So schützen Sie sich vor den

Krypto-Betrügern!

INVESTOR VERLAG

Live-Konferenz im Internet zum Start des Projekts FaktorX-Trading am Samstag, den 11. Oktober 2025, ab 11:00 Uhr – JETZT TEILNAHME SICHERN!

Projekt FaktorX-Trading

- **FaktorX: Sie können 57-mal mehr Gewinn machen als es mit DAX-Aktien möglich ist.**
- **FaktorX: Wenn andere mit Aktien 320% Gewinn machen, können Sie gigantische +18.338% Gewinn erzielen. Im gleichen Zeitraum.**
- **FaktorX: Sie können Ihr Kapital bis zu 31-mal pro Jahr verdoppeln.**

Ihr Ziel: Bis zu 1.523.000 € mit den ersten 14 FaktorX-Trades

FaktorX-Trading ist das erste Projekt, bei dem Anleger ihr Kapital in einem Tempo und mit einer Wucht vervielfachen können, wie es bislang unmöglich schien. Und das in einer Börsensituation, wie wir sie jetzt 2025 und 2026 erleben.

Das „X" steht für die Multiplikation Ihrer Gewinne – für die Verzehnfachung, ja sogar für die Vervielfachung um den Faktor 57.

Schon ab dem ersten Tag multiplizieren die Teilnehmer jeden Gewinn, der mit Aktien möglich ist. Sie vervielfachen jeden Gewinn um einen gigantischen Faktor X. Deshalb der Name FaktorX-Trading.

Mit Aktien sind über einen langen Zeitraum vielleicht 200 oder 300 Prozent möglich, wenn es gut läuft. Mit FaktorX-Trading sprechen wir über +18.338 % Gewinn im gleichen Zeitraum. Über Verdopplungen, die im Schnitt jede Woche oder jede zweite Woche stattfinden können. Bis zu 31 Kapitalverdopplung in einem einzigen Jahr. Darum geht es beim Projekt FaktorX-Trading.

Teilnahme exklusiv für Sie GRATIS

Ihr erster eigener FaktorX-Trade startet sofort am Ende der Live-Übertragung. Sichern Sie sich hier Ihren Platz:

Dr. Gregor Bauer, einer der größten Trader und gleichzeitig einer der einflussreichsten Finanzexperten unserer Zeit, startet das Projekt rechtzeitig zur Jahresendrally 2025. Mit einer Trading-Strategie, die er für diese Börsensituation geschaffen hat. Mit dem Projekt FaktorX-Trading können Sie Gewinne erzielen, die für andere absolut unerreichbar sind.

NUR EIN TERMIN:
Samstag, 11. Oktober 2025
LIVE IM INTERNET
Uhrzeit: 11:00 Uhr
Teilnahme für Sie kostenlos

Jetzt kostenlos Teilnahme sichern! Hier klicken

INHALTSVERZEICHNIS

Lieber Leser,

die Digitalisierung schreitet in unserer Gesellschaft mit immer größeren Schritten voran. Gleichzeitig reißt die digitale Vernetzung von immer mehr Lebensbereichen eine immer größer werdende Lücke in Ihre Privatsphäre. Kaum eine Woche vergeht, ohne dass ein neuer Datenskandal oder eine neue Betrugsmethode offenbart wird. Im Zeitalter der (bald) totalen Digitalisierung sind Ihre persönlichen Daten längst zu einem Handelsgut und somit zu einer wertvollen Währung geworden. Für Sie persönlich, für Staaten, Unternehmen, aber auch für Kriminelle. Daten sind Goldminen, die auch Begehrlichkeiten von Kriminellen und Online-Betrügern wecken.

Neben meinen vielschichtigen Empfehlungen veröffentliche ich regelmäßig Warnungen vor dubiosen Anbietern und Investment-Systemen. Deshalb befasse ich mich auch fortlaufend und sehr intensiv mit schwarzen Schafen und unseriösen bzw. betrügerisch agierenden Anbietern. Darunter auch Provisions-Vermittlungssysteme auf Basis von Multi Level Marketing (MLM) und deren dubiose Vermittler.

Markus Miller
Chefanalyst KRYPTO-X

Angst und Gier sind die besten Verkäufer – aber schlechte Ratgeber

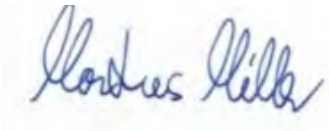
Die zunehmende Digitalisierung unseres täglichen Lebens hat auch im Bereich der Kapitalanlagen dafür gesorgt, dass viele dubiose Online-Investmentsysteme auf den Markt gekommen sind. Geworben wird hier mit blumigen Geschichten, verbunden mit der Aussicht auf den Schutz von Geld und Kapital (Angst) oder sehr hohe Gewinnmöglichkeiten (Gier) in Kombination mit einer ganz einfachen Handhabung. Dabei stellt sich immer wieder heraus, dass Emotionen wie Angst und Gier stets hervorragende Verkäufer sind, aber meist sehr schlechte Ratgeber.

