespielt. So wurde etwa die Stellenausschreibung einer Tiroler Werbeagentur vollständig übernommen und mit einer betrügerischen Weiterleitung versehen. Anstatt eigene Glaubwürdigkeit aufzubauen, wird bestehende Reputation übernommen.

Darüber hinaus wird häufig mit der **Nennung prominenter Marken** wie z. B. Lidl, dm oder Lego gearbeitet, ohne dass eine nachvollziehbare Verbindung zwischen der beworbenen Tätigkeit und dem Unternehmen hergestellt wird. Diese Praxis zielt auf eine Übertragung von Markenvertrauen und Wiedererkennungswert. Die bloße Präsenz eines bekannten Namens oder Logos kann ausreichen, um die wahrgenommene Legitimität der Anzeige zu erhöhen.

Ergänzend kommt eine starke lokale Bindung zum Einsatz – trotz Jobs, die hauptsächlich remote durchgeführt werden können. Anzeigen beziehen sich dabei explizit auf konkrete Städte wie Wien, Salzburg oder Linz oder knüpfen an saisonalen und ereignisbezogenen Kontexte an, wie etwa Weihnachtsjobs, große Sportveranstaltung (z. B. Fußball WM) oder kurzfristige Promotion-Tätigkeiten. Diese situative Einbettung erzeugt den Eindruck, es handle sich um eine reales, zeitlich und räumlich klar verortetes Beschäftigungsangebot

Abbildung 11: Betrügerische Jobanzeigen mit Ereignis- und Lokalbezug und Verweis auf bekannte Unternehmen

4.8. Unseriöse Nahrungsergänzungsmittelangebote

Bei Nahrungsergänzungsmittel (NEM) lassen sich betrügerische Werbeanzeigen für verschiedenste Gesundheitsbereiche sowie Krankheitsbilder beobachten: von Abnahme über Erektionsstörung hin zu Diabetes oder Blutzuckerprobleme. Während die Narrative sowie die Zielgruppe vom Produkt abhängig sind und sich unterscheiden, lassen sich übergreifende Ähnlichkeiten bei den Anzeigen und Strategien identifizieren – dazu zählt der Missbrauch von Handelsnamen, der Missbrauch medizinischer, medialer oder staatlicher Autorität sowie pseudowissenschaftliche Erzählungen.

Missbrauch von Handelsmarken und „Höhle der Löwen“

Eine Strategie ist das Vortäuschen der Zusammenarbeit mit **etablierten Handelsmarken wie** zum Beispiel dm oder Rewe, oder auch mit der **TV-Gründershow „Die Höhle der Löwen“** zu werben. Beispiele solcher Werbeanzeigen lassen sich vor allem im Bereich von Diäten und Abnehmen beobachten. Unter den Top fünf Keywords mit den meisten Anzeigen waren drei zum Thema Abnehmen, mit darunter „Die Höhle der Löwen“. Exemplarisch veranschaulicht Abbildung 14 diese Strategie. Bei den Anzeigen selbst wird dann oft das Logo von dm missbraucht, und ein Siegel mit der Aussage „60 Tage Geld-Zurück-Garantie“, um zusätzliche Legitimität vorzuspielen.

Visuell wird mit KI-generierten Bildern und unrealistischen Darstellungen, z. B. von Bauchfett gearbeitet, mittels „gelbe Kugeln“ werden zum Beispiel Vorher- und Nachher-Bilder dargestellt. Mit unmöglichen Versprechen wie „-14 kg in 3 Wochen“ oder „12 kg in nur 2 Wochen abnehmen!“ wird eine schnelle Abnehm-Wirkung des Produkts suggeriert.

Abbildung 12: Betrügerische Werbeanzeigen für Abnehmmittel

Pseudowissenschaftlichkeit

Eine weitere Strategie sind **pseudowissenschaftliche Narrative**, die Vertrauen und Expertise vermitteln sollen. Dabei werden teils einfache Studien fingiert, die es so nie gab: Aussagen wie „Klinisch getestet an über 27.000 Frauen und Männern (18 – 75 Jahre)“, oder das Wirkungen „zweifelsfrei bestätigt“ wären sind in den Anzeigetexten zu finden. Und in – oft KI-generierten Videos - werden scheinbar evidenzbasierte Behauptungen formuliert wie „Du denkst vielleicht, eine strenge Diät oder der komplette Alkoholverzicht sind der einzige Weg, deine Fettleber zu kontrollieren. Doch die Wissenschaft zeigt: Das ist ein fataler Irrtum.“ Flankiert werden diese Aussagen durch anatomische Darstellungen und Animationen, die an medizinische Dokumentationen erinnern (etwa eine Leber, die „krank“ wird, sich bräunlich verfärbt und „schrumpft“), sowie durch die Aufzählung unspezifischer Symptome wie „Müdigkeit“ oder „Blähungen“.

Gleichzeitig arbeiten die Clips mit **angstmachenden Narrativen** („fataler Irrtum“, „wirkt wie ein schleichendes Gift“, „zieht weitere gesundheitliche Probleme nach sich“). Zur Autoritätssteigerung werden zudem vage Verweise auf Expert:innen genutzt, etwa Formulierungen

wie „laut führenden Hepatologen“ – auch in diesem Fall werden pseudowissenschaftliche Behauptungen aufgestellt, ohne diese nachvollziehbar zu belegen.

Missbrauch medizinischer, medialer oder staatlicher Autorität

Eine noch stärkere Ausprägung dieser Strategie ist der Missbrauch existierender medizinischer, medialer oder staatlicher Autorität. Dabei werden bekannte Ärzt:innen und Gesundheitsexpert:innen durch KI-generierte oder manipulierte Videos missbraucht, um betrügerische NEM-Angebote zu bewerben. Teils werden diese Videos im Stil von Nachrichtenbeiträgen inszeniert, in denen bekannte Moderator:innen wie Armin Wolf oder Susanne Höggerl auftreten. Angstmachende **Anti-Establishment-Narrative** wie „die bösen Pharmakonzerne wollen euch krank halten“ oder „die Regierung verbot dieses Mittel“ werden dadurch ebenfalls verbreitet (Auer et al., 2025). Teilweise werden Werbeanzeigen auch von Accounts geschaltet, deren Namen ebenfalls medizinische Autorität vermitteln sollen - etwa „Dr. Katharina Wolff“ oder „Dr. Leon Schulte“. Die dazugehörigen Profilbilder sind KI-generiert und stellen Personen in weißem Kittel und Stethoskop dar.

Ein exemplarisches Beispiel zeigt zudem eine häufig vertretene Kombination aus Prominenten- bzw. Expert:innen-Inszenierung, Wirkversprechen und institutioneller Autoritätsbehauptung: So wird in einem Video behauptet, der deutsche Arzt und Kabarettist „Dr. Eckhart von Hirschhausen“ habe „eine natürliche Methode entdeckt, um die Erektion zu verstärken“ – „ganz ohne Risiken, Abhängigkeit oder Nebenwirkungen“. Als vermeintliche „Methode“ werden dabei alltagsnahe Hausmittel präsentiert, die den **Eindruck einer einfachen, sofort umsetzbaren Lösung** erzeugen. Zusätzlich wird ein angebliches „Förderprogramm der deutschen Regierung“ adressiert, das sich „an alle Männer über 45“ richtet und verhindern soll, „mit 60 oder 80 unter chronischer Impotenz“ zu leiden oder vom Konsum von „2–3 Viagra Tabletten“ abhängig zu sein. Risiken etablierter Medikamente werden dramatisiert (z. B. die Behauptung, Viagra könne das Schlaganfall- oder Herzinfarktrisiko „um 46% erhöhen“) und in Aussicht gestellt, die beworbene Lösung könne nicht nur körperliche Probleme, sondern auch die Beziehung mit dem Partner verbessern. Verwendet werden dabei auch **Verschwörungsnarrativen**, indem suggeriert wird, der „wahre Grund“ für Erektionsprobleme werde von „deutschen Pharmakonzernen und Ärzten verschwiegen“.

