# KRYPTO BETRÜGEREIEN & ABZOCKEN

## BLEIBEN SIE WACHSAM UND SCHÜTZEN SIE SICH

Das schnelle Wachstum von Kryptowerten und ihre besonderen Merkmale – wie globale Zugänglichkeit, Geschwindigkeit, Anonymität und häufig Unumkehrbarkeit von Transaktionen – machen Sie zu einem Hauptziel für Cyberkriminelle. Betrüger und Abzocker nutzen ausgeklügelte Taktiken, um Sie zu täuschen, wie z. B. „Schneeballsysteme“, gefälschte Anlagemöglichkeiten, kostenlose Angebote in den sozialen Medien und falsche Nachrichten. Sie verwenden viele Methoden wie z.B. Liebesfallen, Anlagebetrug oder vorgetäuschte Adressen, um an Ihr Geld zu kommen. Sie kontaktieren Sie oft über soziale Medien, Messaging-Apps, E-Mails und unerwartete Anrufe, die echt klingen. Sie können Risiken wie finanzielle Verluste, Identitätsdiebstahl und emotionale Belastungen ausgesetzt sein.

Seien Sie vorsichtig und folgen Sie diesen wichtigen Tipps, um sicher zu bleiben:

**Bleiben Sie wachsam bei möglichem Krypto-Betrügereien und Abzocken:**
Weitere Informationen über die verschiedenen Arten von Betrug und Abzocke erfahren Sie hier (Seiten 5, 6, 7 und 8).

**Erkennen Sie Warnzeichen:**
lernen Sie, verdächtige Verhaltensweisen, Nachrichten oder Angebote zu erkennen (Seite 2).

**Schützen Sie sich und Ihr Vermögen:**
schützen Sie Ihre personenbezogenen Daten (Seite 3).

**Wissen, was zu tun ist, wenn Sie Opfer von Betrug oder Betrug werden**
(Seite 4).

# Warnzeichen

Ein Versprechen, das zu gut scheint, um wahr zu sein

Ein unaufgefordertes Angebot

Eine garantiert schnelle und hohe Rendite

Handlungsdrang (z. B. zeitlich begrenzte Angebote, die Sie unter Druck setzen, sofort zu handeln)

Eine Zahlungsaufforderung über nicht rückverfolgbare Wege (z. B. Kryptos, Geschenkkarten, Überweisungen oder Prepaid-Debitkarten)

Eine Einladung, auf einen Link zu klicken, einen QR-Code zu scannen oder eine App herunterzuladen

Eine Anfrage, private Schlüssel und sog. Seed-Phrasen zu senden oder zu teilen (Liste der Wörter, um auf Ihre Krypto-Wallet zuzugreifen und sie wiederherzustellen)


Verdächtige oder falsche URL

Logo mit leichten Verzerrungen, eine Website, die das Aussehen einer echten Unternehmenswebsite kopiert oder professionell aussieht, aber keine überprüfbaren Kontaktdaten, Unternehmens-registrierungsinformationen, Erfolgsbilanzen oder überprüfbare Präsenz aufweist

Unbekannte Austauschplattform

Ein verdächtiger Anhang, insbesondere .exe, .scr, .zip oder makroaktivierte Office-Datei (.docm, .xlsm).

# Schritte, um sich zu schützen:

## 1 Bleiben Sie ruhig und denken Sie nach, bevor Sie handeln:

Lassen Sie sich nicht unter Druck setzen, um zu investieren, Informationen auszutauschen oder auf Links zu klicken- Betrüger schaffen absichtlich ein Gefühl der Dringlichkeit. Bei Zweifeln, selbst wenn sie nur geringfügig sind, handeln oder investieren Sie nicht und überprüfen Sie die Quelle sorgfältig.