Nach meiner Erfahrung wirken diese dubiosen Methoden auf viele Bürger sehr anziehend, speziell in Zeiten politischer und wirtschaftlicher Unsicherheiten. Mein grundsätzlicher Tipp: Angebote, die Sie über provisionsgetriebene Vermittler, Anzeigen im Internet, unaufgeforderte Anrufe, E-Mails und Briefe erhalten, müssen Sie immer doppelt und dreifach prüfen, um nicht auf Betrüger hereinzufallen. Anleger, die das nicht verinnerlicht haben, schlagen bei solchen Angeboten leider häufig sehr schnell zu und überweisen leichtfertig Geld.

Deswegen ist es nicht verwunderlich, dass ich fortlaufend eine Vielzahl an Zuschriften von Anlegern erhalte, die auf dubiose Investmentsysteme und Vermittler hereingefallen sind und jetzt vor einem Scherbenhaufen stehen.

Die Einblicke, die ich hier erhalte, sind teils bestürzend, aber immer auch wichtig für meine Recherchen und Empfehlungen. Gemeinsam mit meinem stetig wachsenden Experten-Netzwerk kann ich vielen Betroffenen helfen und viele andere Leser davor schützen, in dieselben Fallen zu tappen. Prophylaxe durch Wissensbildung ist dabei das wirkungsvollste Schutzkonzept.

Mit den besten Grüßen



Markus Miller

PS: Im Fahrwasser der boomenden Digitalisierung sind in den letzten Jahren speziell die Online-Betrugsfälle im Zusammenhang mit Kryptowährungen massiv angestiegen. Mit diesem Report gebe ich Ihnen eine Gebrauchsanleitung an die Hand, wie Sie sich vor Neppern, Schleppern und Bauernfängern aus der Digital- und Kryptowelt schützen können.

Ganze 1,1 Mio. € mit dieser neuen Digitalwährung: Markus Miller verrät, wie Sie jetzt ein schnelles Vermögen mit dem >> Millionärs-Coin<< machen können

stock.adobe.com – freshidea

HIER Namen erfahren>>>

Lieber Leser,

gerade macht ein unfassbar spektakulärer, neuer Krypto-Coin von sich Reden.

Superreiche wie Cathie Wood, Elon Musk, Mark Cuban und JP Morgan beginnen bereits, sich zu positionieren.

Immer mehr Experten sind sich absolut sicher: **Dieser Coin** hat das Potenzial, den gesamten 100 Billionen Euro schweren Finanzmarkt neu zu ordnen. Darunter der wohl bekannteste Krypto-Experte Deutschlands, Markus Miller, der selten so überzeugt von einer Digitalwährung war.

Der sogenannte >>Millionärs-Coin<<:

- Wird durch einen alles verändernden **Stichtag** revolutioniert– nach diesem Tag dürfte in der verstaubten Finanzindustrie ALLES anders werden
- kann Ihnen (wenn Sie früh investieren) bis zu +37.163 % Gewinn bringen – das wären 1,1 Mio. € Gewinnchance
- Hat das Potenzial, **20-x erfolgreicher als Bitcoin** zu werden – und dass, obwohl er bereits **für wenig Geld zu haben ist**

Das ist die Krypto-Chance des Jahrzehnts – wenn nicht sogar des Jahrhunderts!

Und Markus Miller möchte, dass nicht nur die Superreichen profitieren.

Auch Sie sollen sich Ihr wohlverdientes Stück vom Gewinnkuchen abschneiden.

Darum verrät er Ihnen heute den Namen des Millionärs-Coins.

Damit gehören Sie zu den ersten Privat-Anlegern, die überhaupt in **diesen neuen Mega-Coin** investieren können.

Spätestens am Stichtag selbst, dürfte der Kurs des Millionärs-Coins raketenartig senkrecht nach oben durchstarten.

+37.163 % Auftakt-Gewinn werden schon in Kürze erwartet. Langfristig hat der Coin das Potenzial, 20-x besser als Bitcoin zu werden.

Und wenn Sie sich jetzt positionieren, nehmen Sie diese gigantische Gewinnrallye von Anfang an mit.