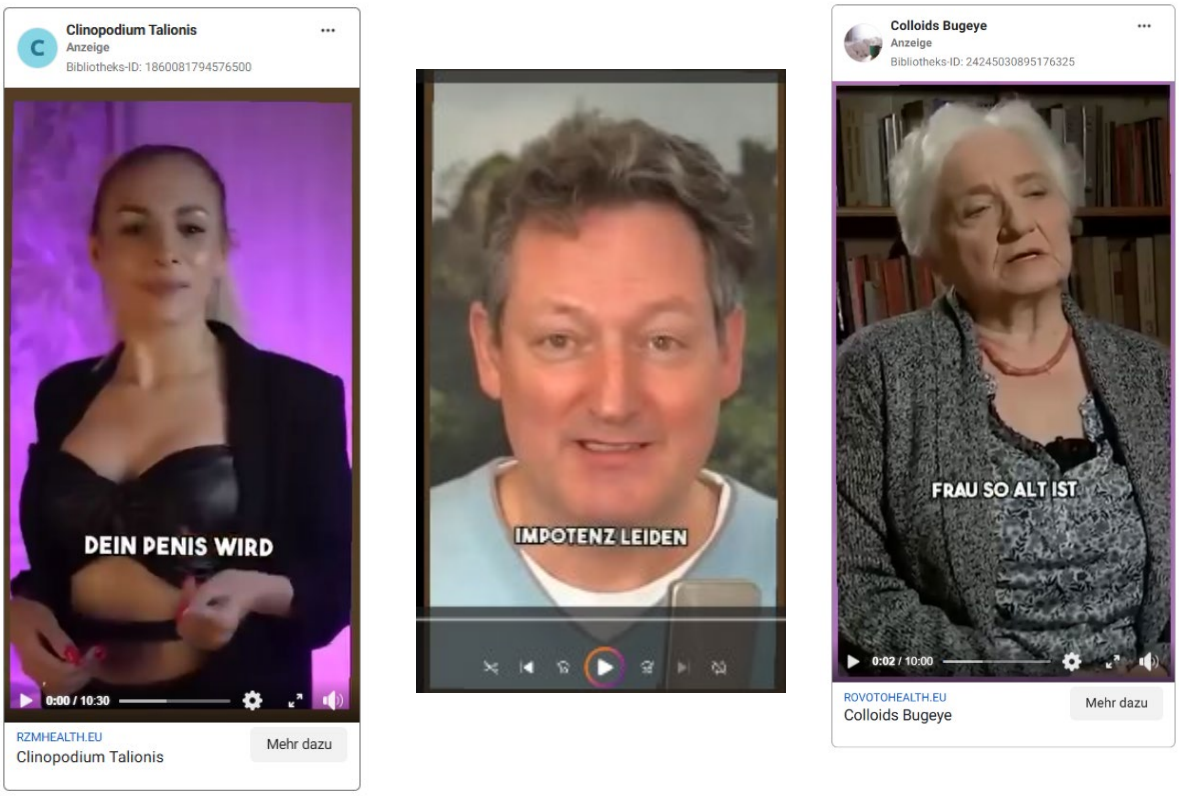

Abbildung 13: Betrügerische Werbeanzeigen zu Nahrungsergänzungsmittel mit angeblicher Impotenz-Heilung und weiterführendes Video mit KI-generiertem Abbild von Dr. Eckart von Hirschhausen (Mitte)

Adressierung chronischer Krankheiten

Eine besonders problematische Dimension dieser Werbeanzeigen ist die gezielte inhaltliche Ansprache von Personen mit chronischen Erkrankungen – darunter Diabetes, Bluthochdruck, Prostatabeschwerden, Erektionsstörungen oder Lebererkrankungen. Die Anzeigen knüpfen gezielt an die Hoffnungen und die Verzweiflung von Betroffenen an und präsentieren beworbene Produkte als vermeintliche Alternativmedizin. Eine Erhebung des ÖIAT zeigt, dass die Manipulation dabei so weit geht, dass Konsument:innen in nachgelagerten Beratungs- und Verkaufgesprächen empfohlen wurde, ihre tatsächlichen Medikamente – etwa bei Diabetes – abzusetzen und stattdessen auf die beworbenen Nahrungsergänzungsmittel zu vertrauen (Auer et al., 2025).

4.9. Ghost Stores

Die Werbeanzeigen für Ghost Stores folgen einem durchgängigen Muster: Die Werbetreibenden inszenieren sich als regional verankerte Familien- und Traditionsbetriebe in Österreich und Deutschland. Über emotionale Abschiedsnarrative werden große Rabatte auf angebliche Qualitätsware legitimiert.

Emotionale Abschiedsnarrative

Die zentrale Strategie der Werbeanzeigen für Ghost Stores ist es, große **Rabatte** mit **emotionalen Abschiedsnarrativen** zu kombinieren. Dabei werden häufig vermeintlich persönliche Geschichten und Beweggründe für die Schließungen des Geschäfts genannt – von Krankheits- und Todesfällen bis hin zu finanziellen Nöten oder aber fröhliche Nachrichten wie die Geburt von Enkelkindern. Beliebt ist auch das Narrativ, die „großen Konzerne hätten gewonnen", und die kleinen österreichischen Läden gäben jetzt nach Jahrzehnten „den Kampf" auf.

Mit Sätzen wie „Mit viel Emotion möchten wir eine wichtige Nachricht teilen. Nach vielen wundervollen Jahren voller Leidenschaft und Hingabe für unsere Boutique haben wir die Entscheidung getroffen, unser Geschäft zu schließen" (siehe Abbildung 16) wird gezielt emotionalisiert. Begleitet von Dankesaussagen an treue Kund:innen werben die Online-Shops mit großen Rabatten auf vermeintlich hochwertige Qualitätsware, die schnell aus dem Lager muss.

Regionalität

Verbunden werden diese Narrative mit der **Konstruktion lokaler Zugehörigkeit**: Dafür werden einerseits Geschäftsnamen mit expliziten Regionalbezug (z. B. „Muller Graz", „Moser Wien") gewählt, die einen lokalen Betrieb suggerieren. Andererseits werden auf der Landing Page, auf die die Werbeanzeigen führen, KI-generierte Bilder von vermeintlichen Geschäftslokalen platziert, die einen physischen Standort am vorgegebenen Unternehmenssitz vortäuschen. Diese Strategie nutzt gezielt das Vertrauen in Regionalität und kleinbetriebliche Strukturen.

Deceptive Design Elemente

Neben der Legitimierung, unglaubliche Rabatte aufgrund der bevorstehenden Geschäftsschließung anzubieten, gibt es auch die Strategie **zeitlich begrenzte Abverkäufe oder Sonder-Aktionen** anzubieten. Dies wird mit Aussagen wie „Nur heute 50% Rabatt" oder „Nur für kurze Zeit – Solange der Vorrat reicht" untermalt. Somit wird eine künstlich erzeugte Dringlichkeit hergestellt, um Käufer:innen zum schnellen Kauf zu animieren.

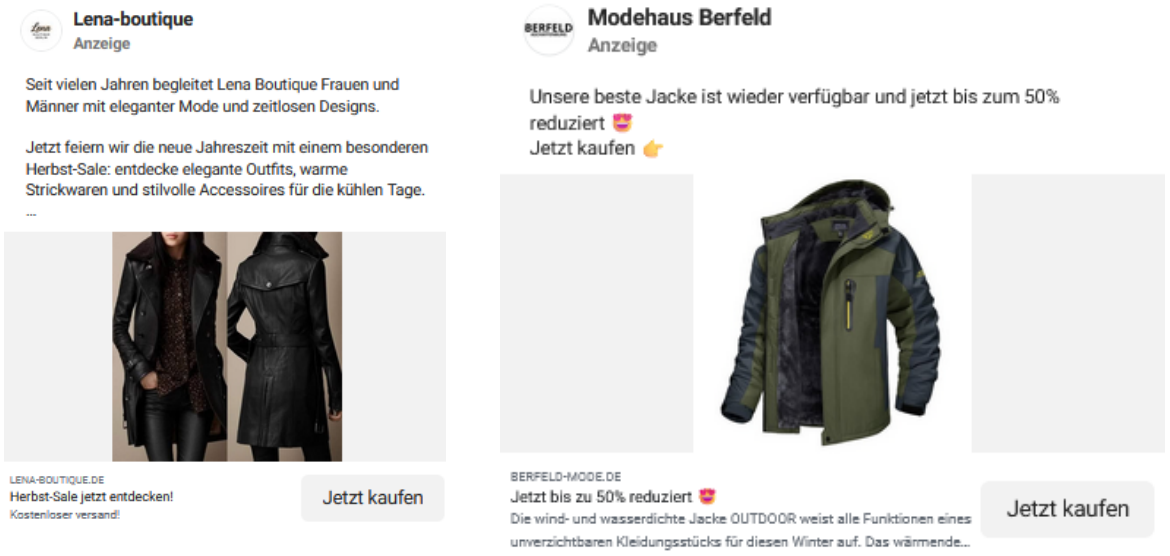

Abbildung 14: Betrügerische Werbeanzeigen zu Ghost Stores

4.10. Fake-Shops (Markenimitationen)

Das Betrugsschema der Fake-Shops und Markenimitationen kombiniert imitierte Markenidentitäten, unrealistische Preisversprechen und eine technisch verschleierte, aber strukturell einheitliche Infrastruktur. Für Konsument:innen ist die Täuschung dabei besonders schwer zu durchschauen, weil die eingesetzten Vertrauenssignale – bekannte Logos, seriöse Garantieversprechen und realistische Produktbilder – gezielt jene Schutzreflexe unterlaufen, die bei offensichtlich dubiosen Angeboten greifen würden.