## 2 Überprüfen Sie die Quelle sorgfältig:

- Überprüfen sie immer, woher die Nachrichten, Anrufe, E-Mails und Links kommen, auch wenn sie offiziell aussehen, oder von einem Freund oder ihrer Familie oder sogar einer öffentlichen Figur zu kommen scheinen. Suchen Sie nach Rechtschreibfehlern, seltsamen URLs oder fehlenden Sicherheitsindikatoren, z. B. überprüfen Sie, ob der Website-Link ein „s“ in „HTTPS“ enthält, um sicherzustellen, dass die Website sicher ist, und suchen Sie nach hinzugefügten oder fehlenden Buchstaben im Firmennamen.
- Öffnen Sie keine Links aus unerwünschten Nachrichten, installieren Sie nur offizielle Anwendungen über vertrauenswürdige App-Stores und scannen Sie keine unbekannten QR-Codes.
- Auch wenn ein Angebot offiziell aussieht, überprüfen Sie es immer mit der Website des Unternehmens oder überprüfen Sie, ob das Social-Media-Konto verifiziert ist (z. B. mit offiziellen Häkchen).
- Verwenden Sie verifizierte Kontaktdaten, um das Unternehmen oder die Person direkt zu erreichen, und verlassen Sie sich niemals auf die Kontaktinformationen der mutmaßlichen Betrüger (z. B. unabhängig nach dem Firmennamen suchen, verifizierte Geschäftsverzeichnisse verwenden). Betrüger können behaupten, zugelassen zu sein oder ahmen die Website eines zugelassenen Unternehmens nach. Sie können überprüfen, ob der Kryptoanbieter in der EU zugelassen ist, indem Sie das ESMA-Register ( ) überprüfen. Sie können auch auf der Website der CSSF ( ) nachsehen, ob Warnungen oder schwarze Listen ausgegeben wurden oder die I-SCAN-Liste der IOSCO (iosco.org/i-scan/).

## 3 Teilen Sie niemals Passwörter, private Schlüssel oder Seed-Phrasen:

Jeder, der Zugriff auf diese Daten hat, kann die Kontrolle über Ihre Vermögenswerte übernehmen. Legitime Unternehmen werden niemals nach Ihren Passwörtern oder Sicherheitscodes per E-Mail, Text oder Telefon fragen.

## 4 Halten Sie Geräte und private Schlüssel sicher:

Verwenden Sie starke und eindeutige Passwörter für jedes Ihrer Krypto-Konten, halten Sie Ihr Passwort geheim und vermeiden Sie die Wiederverwendung derselben Anmeldeinformationen auf verschiedenen Plattformen. Aktivieren Sie nach Möglichkeit die Multi-Faktor-Authentifizierung. Einige Passwörter-Tipps finden Sie unter . Aktivieren Sie Ihre Software und Ihren Antivirenschutz und halten Sie diese auf dem neuesten Stand.

## 5 Seien Sie vorsichtig mit unerwarteten Anlageangeboten:

Seien Sie vorsichtig bei Investitionen, die große Renditen versprechen. Wenn es zu gut klingt, um wahr zu sein, ist es wahrscheinlich auch nicht wahr.

## 6 Denken Sie nach, bevor Sie Informationen in sozialen Medien teilen:

Chat-Gruppen, Foren, Social-Media-Beiträge und Fotos können wertvolle Wissensquellen für Betrüger sein. Wenn Sie zu viel über sich selbst oder Ihre Investitionen preisgeben, können Sie ein einfaches Ziel sein.

# Was tun, wenn Sie Opfer von Betrug oder Abzocke geworden sind?

## Stoppen Sie sofort Transaktionen,

Um weitere Überweisungen auf verdächtige Konten zu blockieren und zusätzliche Verluste zu vermeiden. Stoppen Sie jeden Kontakt mit den Betrügern – ignorieren Sie ihre Anrufe und E-Mails und blockieren Sie den Absender.

## Ändern Sie Ihre Passwörter auf allen Ihren Geräten und Apps/Websites.

Betrüger kaufen gestohlene Passwörter online und probieren sie auf mehreren Konten aus. Nur ein Passwort zu ändern, reicht nicht aus. Stellen Sie sicher, dass sie alle geändert werden, damit Betrüger sie nicht wiederverwenden können.