Klicken Sie HIER für den Namen des Millionärs-Coins und bis zu 1,1 Millionen Euro Gewinnchance

*Jetzt heißt es schnell sein, bevor die breite Masse beginnt, zu investieren!

1. Eröffnen Sie niemals ein Konto mit Hilfe von Dritten!

Eine Fernwartungssoftware oder Remote-Software wie beispielsweise TeamViewer, GoToAssist, UltraVNC, TightVNC, NetSupport Manager, Netop Remote Control oder AnyDesk ermöglicht es, Computer oder Server aus der „Ferne zu steuern“. Dadurch lassen sich – durch vertrauenswürdige und kompetente Dritte – IT-Probleme lösen und Anwendungen installieren. Ebenso kann eine einfache und schnelle Hilfestellung bei Kunden oder Mitarbeitern geleistet werden, zur Behebung von Fehlern.

Die Grundlage für den Einsatz einer Fernwartungssoftware ist ein absolut uneingeschränktes, 100-prozentiges Vertrauensverhältnis zu dem jeweiligen Dritten, dem ein Anwender-Zugriff auf seinen Computer bzw. Server gewährt wird. Und genau hier liegt ein großes Problem, welches wiederholt zu einem Missbrauch und zu gravierenden Betrugs- und Schadensfällen führt im Zusammenhang mit dem Einsatz einer Fernwartungssoftware.

Unterstützung bei der Kontoeröffnung bei einer Kryptobörse durch unbekannte Dritte? Niemals!

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) warnt im Zusammenhang mit Kryptowährungen und der Kryptoverwahrung vor einer Kontoeröffnung mit Hilfe von Dritten. Wörtlich schreibt die BaFin hierzu auf ihrer Internetseite in der Rubrik „Verbraucherschutz“:

„Seien Sie vorsichtig, wenn Unbekannte Sie dabei unterstützen wollen, ein Konto bei einer Kryptobörse zu eröffnen. Dabei handelt es sich sehr wahrscheinlich um Betrug. Meist wollen diese Personen auf Ihre Rechner mit Fernwartungssoftware zugreifen. Das sollten Sie aber auf keinen Fall zulassen. Sobald diese Software auf dem Computer installiert ist, nutzen die Kriminellen diesen Zugriff, um Konten beziehungsweise E-Wallets in Ihrem Namen zu eröffnen und um damit unter anderen Kryptowährungen zu kaufen.“

Auch die BaFin selbst nutzt keine Fernwartungssoftware

Der BaFin ist bereits im Jahr 2021 auch ein erster Fall bekannt geworden, in dem ein unbekannter Täter einen Verbraucher angerufen hat, um diesem angeblich dabei zu helfen, in Bitcoins investiertes Geld „zurückzuholen“. Dabei habe der Täter vorgegeben, im Auftrag der BaFin zu handeln. Der Täter habe sich dann per Fernwartungssoftware auf den Computer seines Gesprächspartners aufgeschaltet und diesen dazu aufgefordert, eine Bankverbindung anzugeben.

Wichtig: Die BaFin beauftragt generell keine Dritten und wendet sich auch nicht von sich aus an einzelne Personen, um sie – beispielsweise zu Finanzprodukten – zu beraten oder um die Zahlung eines Geldbetrags auf ein bestimmtes Konto zu verlangen. Verbraucher sollten generell wachsam sein, wenn Dritte unter dem Namen der BaFin agieren.

Die deutsche Finanzmarktaufsicht empfiehlt allen, die ein entsprechendes Hilfsangebot erhalten, sich keinesfalls darauf einzulassen und Anzeige bei der Polizei oder Staatsanwaltschaft zu erstatten. Wer Zweifel hat, kann sich auch direkt an die Bundesanstalt für Finanzdienstleistungen (BaFin) wenden. Das Verbrauchertelefon ist kostenfrei unter der Telefonnummer 0800 2 100 500 zu erreichen.

Meine Empfehlung: Eröffnen Sie Konten für den Handel mit Kryptowährungen ausschließlich selbst und bei regulierten Anbietern wie **Bitpanda.com**, **Coinbase.com**, **Bitcoin.de** oder **Bisonapp.de**!