Missbrauch etablierter Vertrauensanker

Diese Strategie besteht in der aktiven Imitation bekannter und in Österreich fest verankerter Marken**.** Dabei lassen sich zwei Varianten beobachten, die teils auch kombiniert auftreten: Einerseits werden **bekannte Handelsketten** wie Lidl oder Hofer imitiert, deren Logos direkt in die Produktbilder eingebettet werden. Andererseits werden Marken von insbesondere hochwertigen Herstellern, wie Birkenstock, Bosch, Swarovski, Garmin oder Philips, als Produktversprechen

eingesetzt. Teilweise wird dies verbunden, indem vermeintliche Zusammenarbeit oder Partnerschaft zwischen den Handelsketten und den Herstellern suggeriert wird.

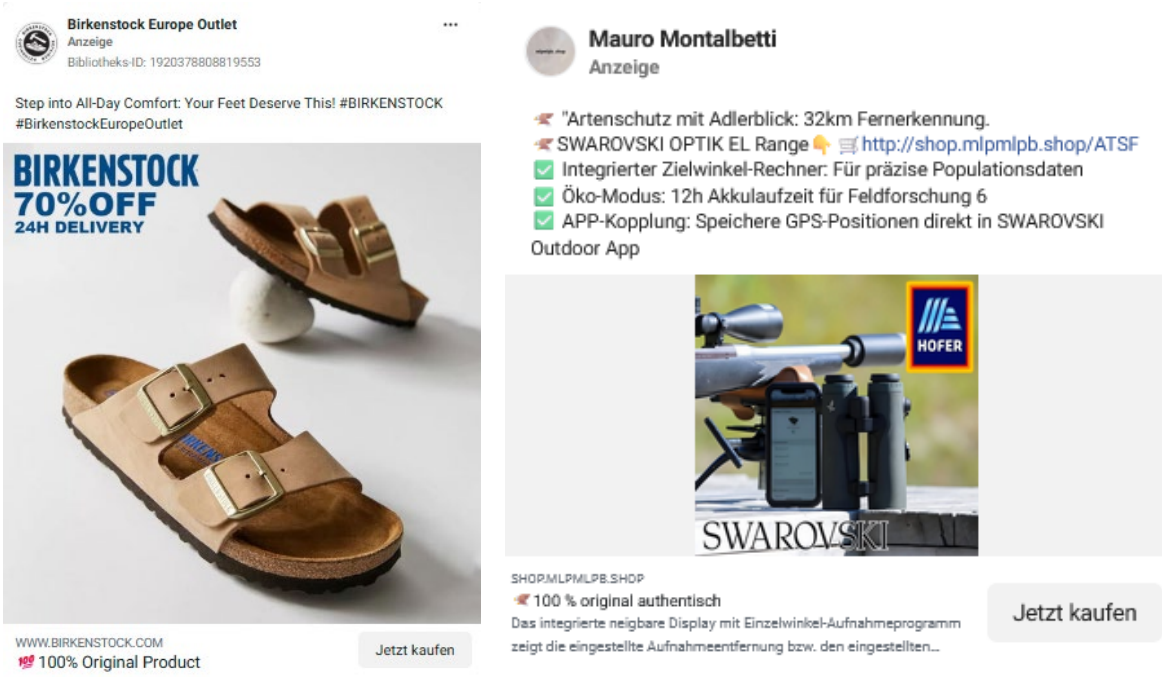

Abbildung 15: Betrügerische Werbeanzeigen für Fake-Shops (links: Birkenstock, rechts: Hofer und Swarovski)

Das tragende Narrativ dieser Strategie ist jenes der **Offiziosität und Authentizität**: Formulierungen wie „100% Original Product" oder „100% original authentisch" betonen dort die Echtheit, wo sie am stärksten angezweifelt werden könnten. Ergänzt wird dies durch ein Lokalitätsnarrativ, „HOFER – Eröffnung neuer Filialen in Österreich!", „Versand aus Österreich/Deutschland", das regionale Verwurzelung und Nähe suggeriert. Seriöse Händlerversprechen wie „5 Jahre Garantie", „100 Tage kostenlose Rückgabe" oder „Shipped within 48 hours" vervollständigen das Bild eines vertrauenswürdigen etablierten Anbieters. Bei den Links in den Werbeanzeigen werden teilweise die offiziellen Links angezeigt, zum Beispiel „www.birkenstock.com", allerdings wird dann zu einem Fake-Shop weitergeleitet mit einem leicht veränderten URL.

Rabatte als Köder

Die zweite zentrale Strategie ist die Werbung mit sehr **niedrigen Preisen für hochwertige Markenprodukte**. Bosch-Kühlschränke oder Waschmaschinen werden für 89,99€ angeboten, Swarovski-Ferngläser zum Bruchteil ihres Marktpreises, Birkenstock-Sandalen mit „70% OFF". Diese Preise liegen systematisch weit unterhalb jedes realistischen Marktniveaus und zielen auf eine gezielte Überrumpelung: Das Angebot ist offensichtlich zu gut, um wahr zu sein – wird aber durch

den vertrauten Markenkontext dennoch als plausibel wahrgenommen. Dies wird einerseits durch die genaue Produktbeschreibung erwirkt, sowie durch die Produktbilder, die oft das beworbene Produkt in einem physischen Laden zeigen.

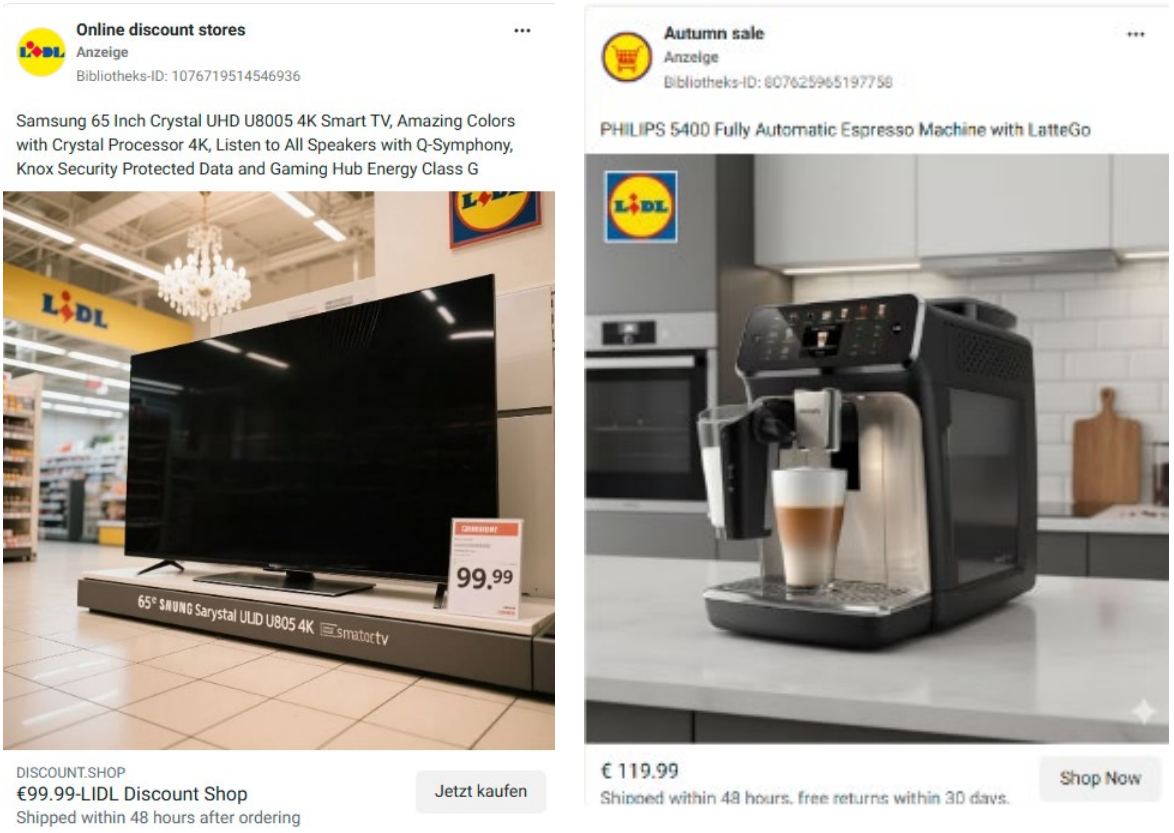

Abbildung 16: Betrügerische Werbeanzeigen zu Markenimitationen von der Handelskette Lidl

Formulierungen wie „Die niedrigsten Preise aller Zeiten! Auf keinen Fall verpassen!“ oder saisonale Anspielungen wie „Autumn sale“ und vorgetäuschte Filialeröffnungen erzeugen eine künstliche Dringlichkeit und suggerieren zusätzlich einen legitimen Ausverkaufskontext. Das Angebot wird als eine einmalige Gelegenheit dargestellt, die man nicht verpassen darf.

