Anlagebetrug erkennen

Wie Betrugsmaschen funktionieren und wie Sie sich schützen können
Auf Warnsignale von Anlagebetrug achten
Wie Kriminelle mit Kryptowährungen locken
Checklisten, Anlaufstellen und die fünf Gebote der sicheren Geldanlage

Europäisches Verbraucherzentrum Österreich

20 Jahre ECC-Net

Rat und Hilfe für Verbraucher in Europa

Geld weg durch Anlagebetrug

Der Finanzmarkt ist ständig in Bewegung. Mal locken hohe Gewinne, mal verunsichern Verluste. Genau das nutzen Betrüger aus. Sie greifen aktuelle Trends auf, passen ihre Betrugsmaschen an – und wirken so für viele glaubwürdig. Besonders stark betroffen: der Bereich Kryptowährungen. Laut Statistik ist Betrug mit Krypto-Werten inzwischen die häufigste Form von Anlagebetrug in Österreich. Im Folgenden zeigen wir, wie ein solcher Krypto-Betrug typischerweise abläuft.

1 – Werbeköder und Anmeldung auf Fake-Seite

Alexander sieht auf Instagram ein aufregendes Kurzvideo. Ein berühmter Rennfahrer berichtet von hohen Gewinnen mit einem bestimmten Finanzprodukt – und empfiehlt es ausdrücklich. Die Anzeige führt auf eine eigens erstellte Website namens Coin-Wunder.de. Dort sieht Alexander erste Informationen zum lukrativen Angebot und trägt neugierig Namen, E-Mail-Adresse und Telefonnummer ein.

- Aufdringliche Werbung oder Reels mit großen Versprechen auf Social Media
- Deepfakes setzen Promis täuschend echt in Szene – ohne deren Wissen
- Verlinkte Webseiten sehen professionell aus, enthalten aber keine echten Anbieterinfos

2 – Erste Manipulation durch persönlichen Kontakt

Kurz nach der Anmeldung wird Alexander von einer Mitarbeiterin von Coin-Wunder.de angerufen. Beim angeblichen „Kundencheck" erfragt sie Beruf, Vermögen und finanzielle Ziele. Das Gespräch wirkt professionell und vertrauenswürdig. Doch in Wahrheit beginnt hier die gezielte Einflussnahme.

- „Betreuer:innen" melden sich persönlich und rufen mit verschiedenen Nummern an – oft aus Deutschland, der Schweiz oder Großbritannien
- Abfrage von Lebenssituation und Vermögen – wie viel Geld ist vorhanden
- Eindruck von Exklusivität – Opfer fühlen sich ausgewählt

3 – Fernwartung und kleine Testbeträge

Es folgt ein angeblicher Verifizierungsprozess. Nicht unüblich bei Kryptohandel (KYC), denkt Alexander. Auf Verlangen schickt er Kopien von Pass und Kreditkarte an Coin-Wunder.de. Er kennt sich mit Kryptowährungen nicht aus, und lässt sich mittels Fernwartungssoftware das vermeintliche Konto einrichten. Danach zahlt er, wie vorgeschlagen, einen ersten Kleinbetrag ein.

- Unechte Identitätsprüfung – Kriminelle missbrauchen ab nun die übermittelten Ausweisdaten
- Opfer installieren Teamviewer oder Anydesk und geben so Kontrolle über ihre Geräte ab
- Testeinzahlung einer geringen Summe – meist 250 Euro

