CRYPTO-BETRUG

SEIEN SIE WACHSAM UND SCHÜTZEN SICH

Das schnelle Wachstum von Kryptowerten und ihre besonderen Merkmale – globale Zugänglichkeit, Geschwindigkeit, Anonymität und häufig Unumkehrbarkeit von Transaktionen – macht es Kriminellen besser möglich, Sie zu betrügen. Dafür nutzen sie ausgeklügelte Taktiken, um Sie zu täuschen, etwa „Schneeballsysteme“, gefälschte Anlagemöglichkeiten, kostenlose Angebote in den sozialen Medien und falsche Nachrichten. Sie nutzen unter anderem Liebes-Investmentbetrug oder täuschend ähnliche Adressen, um Ihre digitale Brieftasche (Wallet) zu manipulieren. Sie erreichen Sie oft über soziale Medien, E-Mails, unerwartete Anrufe und Messaging-Apps, die seriös gemacht sind. Sie können Risiken wie finanzielle Verluste, Identitätsdiebstahl und emotionale Belastungen ausgesetzt sein.

Seien Sie vorsichtig und beachten die folgenden Tipps, um sich zu schützen:

Seien Sie wachsam bei möglichen Krypto-Betrugsversuchen:
Erfahren Sie mehr über verschiedene Betrugsmaschen und speziell über Kryptobetrug (s. Seite 5, 6, 7 und 8).

Warnzeichen beachten:
Lesen Sie, wie Sie verdächtige Verhaltensweisen, Nachrichten oder Angebote *erkennen* (s. Seite 2).

Schützen Sie sich:
Sichern Sie Ihre personenbezogenen Daten (s. Seite 3).

Erfahren Sie, was zu tun ist, wenn Sie Opfer von Betrug werden
(s. Seite 4).

Warnzeichen

Ein Versprechen, das zu gut erscheint, um wahr zu sein.

Ein unaufgefordertes Angebot.

Eine garantiert schnelle und hohe Rendite.

Zeitdruck (etwa zeitlich begrenzte Angebote, die Sie unter Druck setzen, sofort zu handeln).

Eine Zahlungsaufforderung über nicht rückverfolgbare Methoden (wie Kryptos, Geschenkkarten).

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

Eine Anfrage, private Schlüssel und 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 echten Kontaktdaten, Unternehmens-registrierungsinformationen, Erfolgsbilanz oder überprüfbare Präsenz aufweist.

Unbekannte Austauschplattform.

Eine verdächtige Anlage, insbesondere .exe, .scr, .zip oder makroaktivierte Office-Datei (.docm, .xlsm).

So können Sie sich schützen

1 **Nehmen Sie sich Zeit und denken Sie nach, bevor Sie handeln:**

Beeilen Sie sich nicht, Geld zu senden, Informationen auszutauschen oder auf Links zu klicken – Betrügerinnen und Betrüger schaffen absichtlich ein Gefühl der Dringlichkeit. Wenn Sie auch nur geringfügige Zweifel haben, handeln Sie nicht; beenden den Anruf und überprüfen die Quelle oder Identität sorgfältig.