4.11. Online-Glücksspiele

Im Betrugsschema Online-Glücksspiele wird hauptsächlich mit Verweisen auf offizielle Casinos wie z. B. Casino Wien oder Casino Baden oder mit den Online-Glücksspielen „Chicken Road“ oder „Plinko“ geworben. Es lassen sich drei übergeordnete Strategien zur Bewerbung dieser Betrugsmasche anhand der erhobenen Werbeanzeigen beobachten. Alle verfolgen das Ziel, das Vertrauen der Nutzer:innen zu gewinnen und sie zu den jeweiligen betrügerischen Plattformen oder Apps zu locken.

Limitationsfiktion durch Nachahmung bekannter Casinos

Eines der auffälligsten Merkmale der analysierten Glücksspielanzeigen ist die gezielte **Imitation etablierter, lizenzierter lokaler (österreichischer) Casinos.** Die beworbenen Angebote, darunter „Casino Wien online“ und „Casino Baden ist jetzt offiziell online“, erwecken den Eindruck, es handle sich um die offizielle digitale Erweiterung von Casinos Austria. Tatsächlich handelt es sich jedoch um eigenständige, nicht lizenzierte Angebote, die auf unseriöse, ähnlich benannte Domains weiterleiten.

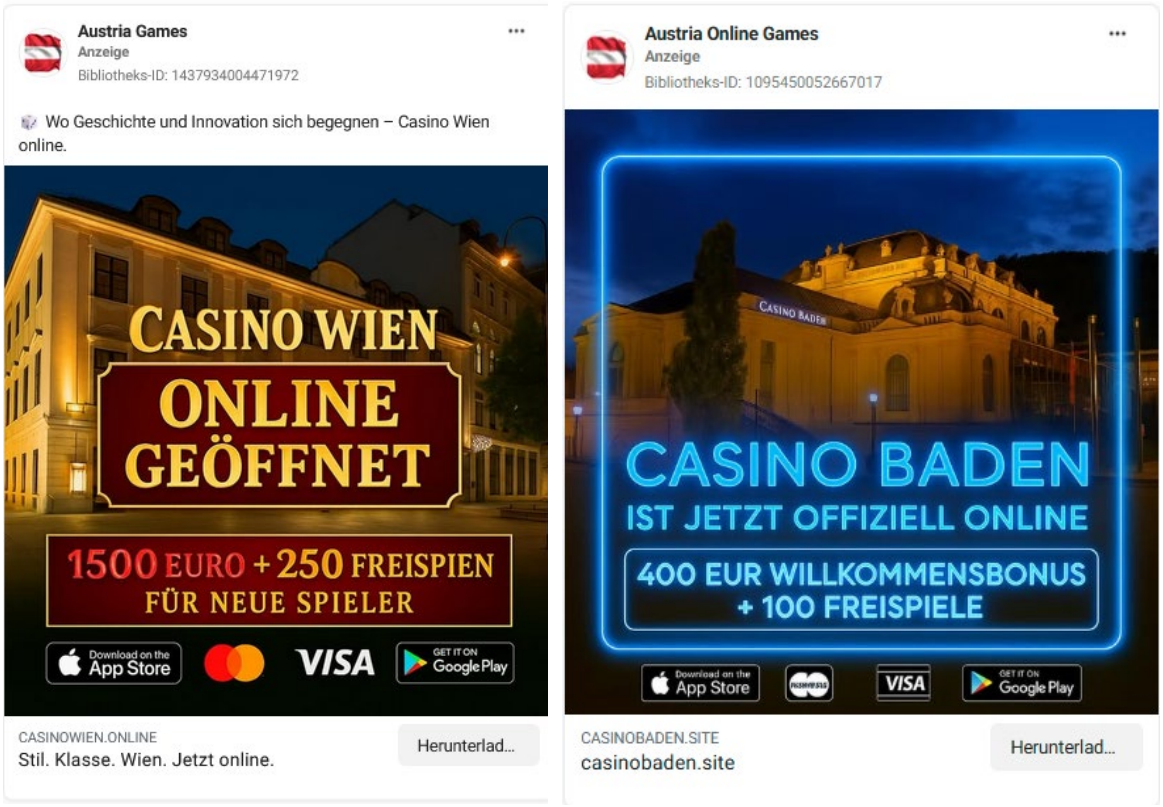

Abbildung 17: Betrügerische Online Casino Werbeanzeige

Diese Strategie bedient sich zweier zentraler Narrative: Erstens wird ein starkes **Prestige- und Lokalidentitätsnarrativ** aufgebaut. Formulierungen wie „Stil. Klasse. Wien.“ oder „Wo Geschichte und Innovation sich begegnen“ präsentieren das Glücksspiel als kulturell verortete, respektable Aktivität. Zweitens verstärken Aussagen dies durch ein **Convenience-Narrativ.** Das Online-Angebot wird als gleichwertige, aber komfortablere Alternative zum physischen Casino-Besuch dargestellt.

Auch auf visueller Ebene bedienen sich die Anzeigen gezielt etablierter Legitimationssignale: Echte Architekturfotos bekannter Casinogebäude werden mit digitalen Neon-Overlays versehen und vereinnahmen so die Authentizität realer Orte. Insgesamt entsteht so eine visuell kohärente

Oberfläche, die Seriosität und institutionelle Zugehörigkeit suggeriert, ohne diese tatsächlich zu besitzen. Die Einbindung offizieller Payment-Logos von Visa, Mastercard, App Store und Google Play in nahezu allen Anzeigen suggeriert Vertrauen und Seriosität durch bekannte Anbieter – unabhängig davon, ob eine echte Zahlungspartnerschaft besteht.

Anreizmanipulation durch Bonusversprechen

Eine zweite Strategie adressiert vor allem Neueinsteiger:innen. Eine Großzahl aller analysierten Anzeigen versprechen **großzügige Willkommensboni** wie etwa bis zu 1.500 Euro Bonusguthaben oder 250 Freispiele, die als explizites Angebot für „neue Spieler" ausgewiesen werden. Diese Praxis ist ein klassisches Akquise-Instrument. Der beworbene Bonus senkt die psychologische Einstiegshürde und erzeugt das Gefühl eines asymmetrisch guten Deals, bei dem der:die Nutzer:in scheinbar wenig riskiert und viel gewinnen kann. Pflichtangaben zu Risiken, Suchtgefahr oder Bonusbedingungen fehlen in den Anzeigen vollständig oder sind so gestaltet, dass sie kaum wahrgenommen werden.

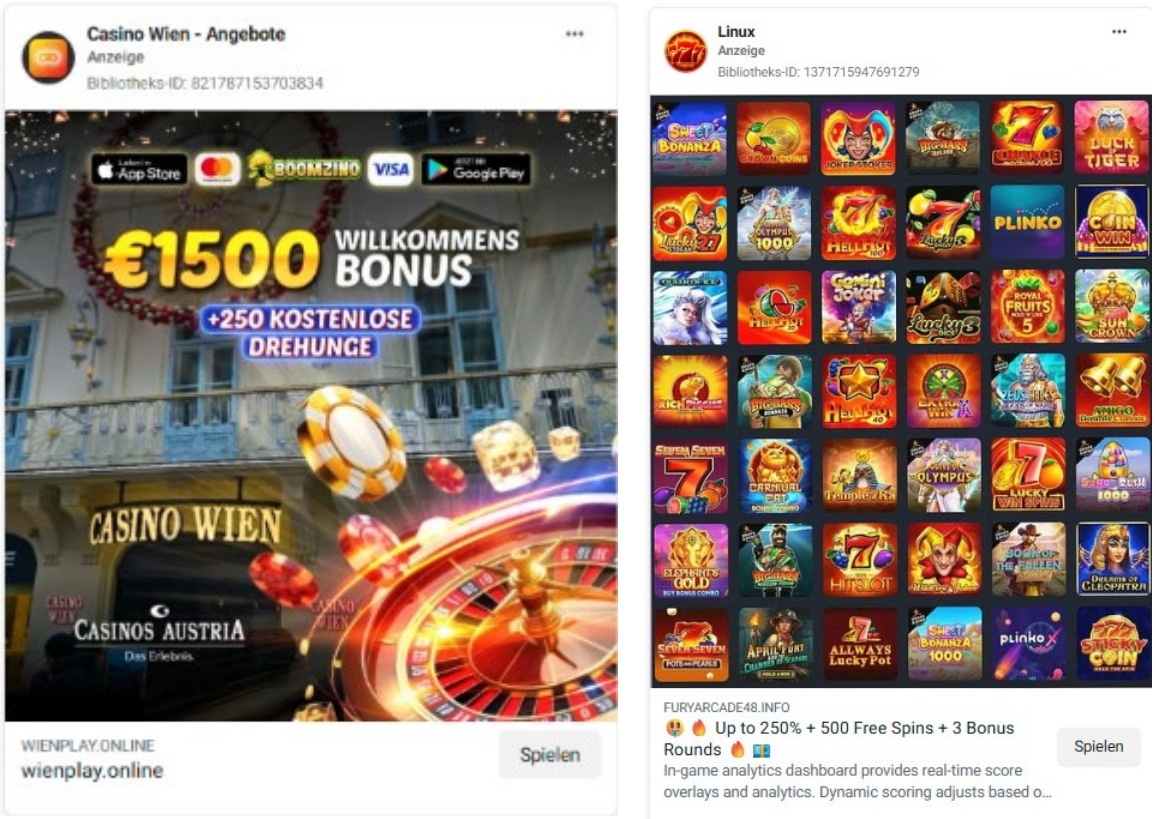

Abbildung 18: Willkommensbonus für Einsteiger:innen bei betrügerischen Online-Glücksspielen

Soziale Validierung und Deceptive Design

Eine dritte Strategie, die besonders bei den Anzeigen für Chicken Road und Plinko Gold zu beobachten ist, kombiniert den Einsatz sozialer Prominenz und von Deceptive Design Element. Ziel

ist es, Vertrauen durch Wiedererkennung und vermeintliche Authentizität herzustellen, sowie Nutzer:innen durch irrelevante, emotional ansprechende Inhalte zum Klicken zu bewegen.