4 – Vertrauen und größere Investitionen

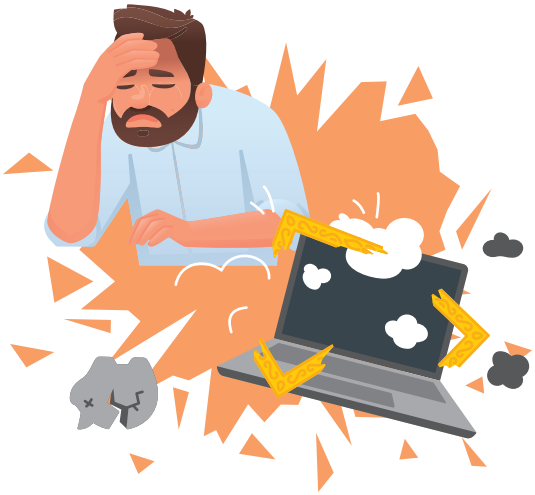
Alexander sieht erste Erfolge: Das Dashboard zeigt steigende Zahlen, zwei Auszahlungen à 50 Euro klappen problemlos. Dann übernimmt ein neuer „Account Manager“ die Betreuung. Herr Braunbart meldet sich regelmäßig, wird aber zunehmend fordernd. Überweisungen sollen wiederholt, Verluste mit Nachschüssen ausgeglichen werden. Per Fernzugriff „unterstützt“ er bei der Abwicklung. Eine Telegram-Gruppe mit weiteren angeblich erfolgreichen Anlegern erhöht den Druck – Alexander investiert weiter.

- Kursanstiege im Fake-Dashboard: Alles sieht nach Erfolg aus
- Kleine Auszahlungen sind möglich
- Emotionale Bindung durch persönliche Gespräche und gemeinsames „Traden“– Kritik wird ausgeblendet
- Opfer erhöhen Einsatz

5 – Hinhalten und auspressen

Mit zunehmendem Druck wird Alexander misstrauisch und möchte größere Auszahlungen haben. Doch plötzlich tauchen unerwartete Hindernisse auf. Auszahlungen seien aufgrund von Zufallsereignissen derzeit unmöglich. Ein Hackerangriff habe die Plattform lahmgelegt. Herr Braunbart, der Berater, hätte einen Unfall gehabt. Hingegen drängt Coinwunder.de mit neuen Vorwänden zu letzten Einzahlungen. Unerwartete Gebühren seien notwendig.

- Taktisches Hinhalten: Technische Probleme oder Sicherheitslücken verhindern momentan angeblich alle Auszahlungen
- Letztes Geld herauspressen: Angebliche Steuern oder Freischaltgebühren für Auszahlung nötig



6 – Plattform weg, Geld weg

Alexander will endlich sein Geld zurück – doch zeigt sein Konto plötzlich massive Verluste. Kurz darauf meldet sich Herr Braunbart ein letztes Mal: Das gesamte Kapital sei verloren, das Risiko habe immer bestanden. Danach ist die Plattform von Coin-Wunder.de und deren Personal verschwunden. Diese Taktik nennt sich „Burnen“ und ist gezielt und jederzeit einsetzbar. Die Kriminellen haben sich abgesetzt – mit allem, was sie bekommen konnten.

- Auf Einzahlungsstopp durch die Opfer folgt der angebliche Totalverlust
- Plötzlicher Rückzug: Plattform, Ansprechpartner und Website verschwinden – der Betrug ist abgeschlossen

Geld gut anlegen – Schritt für Schritt

Bei der Geldanlage kommt es darauf an, Ziele, Risiko, Laufzeit und Kosten im Blick zu behalten. Wichtig ist, Grundbegriffe wie Rendite, Risiko, Diversifikation und Liquidität zu verstehen. Denn sie bestimmen, wie sinnvoll und passend eine Anlage für die eigene Situation ist.

1. Anlageziele klar festlegen und passend investieren

Bevor Sie Geld anlegen, fragen Sie sich: Wofür spare ich und wann möchte ich über das Geld verfügen? Eine sinnvolle Aufteilung unterscheidet zwischen

- kurzfristigem Bedarf (für unerwartete Ausgaben),
- mittelfristigen Zielen (z. B. Auto, größere Reise) und
- langfristigem Vermögensaufbau (z.B. Pension).

Für kurzfristige Rücklagen eignen sich täglich verfügbare Konten, auch wenn sie kaum Zinsen bringen.