2 **Überprüfen Sie die Quelle sorgfältig:**

- Überprüfen sie immer, woher Nachrichten, Anrufe, E-Mails und Links kommen – auch wenn sie scheinbar seriös aussehen und von einer Freundin bzw. einem Freund, ihrer Familie oder sogar einer berühmten Person zu kommen scheinen. Prüfen Sie Nachrichten auf Rechtschreibfehler, seltsame URLs oder fehlende Sicherheitsindikatoren (beispielweise ob der Website-Link ein „s“ in „HTTPS“ enthält, um sicherzustellen, dass die Website sicher ist, und nach hinzugefügten oder fehlenden Buchstaben im Firmennamen der URL).
- 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 immer die Website des Unternehmens oder schauen Sie, ob das Social-Media-Konto verifiziert ist (etwa mit offiziellen Häkchen).
- Verwenden Sie verifizierte Kontaktdaten, um das Unternehmen oder die Person direkt zu erreichen und verlassen Sie sich nie auf die Kontaktinformationen der oder des mutmaßlichen Kriminellen (etwa unabhängige Suche nach dem Firmennamen, Verwendung verifizierter Geschäftsverzeichnisse). Betrügerinnen und Betrüger können behaupten, autorisiert zu sein oder die Website eines autorisierten Unternehmens nachahmen. Sie können überprüfen, ob der Kryptoanbieter in der EU zugelassen ist, indem Sie das ESMA-Register (↖) ansehen. Sie können auch auf der Website Ihrer nationalen Finanzaufsichtsbehörde (http://www.bafin.de/) nachsehen, ob Warnungen oder schwarze Listen veröffentlicht wurden oder auf der I-SCAN-Liste der IOSCO (iosco.org/i-scan/) nachschauen.

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

Alle, die Zugriff auf diese Informationen haben, können die Kontrolle über Ihre Vermögenswerte übernehmen. Seriöse Unternehmen fragen nie nach Ihren Passwörtern oder Sicherheitscodes per E-Mail, SMS oder Telefon.

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 verwenden Sie dieselben Anmeldeinformationen nicht mehrfach auf verschiedenen Plattformen. Aktivieren Sie auch, wenn möglich, die Multi-Faktor-Authentifizierung. In einem Beitrag des BSI finden Sie Tipps zu Passwörtern (↖). Halten Sie Ihre Software und Ihren Antivirenschutz immer auf dem neuesten Stand und aktiviert.

5 **Seien Sie vorsichtig bei unerwarteten Anlageangeboten:**

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

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

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

Was tun, wenn Sie Opfer von Betrug geworden sind?

Brechen Sie Transaktionen sofort ab,

Um weitere Überweisungen auf verdächtige Konten zu blockieren und zusätzliche Verluste zu vermeiden. Vermeiden Sie jeden Kontakt mit den Betrügerinnen und Betrügern, ignorieren Sie deren Anrufe und E-Mails und blockieren den Absender.

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

Kriminelle kaufen durchgesickerte Passwörter online und probieren sie auf mehreren Konten aus. Nur ein Passwort zu ändern, reicht nicht aus. Ändern Sie alles Passwörter, damit Betrügerinnen und 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). So hindern Sie Betrügerinnen und Betrüger, Ihren Krytpowert ohne Ihre Zustimmung auszugeben. Viele Wallets und Blockchain-Explorer bieten Tools, mit denen Sie sehen können, welche Smart Contracts derzeit Zugriff auf Ihren Kryptowert haben. Um dies zu tun, können Sie:

- einen vertrauenswürdigen „Genehmigungsprüfer“ verwenden. Damit wird geprüft, ob eine Nutzerin bzw. ein Nutzer berechtigt ist, eine Blockchain-Adresse auszuführen,
- die Liste der Genehmigungen überprüfen,
- 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 der Kriminellen 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 oder Ihrer nationalen Finanzaufsichtsbehörde und informieren Sie Ihre Bekannten (wie Freunde und Familie), um das Bewusstsein zu schärfen. Diese Maßnahmen können Ihnen helfen, sich selbst und andere zu schützen.

Vorsicht vor Rückgewinnungsbetrug:

Betrügerinnen und Betrüger nutzen ihr Wissen, um Sie bei einem Betrug und der vermeintlichen Rückgewinnung des verlorenen Geldes zu unterstützen. Dafür geben sie vor, eine Behörde zu sein (etwas Polizei, Steuer- oder Finanzbehörde) und bieten Ihnen an, 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.

Schauen Sie sich die Warnung der Gemeinsamen Europäischen Aufsichtsbehörden, um mehr über die Risiken im Zusammenhang mit Kryptowerten zu erfahren (). und das Factsheet „Crypto-assets explained: Was MiCA für Sie als Verbraucher bedeutet“ (Informationsblatt Kryptowerte: Was bedeutet MICA für Sie als Verbraucherin oder Verbraucher?) an.