Auf Ebene der **sozialen Validierung** wird insbesondere der portugiesische Fußballprofi Cristiano Ronaldo als Testimonial für Chicken Road eingesetzt. Die Assoziation mit einer der bekanntesten Sportpersönlichkeiten der Welt soll Erfolg, Wohlstand und Vertrauenswürdigkeit auf die Werbung übertragen – ohne dass eine erkennbare offizielle Lizenzierung vorliegt. Ergänzt wird dies durch inszenierte User-Generated-Content-Ästhetik: Selfie-Videos von (hauptsächlich) Männern vor Villen oder Erklärvideos imitieren authentische Erfahrungsberichte mit den beworbenen Spielen.

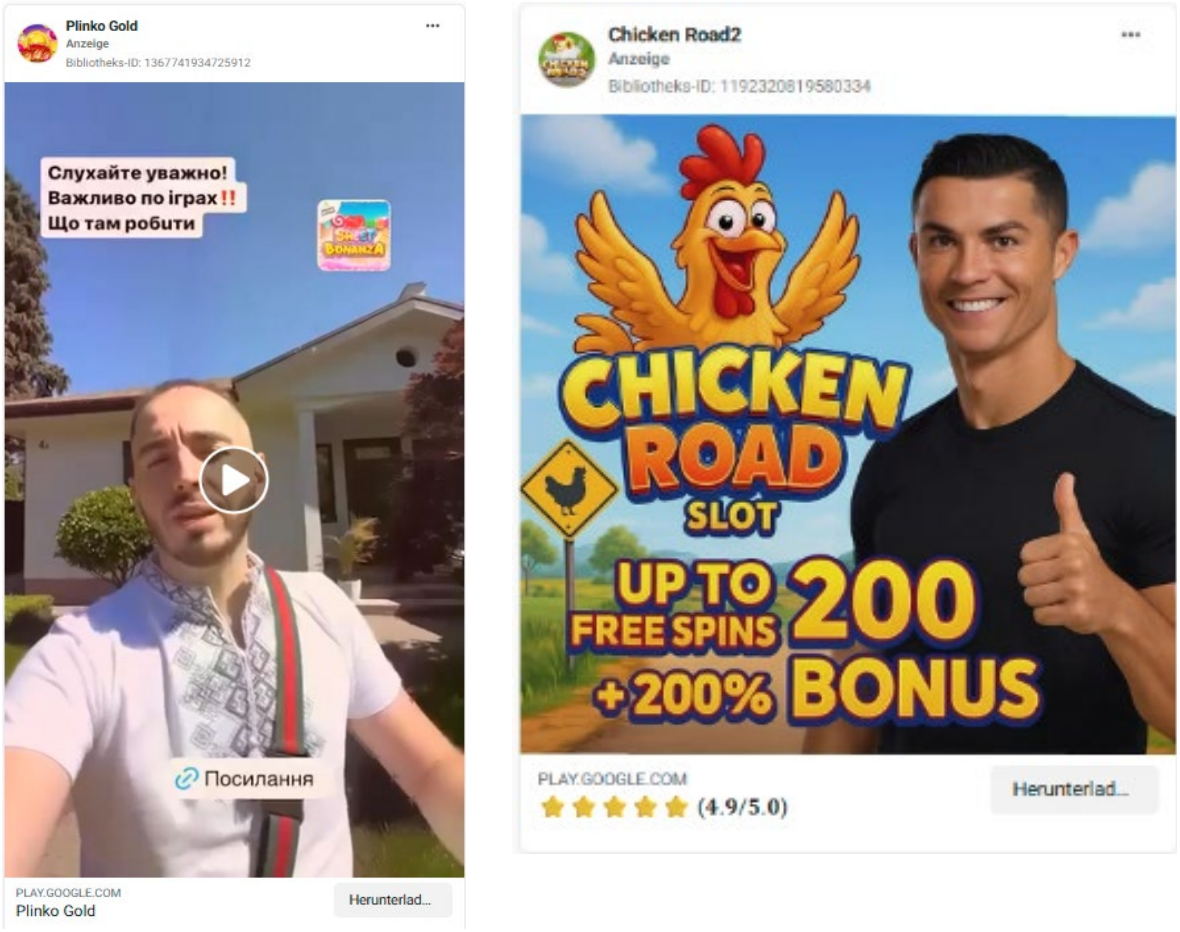

Abbildung 19: Soziale Validierung durch prominente Persönlichkeiten oder User-Generated-Content-Videos

Daneben kommt eine klassische **Bait-and-Switch Methode** zum Einsatz: Die Anzeigenvorschau für einige Chicken Road bewerbende Videos zeigt einen Golden Retriever Welpen – einen emotional wirkungsvollen, aber inhaltlich völlig irrelevanten Bildinhalt. Nach dem Klick auf das Video wird dann ein eindeutiges Werbevideo für das eigentliche Spielprodukt abgespielt. Die Irreführung

ist dabei nicht zufällig, sondern strategisch eingesetzt: Der emotionale Einstieg maximiert die Klickrate, bevor der eigentliche Inhalt offenbart wird.

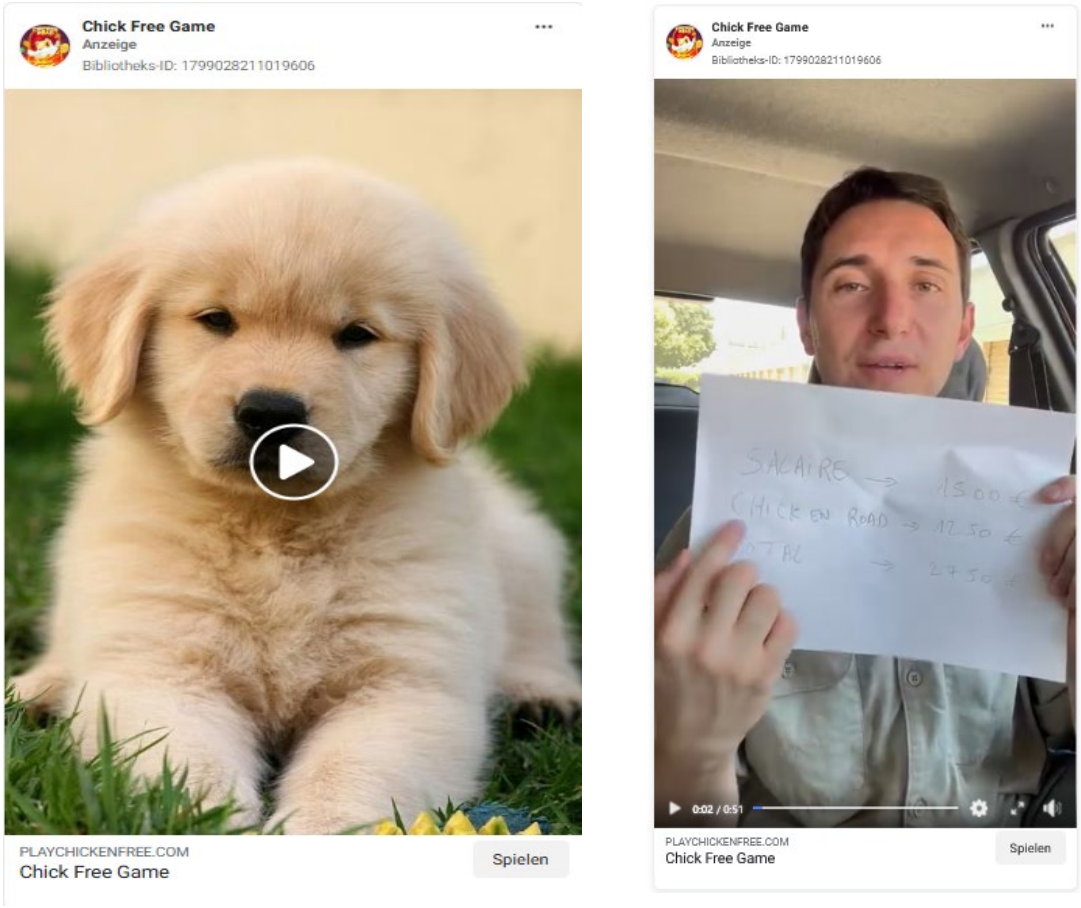

Abbildung 20: Beispiel der Bait-and-Switch Methode bei der Bewerbung von „Chicken Road Game“ (links: Vorschaubild; rechts: tatsächliches Video)

4.12. Fazit

In der qualitativen Analyse wurden die quantitativen Befunde vertieft und untersucht, mit welchen Strategien, Narrativen und Infrastrukturen betrügerische Werbeanzeigen auf Meta-Plattformen operieren.