## Trennen und Entziehen des Zugangs:

Verzichten Sie auf verdächtige Berechtigungen in Ihrer digitalen Vereinbarung, die automatisch auf der Blockchain ausgeführt werden (Smart Contract), um Betrüger daran zu hindern, Ihre Token ohne Ihre Zustimmung auszugeben. Viele Wallets und Blockchain-Explorer bieten Tools, mit denen Sie sehen können, welche Smart Contracts derzeit Zugriff auf Ihre Token haben. Um dies zu tun, können Sie:

- einen vertrauenswürdigen „Genehmigungsprüfer“ verwenden, mit dem überprüft wird, ob ein Benutzer oder eine Blockchain-Adresse zur Ausführung eines Vorgangs berechtigt ist.
- die Liste der Genehmigungen zu überprüfen und
- die Schaltfläche „Widerrufen“ direkt von der Plattform aus verwenden.

## Verschieben Sie Ihr Geld:

Wenn Ihre Wallet kompromittiert ist, übertragen Sie sofort Ihre verbleibenden Vermögenswerte in eine neue, sichere Wallet.

## Wenden Sie sich an Ihren Kryptoanbieter:

Informieren Sie Ihren Krypto-Anbieter so schnell wie möglich über offizielle Kontaktkanäle, um mögliche Optionen zu erkunden. Selbst wenn es in den meisten Fällen nicht möglich sein sollte, die Blockchain-Transaktion rückgängig zu machen, könnte der Anbieter das Konto des Betrügers einfrieren (wenn es sich auf seiner Plattform befindet) und die Wallet-Adresse auf die schwarze Liste setzen.

## Meldung und Warnmeldung:

Melden Sie den Vorfall der Polizei sowie gegebenenfalls der CSSF (https://www.cssf.lu/de/) und informieren Sie Ihr Netzwerk (z. B. Freunde und Familie), um das Bewusstsein zu schärfen. Diese Maßnahmen sind der beste Weg, um sich selbst und andere zu schützen.

## Vorsicht vor Betrug im Rahmen des „Recovery rooms“:

Der Betrüger kann Sie als Opfer eines früheren Betrugs kontaktieren, indem er behauptet, eine Behörde zu sein (z. B. Polizei, Steuer- oder Finanzbehörde usw.) und anbietet, Ihr verlorenes Geld gegen eine Gebühr zurückzufordern. Dies ist oft ein weiterer Versuch, Sie zu betrügen. Denken Sie daran: Einmal betrogen zu werden, hindert Sie nicht daran, erneut betrogen zu werden.

Siehe Warnung der Gemeinsamen Europäischen Aufsichtsbehörden, um mehr über die Risiken im Zusammenhang mit Kryptowerten zu erfahren (↖) und das Informationsblatt „Kryptowerte erklärt: Was MiCA für Sie als Verbraucher bedeutet“ (↖).

Europäische Bankenaufsichtsbehörde, Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, Europäische Wertpapier- und Marktaufsichtsbehörde, 2025

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2025



PDF ISBN 978-92-9407-275-7 doi:10.2853/5311813 DZ-01-25-163-DE-N

# Arten von Krypto-Betrügereien

## „Pump-and-dump"-Regelung oder „Rug pull"

Sie sehen eine Werbung (Anzeige) in den sozialen Medien oder auf einer Website, die eine zeitlich begrenzte Investitionsmöglichkeit in Krypto anpreist und empfiehlt, in ein neues Krypto-Token oder -Projekt zu investieren. Nachdem Sie Ihr Interesse bekundet haben, werden Sie kontaktiert und zu einer Kryptobörse oder einem Messaging-Kanal (z.B. Telegram, Viber oder WhatsApp) weitergeleitet. Ein scheinbar glaubwürdiger Kontakt verspricht schnelle Gewinne oder hohe Renditen, wenn Sie schnell investieren. Sie werden ermutigt, einen kleinen Betrag zu investieren und dann unter Druck gesetzt, mehr zu investieren.