Fonds und ETFs bieten langfristig oft höhere Erträge, sind aber nicht jederzeit verlustfrei verkäuflich. Für langfristige Ziele können Finanzprodukte mit Bindung sinnvoll sein: Sie schwanken zwar im Kurs, bieten aber bessere Renditechancen. Ein regelmäßiger Sparplan ist eine gute Möglichkeit, schrittweise Vermögen aufzubauen.

Tipp: Planen Sie nur mit Beträgen, auf die Sie wirklich verzichten können. So vermeiden Sie unnötigen Druck durch Kursschwankungen.

Was sind ETF?
Was bedeutet Clearing?
Abkürzungen und englischsprachige Fachausdrücke erklärt das Glossar der Finanzmarktaufsicht
www.fma.gv.at/glossar

2. Den richtigen Mix wählen

Eine gute Anlagestrategie setzt nicht nur auf ein einziges Produkt. Wer breit streut, ist besser gegen Schwankungen am Markt geschützt! Je höher die Ertragsaussicht, desto größer meist auch das Risiko. Kombinieren Sie sichere Anlagen (z. B. ein gebundenes Sparkonto) mit renditestärkeren Möglichkeiten. Ein ETF verteilt Geld beispielsweise auf verschiedene Kapitalprodukte. So sinkt das Risiko, da ein Verlust in einem Bereich durch Gewinne in einem anderen ausgeglichen wird. Während Fonds und ETFs langfristig oft höhere Erträge bieten, sind einige davon nicht ohne Abstriche loszubekommen. Da bei einem frühzeitigen Ausstieg Kosten entstehen können, ist es sinnvoll, solche Produkte zumindest mittelfristig (drei bis fünf Jahre) zu halten.

Nicht zu einer einzigen Lösung drängen lassen! Gute Finanzberatung geht auf Alternativen und die angemessene Behaltedauer ein. Sie findet mit Unterlagen und Protokoll statt!

3. Kosten und Anbieter vergleichen

Depotgebühren, Verwaltungskosten und Ausgabeaufschläge können Erträge erheblich schmälern. Onlineangebote sind oft günstiger, aber Vorsicht: Investieren Sie nur bei lizenzierten Anbietern. Seien Sie wachsam bei Tipps von „Finfluencern“ auf TikTok oder YouTube. Nicht alles, was dort empfohlen wird, ist seriös, oft steckt kurzfristige Abzocke dahinter.

Nutzen Sie Vergleichsportale, um sich einen ersten Überblick zu verschaffen. Beachten Sie, dass die empfohlene Behaltefrist kein Zufallswert ist, sondern dazu dient Kursschwankungen und laufende Kosten auszugleichen.

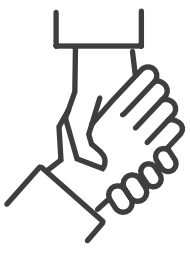
Verständliche Antworten auf die häufigsten Finanzfragen finden Sie im FMA Blog „Reden wir über Geld“.

4. Lockangebote mit Risiko

Unerbetene Anrufe, überraschende Angebote, hoher Zeitdruck: das sind typische Betrugsmerkmale. Kriminelle wirken professionell und nutzen Unsicherheit gezielt aus. Fragen Sie sich immer: Warum werde gerade ich angerufen? Ist die Rendite realistisch? Worin liegt das Risiko?

Googlen Sie nach dem Unternehmensnamen kombiniert mit den Worten „Erfahrung“ oder „Warnung“. Bei Zweifel **vor einem Abschluss** bei FMA oder VKI anrufen (siehe Rückseite).

5. Keine Scheu vor Hilfe



Oft kommen fragwürdige Finanzangebote von langjährigen Bekannten. Dabei handelt es sich nicht selten um „Pyramidenspiele“ oder „Krypto-Fallen“. Aus Scham und weil Betroffene gezielt unter Stress gesetzt werden, schweigen viele über Bedenken und Verluste. Wenn der Druck auf Sie stetig zunimmt, sollten Sie Fachberatung zu Hilfe ziehen.