Auf inhaltlicher Ebene nutzen betrügerische Akteur:innen über alle Betrugsschemata hinweg **Manipulationsstrategien**, die die Nutzer:innen zu unüberlegten Interaktion bewegen sollen – von Deceptive Design über die gezielte Konstruktion von Wissenslücken bis hin zum systematischen Missbrauch etablierter Vertrauensanker – Letzeres auch unter Einsatz von Künstlicher Intelligenz und Deepfakes. Im Hinblick auf die Zielgruppenansprache zeigt sich, dass nicht primär demographische Gruppen adressiert werden, sondern situative Vulnerabilitäten.

Eine besonders relevante Entwicklung ist die zunehmende **Verlagerung von Landing Pages hin zu Messenger-Diensten**, die insbesondere im Bereich des Investmentbetrugs beobachtet wurde. Diese Verlagerung entzieht betrügerische Aktivitäten der Nachvollziehbarkeit durch Behörden und Forscher:innen und nutzt gleichzeitig die vermeintliche Exklusivität privater Chat-Gruppen als Vertrauensmechanismus.

Die ergänzende Infrastrukturanalyse verdeutlicht schließlich, dass hinter dem scheinbar fragmentierten Betrugsökosystem **professionelle Akteur:innen** stehen – erkennbar an geteilten Serverstrukturen, einheitlichen Plattformlösungen und gemeinsamen Tracking-Diensten.

5. Sicherheits- & Compliance-Lücken auf Meta-Diensten

Der Digital Services Act verpflichtet VLOPs wie Meta Transparenzinstrumente bereitzustellen, die eine unabhängige Überprüfung von Werbeanzeigen ermöglichen. Die Meta-Werbebibliothek ist ein zentrales Instrument, das diese Transparenz gewährleisten soll. Im Rahmen der quantitativen und qualitativen Analyse wurden jedoch mehrere strukturelle Defizite identifiziert, die die Nachvollziehbarkeit und Überprüfbarkeit betrügerischer Werbeanzeigen einschränken.

5.1. Intransparenz bei zahlenden Personen

Artikel 39 DSA (EU 2022/2065) schreibt vor, dass durch die Werbebibliothek unter anderem Einblick in „die natürliche oder juristische Person" gewährt werden muss, „in deren Namen die Werbung angezeigt wird" oder „die für die Werbung bezahlt". Damit soll sichergestellt werden, dass die Verantwortlichen identifizierbar sind. Wie bereits in der quantitativen Analyse dargestellt, ist diese **Transparenz in der Praxis nicht gewährleistet**. Das Eingabe-Feld ist ein Freifeld und kann entsprechend beliebig von den Werbetreibenden befüllt werden. Im erhobenen Datensatz finden sich unter den Zahlenden Zahlenreihen, willkürliche Buchstabenfolgen sowie Markennamen, die missbraucht werden.

Diese Compliance-Lücke ist struktureller Natur: Sie betrifft alle untersuchten Betrugsschemata und wird systematisch genutzt, um die Nachvollziehbarkeit zu erschweren. Eng damit verbunden ist das Fehlen einer Identitätsverifikation. So reicht für das Schalten einer Werbeanzeige ein Standard-User-Account, für den lediglich Name, E-Mail-Adresse (oder Telefonnummer) sowie ein Geburtsdatum angegeben werden muss – Angaben, die die Nutzer:innen selbst eingeben und die nicht verifiziert werden.

Laut internen Meta-Dokumenten, die Reuters zugespielt wurden, verfolgt Meta eine „reactive only"-Strategie. So hat sich Meta bewusst gegen die flächendeckende Einführung einer universellen Identitätsverifikation entschieden und diese nur dort eingeführt, wo sie regulatorisch explizit eingefordert wird. Gleichzeitig zeigen die gleichen Dokumente, dass eine universelle Verifikation laut internen Tests von Meta selbst den Anteil betrügerischer Anzeigen signifikant – um bis zu 29% – reduzieren würde (Horwitz, 2025b).

5.2. Nicht mehr auffindbare Werbeanzeigen

Im Zuge der Recherche fiel auf, dass Werbeanzeigen, die im Rahmen der quantitativen Erhebung dokumentiert wurden, zu einem späteren Zeitpunkt über die Werbebibliothek nicht mehr auffindbar waren. Ein konkretes Beispiel betrifft das Keyword „Ella Weber“ (Ghost Stores): Im Erhebungszeitraum wurden für dieses Keyword knapp 2.300 Werbeanzeigen identifiziert. Bei einer erneuten manuellen Suche im Rahmen der qualitativen Analyse lieferte dasselbe Keyword keinerlei Ergebnisse mehr.

Gemäß Artikel 39 des DSA (EU 2022/2065) sind VLOPs verpflichtet, Informationen zu Werbeanzeigen mindestens ein Jahr lang in einem öffentlich zugängliche Repository bereitzuhalten – auch wenn diese nicht mehr aktiv sind. Das **Nichtauffinden zuvor dokumentierter Anzeigen** wirft daher die Frage auf, ob Meta dieser Aufbewahrungspflicht in vollem Umfang nachkommt.

Auch im Hinblick auf die bereits genannten Reuters-Recherchen kann das Verschwinden von Werbeanzeigen bewertet werden: So sollen interne Dokumente belegen, dass Meta-Mitarbeiter:innen die Werbebibliothek gezielt nach Keywords durchsuchen, die von Regulierungsbehörden, Forscher:innen und Journalist:innen verwendet werden, um die dabei gefundenen Anzeigen zu entfernen. Intern wird dieses Vorgehen als Management der **„prevalence perception“** bezeichnet, da damit die wahrgenommene Häufigkeit betrügerischer Inhalte bei externen Prüfungen reduziert werden soll. Diese Strategie wurde zunächst in Japan erprobt und anschließend global ausgerollt, unter anderem in Europa und den USA. Meta wies diese Darstellung in einer Stellungnahme gegenüber Reuters zurück und erklärte, dass das Entfernen von Anzeigen aus der Werbebibliothek keineswegs irreführend sei – im Gegenteil: Weniger sichtbare Betrugsanzeigen in der Bibliothek bedeuteten auch weniger betrügerische Anzeigen auf der Plattform (Horwitz, 2025b).

5.3. Weitere Werbeaktivität bei (vermeintlich) deaktivierten Accounts

In der quantitativen Erhebung wurden zahlreiche Anzeigen gefunden, die von Meta bereits entfernt wurden – u.a. aufgrund einer Seite oder eines Accounts, der deaktiviert wurde („This ad was run by an account or page we later disabled for not following our advertising standards“). Im Rahmen weiterer Erhebungen konnte jedoch beobachtet werden, dass zu einem späteren Zeitpunkt erneut Werbeanzeigen auf demselben Account mit derselben Page ID geschaltet wurden – trotz angeblicher Deaktivierung dieses Accounts. Dieses Phänomen geht über die bereits bekannte Praxis hinaus, dass deaktivierte Accounts unter leicht veränderten Namen (z. B. „Höhle der Löwen“ oder „Schneider Salzburg“ in zahlreichen Varianten) wieder auftauchen.

5.4. Werbeanzeigen über Textsuche nicht auffindbar

Eine weitere beobachtbare Lücke vonseiten Meta betrifft die Suchfunktion der Werbebibliothek. So werden – insbesondere beim Betrugsschema Investmentbetrug – immer wieder betrügerische Werbeanzeigen identifiziert, die über eine Textsuche nicht auffindbar sind. Ein Beispiel ist eine Werbung mit dem Text „EXKLUSIV: Benko gesteht, wohin das Geld wirklich ging“, die vom Account „Sorglode“ geschalten wurde. Die Anzeige ist über die Suche nach dem Accountnamen „Sorglode“ auffindbar. Eine **Suche nach Textphrasen** aus dem Anzeigentext – beispielsweise „Benko gesteht“ – lieferte jedoch **keine Ergebnisse**. Aus diesem Grund mussten einige Prominentennamen von der Keywords-Liste bei Investmentbetrug entfernt werden – zwar war bekannt, dass Werbeanzeigen zu diesen Keywords existieren, allerdings wurden mit der Textsuche keine Ergebnisse erzielt.