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-Betrügern

„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 anbietet und empfiehlt, in ein neuen Kryptowert zu investieren. Nachdem Sie Ihr Interesse bekundet haben, werden Sie kontaktiert und zu einer Kryptobörse oder einem Messaging-Kanal (wie 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 könnte passieren:

Sie entdecken, dass der Kryptowert wertlos ist und der Kontakt, mit dem Sie in Verbindung standen, nicht mehr reagiert. Wenn Sie versuchen, Ihr Geld abzuheben, existiert die Website nicht mehr und das Unternehmen ist nicht erreichbar. Betrügerinnen und Betrüger erhöhen (teilweise übertrieben) den Wert eines Kryptowertes, der zuvor einen niedrigeren Wert hatte („Pump"). Anschließend verkaufen sie ihre eigenen Vermögenswerte („Dump"), wodurch der Wert abstürzt und die anderen Anlegerinnen und Anleger Verluste erleiden. Alternativ könnten sie das Projekt schließen und mit den Mitteln verschwinden („rug pull").

Identitätsbetrug

Sie haben eine Frage auf einer Social-Media-Plattform oder einer Website zu einem Krypto-Wallet-Problem gestellt. Anschließend erhalten Sie eine unerwartete Direktnachricht (DM) oder eine E-Mail von jemandem, der vorgibt, ein vertrauenswürdiger Kontakt zu sein (zum Beispiel ein Krypto-Austausch, Wallet-Anbieter, IT-Support oder sogar ein Freund). Die Person fragt nach Ihren Seed-Phrasen (also nach einer Wortfolge, die als zentrale Sicherung für den Zugriff auf Ihre digitale Brieftasche 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 die Betrügerin oder der Betrüger sie, um Ihre Kryptowährung oder andere Gelder zu stehlen. Denken Sie daran: der Verlust privater Schlüssel führt zu einem dauerhaften und irreversiblen Verlust des Zugangs und Eigentums an Ihren Kryptowerten. Im Gegensatz zu Banktransaktionen ist bei Krypto-Überweisungen eine Wiederherstellung fast unmöglich, sobald Ihr Geld weg ist.

Phishing

Sie erhalten per E-Mail, Telefon, Pop-up oder Social Media eine unerwartete Nachricht, die anscheinend von einem bekannten Krypto-Asset-Anbieter stammt. Sie werden eingeladen, sich anzumelden oder eine neue App herunterzuladen. Möglicherweise erhalten Sie auch eine E-Mail von Ihrer Krypto-Wallet-App. Darin werden Sie aufgefordert, 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:

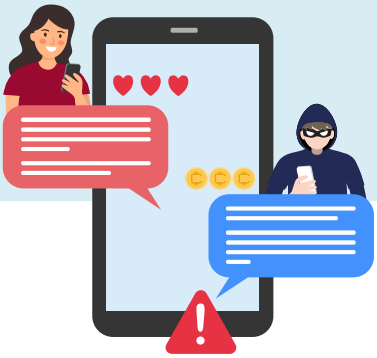
Indem Sie auf den Link klicken, die App herunterladen oder einen QR-Code scannen, installieren Sie eine Malware. Sie erlaubt es den Kriminellen, auf Informationen zuzugreifen und sie zu verwenden, um Ihre Kryptowerte oder Ihr Geld zu stehlen.

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 einer berühmten Person oder Marke – in der Regel gefälscht oder ohne Genehmigung erhalten. Es wird versprochen, Ihre Kryptowerte zu verdoppeln, wenn Sie zuerst Geld senden. Das Logo, das Layout, die Empfehlungen und die verwendete Sprache sehen professionell und offiziell aus, ebenso wie die Website, auf die Sie weitergeleitet werden.