Investmentbetrug läuft professionell ab

Immer mehr Menschen in Österreich werden Opfer von professionell organisiertem Anlagebetrug. Dahinter stehen internationale kriminelle Netzwerke, die mit hoher technischer und organisatorischer Raffinesse arbeiten. Scheinbar seriöse Angebote – etwa durch betrügerische Online-Broker, Bekanntschaften auf Dating-Plattformen oder überraschende Anrufe mit Renditeversprechen – entpuppen sich oft als Teil eines ausgeklügelten Systems.

Ein zentrales Element dieser Betrugsstrukturen sind professionell geführte Callcenter. Dort arbeiten „Agents" in klar organisierten Teams, unterstützt von Managern und einem Backoffice für IT, Zahlungsabwicklung und Dokumentenfälschung.

Kriminelle Dienste auf Bestellung

Zusätzlich werden Dienste externer Spezialisten zugekauft (Crime-as-a-Service), etwa Hacker oder Programmierer für die Erpressungssoftware (Ransomware) oder die Manipulation der Tradingplattformen und Webseiten. Auch die Werbung selbst wird oft ausgelagert: Dubiose Werbefirmen – sogenannte „Affiliates" – locken mit gefälschter Promi-Werbung, aggressiven Online-Anzeigen oder mit Phishing-Mails an gestohlene Emailkontakte die potenziellen Opfer an.

Das erbeutete Geld wird anschließend über ein internationales Netzwerk aus Briefkastenfirmen, Zahlungsdienstleistern und Kryptowährungen verschleiert.

Exekutive ebenfalls vernetzt

Aber auch die Polizei reagiert mit grenzüberschreitender Zusammenarbeit und geht gegen diese crime networks über Landesgrenzen hinweg vor. Investmentbetrug gilt laut Interpol mittlerweile als eine der größten kriminellen Bedrohungen in Europa. 2023 unterstützte die Organisation Ermittlungen zu rund 700 größeren Fällen – mit einem Gesamtschaden von über 1,1 Milliarden Euro. Die Zahlen steigen rasant – das zeigt auch die österreichische Kriminalstatistik.

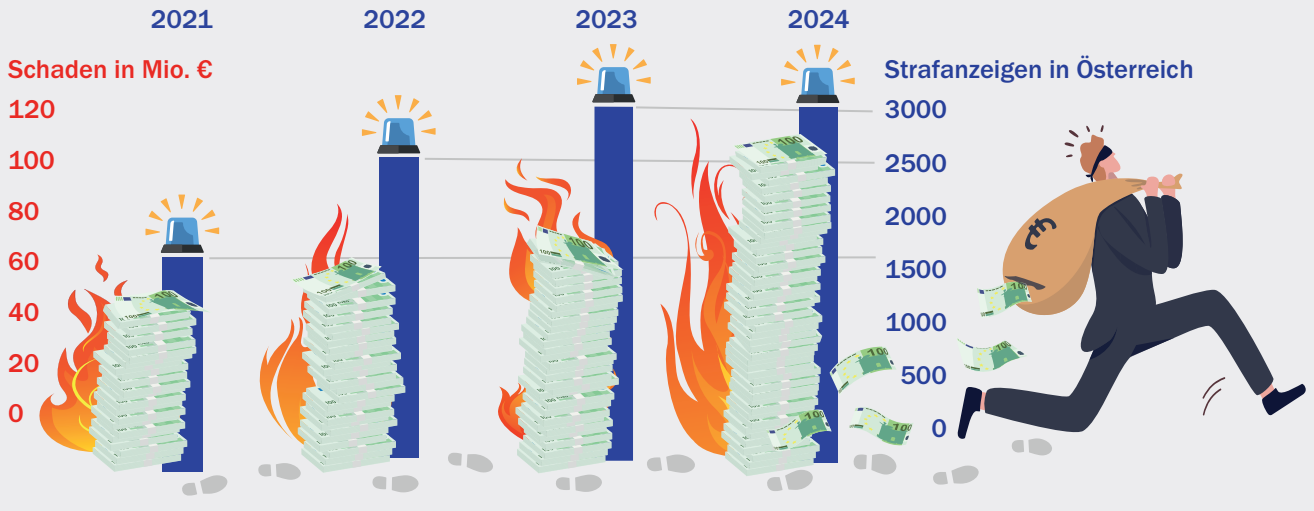
Wenn Sie Opfer eines Betrugs geworden sind:

1. Kontakt zu den Betrüger:innen abbrechen. Falls eingerichtet, Fernzugriff auf Ihren Geräten kappen!
2. Passwörter sofort ändern!
3. Beweise sichern: Chatverläufe, verdächtige Webseiten, E-Mails, Telefonnummern, Screenshots von Plattform und Konto. Je mehr Sie dokumentiert haben, desto aussichtsreicher die folgende Ermittlung.
4. Erstatten Sie rasch Anzeige bei der nächsten Polizeidienststelle. Nehmen Sie betroffene Geräte (Smartphone, Tablet, Laptop) mit.
5. Informieren Sie die Finanzmarktaufsicht und die Meldestelle für Internetkriminalität, damit potenzielle Opfer gewarnt werden.

Ermittlungen unterstützen

Schildern Sie den Sachverhalt klar mit dem gesamten Ablauf. Wie kam es zur Investition? Welche Zahlungen wurden wann, vom wem und wohin durchgeführt? Wie lief der Kontakt mit den Kriminellen ab? Opfer von Krypto-Betrug sollten zur Anzeige möglichst Folgendes parat haben:

- Namen der Kryptowährungen
- Kryptowährungsadressen
- Transaktions-Hashes
- verwendete Wallets und Exchanges
- Aufstellung der getätigten Transaktionen



Kampf gegen Anlagebetrug: 300 Millionen Euro Schaden, 11.000 Anzeigen (2021-2024) Quelle: Bundeskriminalamt

Betrug erkennen, bevor es passiert

Wer die Tricks kennt, fällt seltener darauf herein. Auf diesen beiden Seiten sind die derzeit in Österreich häufigsten Maschen und entsprechende Warnzeichen nach Häufigkeit geordnet. Vertrauen Sie keinen unbekannten Anrufen oder einer hochtrabenden Werbung im Netz – es könnte der Einstieg in einen perfiden Betrug sein.

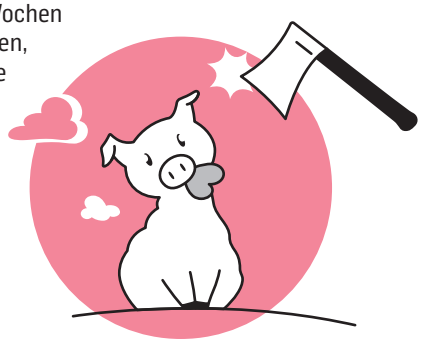
1. Crypto Trading Fraud – weltweit am häufigsten

Über auffällige Social-Media-Werbung werden hohe Gewinne mit Aktien, Krypto-Assets, Forex oder CFDs versprochen. Wer sich registriert, wird kurz darauf kontaktiert. Zum Einsatz kommen betrügerische Plattformen, die echten Online-Brokern täuschend ähnlich sind: Mit seriös wirkenden Logos, Charts und Zugängen zu Nutzerkonten. Doch alles ist nur Show – die Kursverläufe sind manipuliert, die Gewinne erfunden.