Ob es sich dabei um ein technisches Defizit oder um eine gezielte Einschränkung handelt, lässt sich von außen nicht abschließend beurteilen. Im Kontext der dokumentierten „prevalence perception“-Strategie (Horwitz, 2025b) scheinen solche Unschärfen jedoch systematisch zu sein.

5.5. Multiple Anzeigenversionen nicht einsehbar

Wie in Kapitel 5.2 „Täterstrategien zur Umgehung von Sicherheitsmechanismen & Content-Moderation“ beschrieben, nutzen betrügerische Akteur:innen häufig die Funktion der **dynamischen Anzeigenschaltung**, um betrügerische Inhalte in einer von mehreren Anzeigenversionen zu „verstecken“. Während die in der Werbebibliothek zunächst sichtbare Version harmlos erscheint, enthält eine der anderen Varianten die problematischen Inhalte – im Normalfall kann durch die unterschiedlichen Versionen geklickt werden, um (meist gegen Ende) die problematische Version zu sehen.

Im Rahmen der Recherche fiel jedoch zunehmend auf, dass diese Funktion nicht mehr zuverlässig funktioniert. In mehreren Fällen wurde zwar angezeigt, dass mehrere Versionen einer Werbeanzeige existieren, jedoch war nur eine einzige Version sichtbar. Dieses Defizit verhindert die Überprüfung dynamischer Anzeigen und entzieht Regulierungsbehörden sowie Forscher:innen eine wichtige Überprüfungsmöglichkeit für versteckte betrügerische Inhalte.

6. Zusammenfassung

Die vorliegende Untersuchung nutzt die durch den DSA vorgeschriebene Werbebibliothek von Meta, um die Größenordnung betrügerischer und problematischer Werbung systematisch zu erfassen. Dafür wurden acht zentrale Betrugsschemata identifiziert: Abo-Fallen, Investmentbetrug, Kreditbetrug, Jobbetrug, unseriöse Nahrungsergänzgungsmittelangebote, Ghost Stores, Fake-Shops (Fokus Markenimitation) und Online-Glücksspiele. Die Größenordnung der geschalteten Werbeanzeigen für diese Schemata auf den Plattformen Facebook und Instagram wurde quantitativ erhoben und mit einer qualitativen Analyse exemplarischer Anzeigen je Betrugsschema ergänzt.

Quantitative Erhebung: Zentrale Ergebnisse

Innerhalb von drei Monaten wurden über acht Betrugsschemata hinweg **634.000** betrügerische bzw. problematische Werbeanzeigen identifiziert. Diese erreichten **EU-weit über 1 Milliarde Impressionen,** allein in Österreich waren es rund 123 Millionen. Dabei dominieren insbesondere Online-Glücksspiele (knapp 450.000 Anzeigen), gefolgt von Investmentbetrug (83.216) und unseriösen Nahrungsergänzungsmittelangebote (27.171 Anzeigen), während Kreditbetrug (805) die geringste Anzeigenanzahl aufweist.

Diese Zahlen sind jedoch als konservative Untergrenze zu verstehen: Die Studie erhebt keinen Anspruch auf Vollständigkeit, da die Keyword-basierte Suche nur Anzeigen mit erkennbaren Mustern erfasst, die tatsächlichen Zahlen also deutlich höher liegen dürften. Zudem sind die Daten von der Vollständigkeit und Genauigkeit der von Meta bereitgestellten Informationen abhängig.

62,4% aller im Rahmen der Studie identifizierten Anzeigen waren zum Zeitpunkt der Erhebung bereits von Meta aufgrund von Verstößen **entfernt**. Zugleich weisen die identifizierten Anzeigen meist sehr **kurze Laufzeiten** von wenigen Tagen oder sogar Stunden auf, und neue Anzeigen mit vergleichbaren Inhalten erscheinen kontinuierlich.

Zudem zeigen sich schemaübergreifend strukturelle Muster in der Zielgruppenansprache: Während betrügerische Akteur:innen beim demografischen Targeting kaum nach Geschlecht oder Alter differenzieren, spiegeln die tatsächlichen Reichweitendaten eine **gezielte Ansprache situativ vulnerabler Gruppen** wider, die auch im Rahmen der qualitativen Analyse erhoben werden konnte. So erreichten etwa Werbungen für Nahrungsergänzungsmittel insbesondere eine ältere Zielgruppe, während Jobbetrug-Werbungen vor allem Personen im erwerbsfähigen Alter ansprachen.

Qualitative Analyse: Zentrale Ergebnisse

Über alle Betrugsschemata hinweg zeigen sich vier wiederkehrende Muster in Narrativen und der damit einhergehenden Zielgruppenansprache:

- **Deceptive Design:** Künstliche Verknappung, inszenierte Dringlichkeit oder „Confirmshaming" sind konsistente Deceptive Design Strategien, die Nutzer:innen zu schnellen, unüberlegten Entscheidungen verleiten sollen
- **Curiosity Gap:** Die systematische Konstruktion von Wissenslücken – zum Beispiel durch IQ-Tests oder angebliches Insider-Wissen über Finanzmärkte – wird in vielen Betrugsschemata genutzt, um die Neugierde der User in Handlungsimpulse zu übersetzen.
- **Missbrauch etablierter Vertrauensanker:** Bekannte Persönlichkeiten, Logos und Namen von Medienhäusern oder auch das Herstellen regionaler Bezüge werden systematisch missbraucht, um Glaubwürdigkeit zu imitieren und das Vertrauen in Bekanntes zu nutzen. Der zusätzliche Einsatz von KI-generierten Deepfakes kann diesen Effekt verstärken, z. B. wenn Prominenten Worte in den Mund gelegt werden, die sie so nie gesagt haben.
- **Ausnutzung situativer Vulnerabilitäten:** Beim Großteil der Betrugsschemata werden durch die verwendeten Narrative gezielt vulnerable Personen adressiert – weniger nach demografischen Merkmalen, sondern nach individuellen Lebenslagen. So werden etwa Personen in finanziellen Notlagen (Kreditbetrug), mit gesundheitlichen Sorgen (Nahrungsergänzungsmittel) oder Arbeitslose (Jobbetrug) durch die inhaltliche Gestaltung der Werbeanzeigen angesprochen.

Diese inhaltlichen Strategien gehen gleichzeitig einher mit kriminellen Taktiken, um möglichst unerkannt auf den Plattformen agieren zu können. Dafür werden unterschiedliche Sicherheitsmaßnahmen der Plattformen sowie die Content-Moderation umgangen. Dazu zählt:

- Cloaking, durch das Nutzer:innen mit einem Klick auf eine Werbeanzeige zu einer betrügerische Website weitergeleitet werden, Überprüfungssysteme jedoch eine harmlose „White Page" zu sehen bekommen;
- die Nutzung von kompromittierten und oftmals auch verifizierten Accounts, sowie
- das Schalten von multiplen Anzeigenversionen mittels der Funktion „Dynamic Ads", um betrügerische Anzeigen unter scheinbar harmlosen Anzeigen zu verstecken.

Dieses Zusammenspiel von inhaltlichen und technischen Strategien zeigt ein Betrugsökosystem bei dem die Infrastruktur der Plattformen genauso ausgenutzt werden, wie die Vulnerabilitäten der Zielgruppen.

Eine ergänzende Infrastrukturanalyse ausgewählter Weiterleitungsziele zeigt zudem, dass das Betrugsökosystem auf einer professionalisierten, teils geteilten technischen Basis operiert: Cloudflare wird flächendeckend genutzt, um die tatsächlichen Serverstandorte zu verschleiern und die Rückverfolgung zu erschweren. Gleichzeitig ermöglichen eingebettete Tracking-Dienste eine kontinuierliche Optimierung der Zielgruppenansprache. HTML-Ähnlichkeitsanalysen offenbaren zudem Cluster von Websites, die trotz unterschiedlicher Auftritte wahrscheinlich von denselben Akteur:innen betrieben werden.