Was passieren könnte:

Nach Sie Ihre Kryptowerte versendet haben, erhalten Sie nichts im Gegenzug und Sie haben das gesendete Geld verloren. Das Werbegeschenk war gefälscht und der Post oder Livestream, der sich berühmten Person oder Unternehmen ausgab, wurde entwickelt, um Sie zu täuschen.



Liebesbetrug

Sie werden in sozialen Medien, Dating-Apps oder per SMS von jemandem kontaktiert, den sie im wirklichen Leben noch nicht getroffen haben. Diese Person führt häufige, persönliche und romantische Gespräche mir Ihnen und baut Vertrauen mit gefälschten Profilen auf. Im Laufe der Zeit verschiebt sich das Gespräch in Richtung finanzielle Möglichkeiten wie Krypto-Investitionen und dem Versprechen von hohen Renditen und geringem Risiko. Die Person bittet Sie, Geld auf ein Konto zu überweisen oder richtet mit Ihnen ein Konto ein. Sie werden zu einer kleinen Ersteinzahlung geführt, um das System zu legitimieren.

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

Was passieren könnte:

Die Betrügerin bzw. der Betrüger zieht so viel Geld wie möglich ab, stellt die gesamte Kommunikation mit Ihnen ein und verschwindet. Die betrügerische Investment-Website oder -App wird offline genommen, so dass Sie nicht auf die angeblichen Investitionen zugreifen können. Zusätzlich zu finanziellen Verlusten können die von Ihnen weitergegebenen persönlichen Daten verwendet werden, um Ihre Freundinnen, Freunde und Familie zu kontaktieren oder für Identitätsdiebstahl, der finanzielle oder rechtliche Konsequenzen für Sie haben kann. So könnte ein Betrüger Einkäufe tätigen oder Kredite in Ihrem Namen aufnehmen. Sie könnten auch 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 und die oft durch Erfahrungsberichte oder gefälschte Erfolgsgeschichten gestützt werden. Das Programm kann als Multi-Level-Marketing-Möglichkeit präsentiert werden. Bei solchen werden Sie nicht nur durch Ihre eigene Investition, sondern auch durch die Rekrutierung anderer belohnt. Frühe Investorinnen und Investoren scheinen Auszahlungen zu erhalten und ermutigen weitere Menschen, sich dem System anzuschließen und es zu fördern.

In Wirklichkeit wird kein echtes Geschäft oder ein Gewinn generiert. Stattdessen stammt das Geld ausschließlich aus dem Beitrag neuerer Investorinnen und Investoren, den die Organisatoren zur Auszahlung in die eigene Tasche sowie an Erstteilnehmerinnen und Erstteilnehmer verwenden.

Was passieren könnte:

Sobald sich neue Investitionen verlangsamen, bricht das System zusammen, und Sie und die meisten anderen verlieren Geld. Die Organisatoren verschwinden und lassen keine Möglichkeit, Gelder zurückzufordern. Die mehrstufige Struktur hilft dem Betrugssystem, sich schnell zu verbreiten, da Opfer die Idee unwissentlich fördern.

Täuschend ähnliche Adressen in der Wallet

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. Betrügerinnen und Betrüger können gefälschte Wallet-Adressen in Ihrem Transaktionsverlauf erscheinen lassen. Dafür senden sie eine winzige Krypto-Menge von einer ähnlichen Adresse an Ihre Wallet. Sie speichern die gefälschte Adresse in den jüngsten Aktivitäten oder automatischen Vorschlägen Ihrer digitalen Brieftasche. Kriminelle 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, Kryptowerte zu senden und die falsche Adresse aus Ihrem Wallet-Verlauf zu kopieren, senden Sie unwissentlich Geld an die Wallet der Betrügerin oder des Betrügers. Da Krypto-Transaktionen oft irreversibel sind, gehen Ihre Gelder meist dauerhaft verloren. Dieser Betrug beruht auf visueller Täuschung und Benutzerfehlern und nutzt die Gewohnheit aus, Wallet-Adressen ohne genaue Inspektion zu kopieren und einzufügen.