- Ersteinstieg mit geringen Summen (meist 250 Euro)
- Manipulierte Trading-Software oder Fake-Plattformen täuschen Handel nur vor
- Angebliche Gewinne sind fingiert
- Opfer werden zu immer höheren und weiteren Einzahlungen gedrängt
- Kriminelle Callcenter und internationale Geldwäsche-Netzwerke im Hintergrund

2. Emotionales Vertrauen als Falle – der „Pig Butchering Scam“

Vertrauen wird gezielt aufgebaut – und dann eiskalt ausgenutzt. Über Soziale Medien, Datingportale und Messenger-Apps bauen Kriminelle Kontakte auf. Sie erschleichen sich über Wochen oder Monate Vertrauen, eine freundschaftliche Beziehung oder Hoffnung auf eine romantische Zukunft. Dann folgen „sichere“ oder exklusive Investmentchancen oder Bitten um Geld wegen einer angeblichen Notlage.

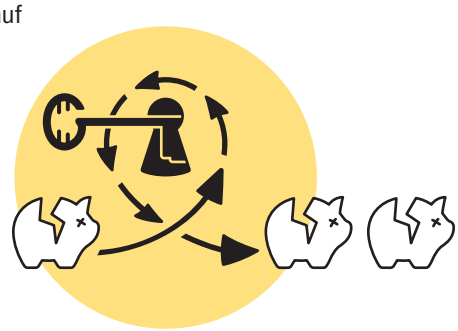


Der Begriff „Pig Butchering“ („Schweineschlachten“) beschreibt bildlich das Vorgehen: Mit Aufmerksamkeit, Zuneigung und falschen Versprechungen wird „gemästet“. Danach zu hohen fatalen Scheininvestitionen gedrängt. Weltweit wird auf diese Weise um viele Milliarden betrogen.

- Schnelle emotionale Bindung ohne reale Treffen, alles findet online statt
- Geschichten oder Identitäten sind nicht überprüfbar
- Plötzlicher Themenwechsel zu Anlagetipps oder Manipulation zu Überweisungen aus Mitleid, Liebesbekundungen oder angeblichen Notlagen
- Genaue Zahlungsanweisung über unbekannte Apps oder in Kryptowährung

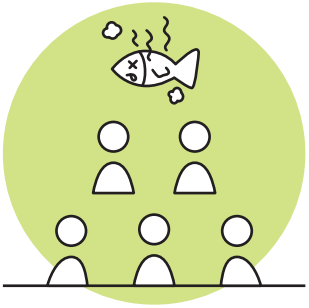
3. Recovery Scam - der Betrug nach dem Betrug

Monate nach dem ersten Betrug durch Fake-Plattformen (siehe Nr.1) melden sich angebliche Behörden, Kanzleien oder Krypto-Firmen. Sie behaupten, das verlorene Geld sei auf einem Konto gesichert, und warte darauf „freigeschaltet“ zu werden. Dafür sollen Opfer behördliche Gebühren, Steuern oder Lizenzen bezahlen. Das Ganze klingt vorerst plausible, da Details aus dem ersten Betrug genannt werden. Jedoch stammen diese Informationen aus Datenleaks oder wurden den ersten Kriminellen abgekauft. Verzweifelte Geschädigte sehen hier die letzte Chance auf Rettung – und verlieren erneut viel Geld.



- Drängen zur schnellen Zahlung durch behauptete gesetzliche Fristen
- Behörden verlangen niemals Gebühren für Rückholung von verlorenem Geld
- Behörden nutzen für Geldforderungen niemals Emails, Anrufe oder Messenger
- Echte Behörden fordern immer formell mit Bescheiden per Post

4. Ketten- oder Pyramidenspiele

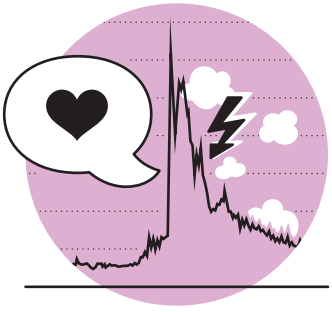


Hinter auffälliger Online-Werbung für gewisse Krypto-Werte (z. B. OneCoin) oder Wertpapiere steckt oft ein Schneeballsystem. Neue Mitglieder investieren Geld – und finanzieren damit die Auszahlungen an andere Geschädigte, die wiederum die nächsten Opfer in die Falle locken. Kein echtes Geschäftsmodell, nur eine endlose Rekrutierung neuer Personen, die in die Falle tappen. Das eingezahlte Geld ist im System gefangen. Es ist nicht in andere (echte) Währungen oder unabhängige Marktplätze übertragbar. Das System wächst in die Breite – und bricht später zusammen. Fast alle verlieren ihr gesamtes Geld.