***Was passieren könnte:***

*Sie entdecken, dass das investierte Token wertlos ist und der Kontakt, mit dem Sie in Kontakt standen, nicht mehr reagiert. Wenn Sie versuchen, Ihr Geld abzuheben, existiert die Website nicht mehr und das Unternehmen ist nicht erreichbar. Betrüger überhöhten oder übertrieben künstlich eine Krypto mit niedrigem Wert, um ihren Wert zu erhöhen („Pump"), verkauften dann ihre Vermögenswerte („Dump"), wodurch der Wert abstürzte und die Anleger Verluste erlitten. Alternativ könnten sie das Projekt schließen und mit den Mitteln verschwinden („Rug pull").*

## Identitätsbetrug

Nachdem Sie eine Frage auf einer Social-Media-Plattform oder einer Website zu einem Krypto-Wallet-Problem gestellt haben, erhalten Sie eine unerwartete Direktnachricht (DM) oder eine E-Mail von jemandem, der vorgibt, ein vertrauenswürdiger Kontakt zu sein (z. B. ein Krypto-Austausch, Wallet-Anbieter, IT-Support oder sogar ein Freund). Die Person fragt nach Ihren Seed-Phrasen (d.h. nach einer Wortfolge, die als zentrale Sicherung für den Zugriff auf Ihre digitale Wallet dient), Passwörtern oder privaten Schlüsseln (ein automatisch generierter kryptografischer Code, der das Eigentum an digitalen Assets beweist).

***Was passieren könnte:***

*Sobald sie ihre Seed-Phrase, Passwörter oder privaten Schlüssel teilen, verwendet der Betrüger sie, um ihre Kryptowährung oder andere Gelder zu stehlen. Denken Sie daran, dass der Verlust privater Schlüssel zu einem dauerhaften und irreversiblen Verlust des Zugangs und Eigentums an Ihren Kryptowerten führt. Im Gegensatz zu Banktransaktionen ist bei Krypto-Überweisungen eine Wiederherstellung fast unmöglich, sobald Ihr Geld weg ist.*

## Phishing

Sie erhalten eine unerwartete Nachricht per E-Mail, Telefon, Pop-up oder soziale Medien, die behauptet, von einem bekannten Kryptowertenanbieter zu sein. Die Nachricht lädt Sie ein, sich anzumelden oder eine neue App herunterzuladen. Möglicherweise erhalten Sie auch eine E-Mail von Ihrer Krypto-Wallet-App, in der Sie aufgefordert werden, ein Sicherheitsproblem zu beheben, indem Sie auf einen Link klicken, der von einer inoffiziellen Quelle bereitgestellt wird, oder indem Sie die App aktualisieren.

***Was passieren könnte:***

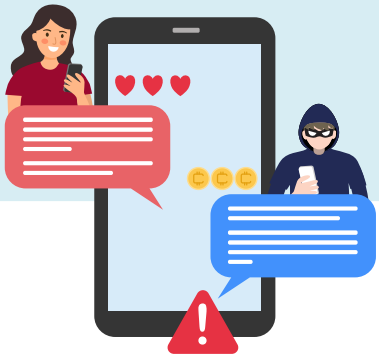
*Indem Sie auf den Link klicken, die App herunterladen oder einen QR-Code scannen, installieren Sie eine Malware, die es dem Betrüger ermöglicht, auf die Informationen zuzugreifen und sie zu verwenden, um Ihre Kryptowerte oder Ihr Geld zu stehlen.*

## Werbegeschenk-Betrug

Sie stoßen auf eine Ankündigung in den sozialen Medien, in der behauptet wird, dass Unternehmen nach einer kleinen Kryptoinvestition Kryptowerte verschenken. Dazu gehört ein Video oder ein Beitrag mit Fotos eines Prominenten oder einer Marke – in der Regel gefälscht oder ohne Genehmigung erhalten –, in dem versprochen wird, „Ihre Krypto zu verdoppeln“, wenn Sie zuerst Geld senden. Das Logo, das Layout, die Testimonials und die verwendete Sprache sehen professionell und offiziell aus, ebenso wie die Website, auf die Sie weitergeleitet werden.

***Was passieren könnte:***

*Nach dem Senden Ihrer Krypto erhalten Sie nichts im Gegenzug, und Sie haben das gesendete Geld verloren. Das Werbegeschenk war gefälscht, und der Post- oder Livestream, der sich als Prominente oder Unternehmen ausgab, wurde entwickelt, um Sie zu täuschen.*



## Liebesbetrug

Sie wurden in sozialen Medien, Dating-Apps oder Telefon/Nachricht von jemandem kontaktiert, den sie im wirklichen Leben nicht getroffen haben. Diese Person kann häufige, persönliche und romantische Gespräche führen und vertrauen mit gefälschten Profilen aufbauen. Allmählich lenken sie das Gespräch in Richtung finanzieller Möglichkeiten, beanspruchen riesige Gewinne aus Krypto-Investitionen und ermutigen Sie, mit Versprechen hoher Renditen und geringem Risiko zu investieren. Sie führen Sie durch die Einrichtung eines Kontos und eine kleine erste Einzahlung, damit das System legitim erscheint.