Compliance-Lücken bei Meta

Im Zuge der qualitativen Analyse wurden zudem strukturelle Defizite vonseiten der Plattform selbst dokumentiert:

- **Intransparenz bei zahlenden Personen:** Das Freifeld für Zahlende wird systematisch von den Betrüger:innen mit falschen oder sinnlosen Angaben befüllt. Eine Identitätsverifikation findet nicht statt. Damit verstößt Meta gegen Artikel 39 DSA (EU 2022/2065).
- **Verschwinden dokumentierter Werbeanzeigen:** Zuvor erfasste Werbeanzeigen waren bei späteren Suchen in der Werbebibliothek nicht mehr auffindbar. Eine vollständige Analyse oder Nachvollziehbarkeit der auf Meta geschalteten Werbeanzeigen wird so erschwert.
- **Persistenz deaktivierter Accounts:** Auch nach einer Deaktivierung eines Accounts oder einer Seite aufgrund Nicht-Einhaltens von Policy-Vorgaben wurden unter derselben Page ID erneut Werbeanzeigen zu einem späteren Zeitpunkt geschaltet.
- **Eingeschränkte Textsuche:** Relevante Werbeanzeigen waren über die Textsuche nicht auffindbar – auch dadurch wird eine systematische Prüfung durch Behörden und Forschende erschwert.
- **Unvollständige Anzeigenversionen:** Insbesondere in den vergangenen Monaten wurde beobachtet, dass die Überprüfbarkeit multipler Anzeigenversionen bei dynamischen Anzeigenkampagnen teils nur eingeschränkt möglich ist, da in mehreren Fällen nur eine von mehreren Versionen in der Werbebibliothek sichtbar waren. Die betrügerischen Anzeigen konnten so nicht detektiert werden.

Auch wenn einzelne dieser Defizite auf technische Ursachen zurückzuführen sein können, legt die Gesamtschau der dokumentierten Compliance-Lücken in Verbindung mit den durch Reuters veröffentlichten internen Meta-Dokumenten – darunter eine „reactive only"-Verifikationsstrategie

sowie ein „Global Playbook" zum Management regulatorischer Wahrnehmung – einen systematische Vorgehensweise nahe.

Systemisches Risiko im Sinne des DSA

Die Untersuchung zeigt, dass die im Digital Services Act (DSA) vorgesehenen Transparenzmechanismen wichtige Ansatzpunkte für die regulatorische Aufsicht bieten. Die Möglichkeit, Werbeanzeigen systematisch zu erfassen und zu analysieren, ermöglicht eine evidenzbasierte Dokumentation der Problematik, die als Grundlage für Durchsetzungsmaßnahmen dienen kann.

Gleichzeitig verdeutlichen die Ergebnisse, dass die bloße Bereitstellung einer Werbebibliothek nicht ausreicht, um gegen betrügerische Werbeanzeigen vorzugehen. So zeigt die Studie auch, dass betrügerische und problematische Werbung auf Plattformen des Unternehmens Meta kein Randphänomen ist, sondern ein systemisches Risiko im Sinne von Artikel 34 DSA (EU 2022/2065) darstellt: Das Phänomen ist nicht auf Einzelfälle beschränkt, sondern betrifft über acht thematisch unterschiedliche Betrugsschemata hinweg zahlreiche Anzeigen mit Milliardenreichweiten.

Der DSA sieht vor, dass VLOPs systemische Risiken nicht nur ermitteln, sondern durch angemessene Maßnahmen minimieren müssen (Artikel 35 DSA). Die erhobenen Mängel deuten jedoch darauf hin, dass aktuelle Maßnahmen gegen betrügerische Werbeanzeigen zu wenig greifen.

7. Quellenverzeichnis

Abraham, J. (2025). *Global State of Scams 2025*.

Auer, V., Trell, N., & Brugger, M. (2025). *Dubiose Werbung auf Meta-Plattformen: Wie Celebrity-Ärzte zur Bewerbung von Nahrungsergänzungsmitteln missbraucht werden*. https://research.oiat.at/fileadmin/Research/Dokumente/Safe-NEM-Bericht.pdf

Beltzung, L., Krickl, J., Hölzl, I., & Lindley, A. (2024). *Platform Compliance—Fallstudien zu manipulativen Tricks in der Gestaltung von Interfaces und Prozessen*.

Bouchand, P., Salvatore Romano, Raziye Buse Çetin, Marc Faddoul, Karla Pajares Sangay, & Jinyu Liu. (2025). *Meta's Failing Ad Moderation: Health Scams Targeting EU Users*. AI Forensics. https://aiforensics.org/work/meta-health-ads

Brignull, H. (2023). *Deceptive Patterns*. Deceptive Patterns. https://www.deceptive.design/

Bundesministerium für Inneres. (2025). *Cybercrimereport 2024*. https://www.bmi.gv.at/magazin/2025_11_12/01_Cybercrime_Report.aspx

Burt, J. (2025, Juli 17). Emerging Cloaking-as-a-Service Offerings are Changing Phishing Landscape. *Security Boulevard*. https://securityboulevard.com/2025/07/emerging-cloaking-as-a-service-offerings-are-changing-phishing-landscape/

Europäische Kommission, London Economics, VVA Consulting, & Ipsos Mori. (2016). *Consumer vulnerability across key markets in the European Union*.

Europäisches Parlament & Rat der Europäischen Union. (2006). Verordnung (EG) Nr. 1924/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über nährwert- und gesundheitsbezogene Angaben über Lebensmittel. Amtsblatt der Europäischen Union, L 404, 9–25. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32006R1924

Europäisches Parlament & Rat der Europäischen Union. (2022). Verordnung (EU) Nr. 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste). Amtsblatt der

Europäischen Union, L 277, 1–102. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2065

Federal Trade Commission. (2023). FTC Issues Orders to Social Media and Video Streaming Platforms Regarding *Efforts to Address Surge in Advertising for Fraudulent Products and Scams*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18*, 1–14. https://doi.org/10.1145/3173574.3174108

Hatmaker, T. (2023, Mai 5). Hacked verified Facebook pages impersonating Meta are buying ads from Meta. *TechCrunch*. https://techcrunch.com/2023/05/05/hacked-verified-facebook-pages-impersonating-meta-are-buying-ads-from-meta/

Horwitz, J. (2025a). Meta is earning a fortune on a deluge of fraudulent ads, documents show. *Reuters*. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Horwitz, J. (2025b, Dezember 31). Meta created 'playbook' to fend off pressure to crack down on scammers, documents show. *Reuters*. https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763–783. https://doi.org/10.1002/mar.1029

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

OCCRP. (2025). *Scam Operations Relied on Third-Party Marketing Companies for Steady Stream of Potential Victims*. https://www.occrp.org/en/project/scam-empire/scam-operations-relied-on-third-party-marketing-

companies-for-steady-stream-of-potential-victims

Österreichisches Institut für Angewandte Telekommunikation. (2025). *Verbreitung von Abo-Fallen durch Google Ads*. ÖIAT. https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf

Sapra, B. (2020). *Facebook just filed a lawsuit against a software engineer who it says was helping scammers dodge its ad-review system and post ads related to coronavirus, cryptocurrency and diet pills*. Business Insider. https://www.businessinsider.com/facebook-sues-engineer-leadcloak-helping-covid-19-scammers-ads-2020-4

Scott, K. (2021). You won't believe what's in this paper! Clickbait, relevance and the curiosity gap. *Journal of Pragmatics*, *175*, 53–66. https://doi.org/10.1016/j.pragma.2020.12.023

Social MediaLab. (2025, April 21). The Hidden Game: How Scammers Use „Chameleon Ads" to Bypass Meta's Moderation. *Social Media Lab*. https://socialmedialab.ca/2025/04/21/the-hidden-game-how-scammers-use-chameleon-ads-to-bypass-metas-moderation/

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Vorster, A. (2026). *Fraud and Scams in 2026: What Benelux Banks Can Learn from The Global State of Scams*. https://thebankingscene.com/opinions/fraud-and-scams-in-2026-what-benelux-banks-can-learn-from-the-global-state-of-scams

Watchlist Internet. (2022a). *So schützen Sie sich vor betrügerischen Kreditangeboten*. https://www.watchlist-internet.at/news/so-schuetzen-sie-sich-vor-betruegerischen-kreditangeboten/

Watchlist Internet. (2022b, März 1). *So schützen Sie sich vor betrügerischen Investmentplattformen*. Watchlist Internet. https://www.watchlist-internet.at/news/so-schuetzen-sie-sich-vor-betruegerischen-investmentplattformen/

Watchlist Internet. (2024). *Promis als Lockvögel: Werbung für betrügerische Investmentplattformen erreicht täglich 200.000 Österreicher:innen*. Watchlist Internet. https://www.watchlist-internet.at/news/werbung-promis-investmentbetrug/

Watchlist Internet. (2025a). *Betrügerische Jobangebote*. Watchlist Internet. https://www.watchlist-

internet.at/liste-jobangebote/

Watchlist Internet. (2025b). *Betrügerische Werbeanzeigen: Mehr als 30 Millionen Mal an Personen in Österreich ausgespielt.* Watchlist Internet. https://www.watchlist-internet.at/news/betruegerische-werbeanzeigen-mit-vermeintlicher-geschaeftsschliessung/

Which. (2022). *TOWARD A FUTURE WITHOUT FRAUD: How platforms can do more to tackle misleading and fraudulent adverts online*. Site. https://www.which.co.uk/policy/policy/digital/9228/toward-a-future-without-fraud-how-platforms-can-do-more-to-tackle-misleading-and-fraudulent-adverts-online