- Hohe Renditen ohne klar erkennbares Produkt oder Geschäftsmodell
- Druck, neue Mitglieder zu werben – Empfehlungen werden mit Boni belohnt
- Intransparente Plattformen, unbekannte Unternehmen
- Kein freier Zugriff aufs Geld – Auszahlungen verzögert, verweigert oder eingeschränkt? Höchste Alarmstufe!

5. Unbekannte gehypte Kryptos als Falle

Bei der Abzocke mit ICOs (Initial Coin Offerings) locken Fake-Broker mit hohen Gewinnaussichten durch ein neues Krypto-Projekt und sammeln für dessen angebliche Gründung Gelder ein. Ein Geschäftsbetrieb wird nur zum Anschein aufrechterhalten. Danach folgt der von vornherein geplante „Exit" oder „Rug Pull", bei dem sich die Kriminellen mit allen Einlagen aus dem Staub machen. Dieses geplante Verschwinden zieht allen anderen bildlich gesprochen den Teppich unter den Füßen weg.



- Plattformbetreiber:innen anonym, Verantwortliche nicht greifbar
- Zulassung fehlt, keine externe Prüfung oder Regulierung
- Nutzen des Tokens nicht erkennbar und nur auf dubiosen Plattformen im Handel
- Unseriöse Finfluencer betreiben mit unrealistischen Gewinnversprechen auf TikTok, Instagram oder Telegram einen künstlichen Hype für das Projekt
- Keine Kontaktaufnahme außerhalb von moderierten und unkritischen Chats
- Eine Variante davon nennt sich „Pump and Dump": Dabei kaufen die Initiatoren des Betrugs eine echte, aber wertlose Kryptowährung in großen Mengen, und bewerben diese aggressiv. Ahnungslose Neulinge bewirken daraufhin einen kurzen Höhenflug. Schlagartig verkaufen die Drahtzieher:innen nun all ihre Bestände und lösen einen Komplettabsturz aus. Von diesem erholen sich weder Währung noch die ehrlichen Investitionen.

6. Cold Calling – hier spricht Ihre Bank

Kriminelle rufen unangekündigt an und geben vor z.B. von einer bekannten Bank zu sein. Als Sonderangebot werden exklusive Investitionen mit hohen, sicheren Gewinnen angepriesen. Es wird versucht Vertrauen zu gewinnen und zu einer Einzahlung auf ein angebliches Investitionskonto zu überreden. Der Anruf ist freundlich, professionell und scheint vertrauenswürdig. Gleichzeitig wird subtil Druck aufgebaut: Das Angebot sei streng limitiert oder nur heute verfügbar.

- Vorsicht bei überraschendem Anruf von unbekannter Nummer mit Anlagetipps
- Alarmsignale: Zeitdruck und Phrasen wie „letzte Chance" oder „nur heute"
- Schriftliches Angebot unmöglich: Wer nichts belegt, hat etwas zu verbergen
- Kein Rückrufkontakt
- Sagen Sie klar Nein und beenden Sie das Gespräch

CHECKLISTE BEVOR SIE INVESTIEREN

Der Finanzdienstleister ist zugelassen
Investmentplattformen und Online-Broker im Finanz- und Kryptowert Bereich brauchen eine staatliche Lizenz. Prüfen Sie für
Österreich bei der FMA
und den Europäischen Wirtschaftsraum bei der ESMA

Vor dem Unternehmen wird nicht gewarnt
Betrugsfirmen sind hier offiziell gelistet:

FMA (Ö) BaFin (DE) SEC (USA) IOSCO (weltweit)

Sie haben einen Investmentplan und kennen Ihre Ziele, Dauer, Risiken und Alternativen

ACHTSAM BLEIBEN

Man lockt Sie mit unrealistischen Renditen
Nicht das Blaue vom Himmel versprechen lassen!