Betrüger erstellen gefälschte Online-Profile und verwenden gestohlene oder mit künstlicher Intelligenz-generierte Bilder, um sich Ihnen zu nähern.

***Was passieren könnte:***

*Der Betrüger nimmt von Ihnen so viel Geld wie möglich, schneidet dann die gesamte Kommunikation ab und verschwindet. Die betrügerische Investment-Website oder -App wird offline genommen, so dass Sie keinen Zugriff auf die angeblichen Investitionen haben. In einigen Fällen können Betrüger die während des Betrugs erhaltenen Informationen verwenden, um Ihre Freunde und Familie ins Visier zu nehmen und Identitätsdiebstahl zu begehen, der finanzielle oder rechtliche Konsequenzen für Sie haben kann (z. B. kann der Betrüger gestohlene Wallets in Ihrem Namen überprüfen und Sie könnten für Schulden oder Verbrechen verantwortlich gemacht werden, die unter Ihrem Namen begangen wurden, bis das Gegenteil bewiesen ist).*

## Schneeballsystem

Sie sind eingeladen, an einem Projekt teilzunehmen, das konstant hohe Renditen aus Krypto-Anlagen verspricht, die oft durch Erfahrungsberichte oder gefälschte Erfolgsgeschichten gestützt werden. Das Programm kann als Multi-Level-Marketing-Möglichkeit präsentiert werden, bei der Sie nicht nur durch Ihre eigene Investition, sondern auch durch die Rekrutierung anderer belohnt werden. Frühe Investoren scheinen Auszahlungen zu erhalten und ermutigen mehr Menschen, sich dem System anzuschließen und es zu fördern.

In Wirklichkeit wird kein echtes Geschäft oder Gewinn generiert. Stattdessen stammt das Geld ausschließlich aus dem Beitrag neuerer Investoren, der zur Auszahlung von Renditen an die Organisatoren und Erstteilnehmer des Systems verwendet wird.

***Was passieren könnte:***

*Sobald sich neue Investitionen verlangsamen, bricht das System zusammen, und Sie verlieren, wie die meisten Teilnehmer, Ihr Geld. Die Organisatoren verschwinden und lassen keine Möglichkeit, Gelder zurückzufordern. Die mehrstufige Struktur hilft dem Betrug, sich schnell zu verbreiten, da Opfer unwissentlich Anwerber werden.*


## Eine ähnliche Adresse, die Ihre Wallet kompromittiert

Nachdem Sie eine Kryptotransaktion durchgeführt haben, bemerken Sie eine neue Adresse, die in Ihrem Wallet-Verlauf angezeigt wird. Diese Adresse sieht ähnlich aus wie eine, mit der Sie zuvor interagiert haben. Betrüger können gefälschte Wallet-Adressen in Ihrem Transaktionsverlauf erscheinen lassen, indem sie eine winzige Menge Krypto von einer ähnlichen Adresse an Ihre Wallet senden. Sie speichern die gefälschte Adresse, die vom Betrüger erstellt wurde, in den jüngsten Aktivitäten oder automatischen Vorschlägen Ihrer Wallet. Betrüger erstellen absichtlich ähnliche Adressen, indem sie nur wenige Zeichen ändern, oft in der Mitte der Adresse, um eine Erkennung zu vermeiden.

***Was passieren könnte:***

*Wenn Sie versuchen, Krypto zu senden und die falsche Adresse aus Ihrem Wallet-Verlauf zu kopieren, senden Sie unwissentlich Geld an die Wallet des Betrügers. Da Krypto-Transaktionen oft irreversibel sind, gehen Ihre Gelder in den meisten Fällen dauerhaft verloren. Dieser Betrug beruht auf visueller Täuschung und Benutzerfehlern und nutzt die Gewohnheit aus, Wallet-Adressen ohne genaue Überprüfung zu kopieren und einzufügen.*