Vertrauliche Informationen werden abgefragt
nachdem Sie einem zugeschickten Link folgten. Schließen Sie die Seite!

Sie sollen Fernzugriff erlauben
Nie mit Fernwartungssoftware die Kontrolle über Ihren Computer, das Handy oder Konto abgeben!

Die Anlageplattform hat keine Lizenz
Prüfen Sie ob das Unternehmen über die nötige Berechtigung verfügt!

Man drängt Sie zu einer schnellen Entscheidung
Kluge Entscheidungen brauchen Zeit und verlässliche Informationen!

Auffälligkeiten und Warnhinweise auf Ihrem Konto
Ungewöhnlichen Aktivitäten oder dubiosen Logins auf Ihrem Konto sofort auf den Grund gehen!

FMA

Banken, Versicherungen, Wertpapierfirmen und andere Finanzunternehmen benötigen eine **Zulassung** der Finanzmarktaufsicht (FMA), um in Österreich Finanzdienstleistungen anbieten zu dürfen. Diese Unternehmen sind in der öffentlichen **Unternehmensdatenbank** auf der Webseite der FMA gelistet. Die FMA schreitet ein, wenn Anbieter ohne Erlaubnis – und damit oft auch betrügerisch – tätig sind. Fragen Sie im Zweifel die Verbraucherinformation der FMA, ob ein Unternehmen seriös und zugelassen ist:

Schriftliche Anfragen www.fma.gv.at/kontakt
Verbrauchertelefon: +43 (0)1 – 249 59 3444, Mo-Do 09:00 – 11:30 und Do 13:00 – 16:00 Uhr

Bundesministerium Inneres
Bundeskriminalamt

Geschädigte erstatten **Anzeige** direkt in der **nächstgelegenen Polizeidienstelle**. Melden Sie Betrugsfälle mit Onlinehintergrund zusätzlich der **Meldestelle für Internetkriminalität**.
Für Prävention oder sonstige Opferanliegen wenden Sie sich an das **Landeskriminalamt** Ihres Bundeslandes:
www.bundeskriminalamt.at/201

Europäisches Verbraucherzentrum Österreich
ECC-Net

Das **Europäische Verbraucherzentrum** ist beim Verein für Konsumenteninformation (VKI) angesiedelt. Im ECC-Net mit 30 Stellen in der EU, Großbritannien, Island und Norwegen prüfen wir die Seriosität ausländischer Firmen über internationale Datenbanken. Wichtig: Bei einem konkreten Betrugsverdacht empfehlen wir, zusätzlich eine Anzeige bei der Polizei zu erstatten und die Finanzmarktaufsicht (FMA) zu informieren.

Schriftliche Anfragen www.europakonsument.at/beschwerdeformular
EVZ-Hotline: +43 (0)1 – 588 77 81, Di und Do 9:00 – 13:00 Uhr

Wir bedanken uns bei der FMA und dem Bundeskriminalamt für die Zusammenarbeit bei der Erstellung der Informationen.

Finanziell unterstützt durch die Europäische Union

VKI

Eine Initiative der Europäischen Kommission und des VKI

Impressum: Herausgeber und Medieninhaber
Verein für Konsumenteninformation
Linke Wienzeile 18, 1060 Wien, ZVR-Zahl 389759993
Verlags- und Herstellungsort Wien
Grafische Gestaltung Nicole Ender/VKI
Piktogramme Barbara Weingartshofer, NAU*Design
Coverbild, Illustrationen stock.adobe.com
Druck Walstead Leykam Druck GmbH, 7201 Neudörf