2. Fallen Sie nicht auf die Bitcoin-Betrugsmasche Hacking-Bluff herein

8com gehört zu den führenden Anbietern von Awareness-Leistungen (Bewusstseinsschärfung für Risiken und Schutzfunktionen) und Informationssicherheit in Europa. Das sogenannte Cyber Defense Center schützt die digitalen Infrastrukturen seiner Kunden effektiv vor Cyberangriffen. Vor Kurzem hat 8com GmbH & Co. KG eine sehr interessante Pressemitteilung veröffentlicht, mit Bezug zu einem aktuellen Betrugsversuch, bei dem wieder einmal Lösegeldzahlungen in Bitcoin gefordert werden: Hacker versuchen dabei, Betreiber von Webseiten mit einer neuen Betrugsmasche zu erpressen. Besonders dreist daran ist, dass sie eigentlich überhaupt kein Druckmittel gegen ihr Opfer in der Hand haben.

Die Drohung: „Your website, databases and emails has been hacked"

Webseitenbetreiber und Admins weltweit haben wiederholt E-Mails erhalten, in denen Kriminelle damit drohen, vermeintlich erbeutete Daten dazu zu nutzen, den Ruf des Opfers zu zerstören. Um das zu vermeiden, soll das Opfer 2.500 US-Dollar in Bitcoin zahlen. Die Drohung selbst erreicht die Opfer per E-Mail mit dem Betreff „Your website, databases and emails has been hacked". In der Nachricht selbst behaupten die Kriminellen, dass sie die Webseite des Opfers gehackt und die Daten inklusive des E-Mail-Kontos vollständig heruntergeladen haben. Als Beweis führen sie an, dass ihre E-Mail ja über den Server des Opfers verschickt worden sei.

Sollte das Opfer nicht innerhalb von 72 Stunden 2.500 US-Dollar in der Kryptowährung Bitcoin zahlen, würde man diese Daten dazu nutzen, systematisch den Ruf des Webseitenbetreibers zu zerstören.

Dazu würde man nicht nur die gestohlenen Daten veröffentlichen, sondern auch E-Mails an alle bekannten Kontakte schicken, um diese wissen zu lassen, dass der Webseitenbetreiber die Veröffentlichung der Daten zu verantworten habe. Außerdem würde man die Webseite auf jede Blacklist des Landes setzen. Aufhören würde man erst dann, wenn das Lösegeld auf einem von zwei Bitcoin-Wallets eingegangen wäre. Zu guter Letzt wird erneut betont, dass es sich bei dieser E-Mail keinesfalls um einen Scherz handle und ein Versuch zu verhandeln sinnlos sei.

Drohung und Bitcoin-Erpressung basieren auf einem Bluff!

Das „Problem“ an der Sache ist allerdings: Die Webseiten der Opfer wurden überhaupt nicht gehackt und die Kriminellen haben somit tatsächlich keinerlei Druckmittel in der Hand. Recherchen von BleepingComputer zufolge sind auf den beiden bekannten Bitcoin-Wallets trotzdem bereits Zahlungen eingegangen. Das bedeutet, dass zumindest einige der Angeschriebenen die Drohungen ernst genommen haben und nun 2.500 Dollar ärmer sind.

Urheber der Betrugsmasche ist eine Gruppe, die sich selbst Team Montesano nennt, weitere Informationen sind allerdings bislang nicht bekannt. Verbreitet werden die Erpresser-Mails über Phishing-Nachrichten, die scheinbar nach dem Gießkannenprinzip weltweit an alle möglichen Branchen verschickt werden, darunter Blogger, Regierungsbehörden und Unternehmen jeglicher Größe.

Meine Empfehlung: Der grundlegende Ratschlag des Bundeskriminalamtes BKA im Zusammenhang mit Cyberangriffen lautet: „Nicht mit Erpressern verhandeln“. Dazu gehört selbstverständlich auch, keine Zahlungen zu leisten. Erstatten Sie bei derartigen Vorfällen im Bedarfsfall eine Strafanzeige bei der Polizei. Ansonsten ignorieren Sie derartige Erpressungsversuche einfach und bezahlen Sie niemals!

3. Achtung vor Smishing

Wiederholt versenden Kriminelle viele Mails, WhatsApps oder SMS mit schädlichen Links. Beim Draufklicken wird Schadsoftware auf dem PC oder Handy installiert. Oder aber die Empfänger werden über den Link aufgefordert, persönliche Daten einzugeben, etwa Passwörter oder Kontodaten. Damit bereichern sich die Diebe.

Menschen fallen auf die Masche herein, da sich die Täter als vertrauenswürdige Absender ausgeben. Aktuell landen zum Beispiel SMS auf zahlreichen Handys, die angeblich vom Finanzministerium stammen und etwa eine Steuererstattung versprechen – natürlich nur durch Klick auf den beigefügten Link. Derartige Betrugsversuche nennen sich Smishing, zusammengesetzt aus „SMS“ und „Phishing“ = Datendiebstahl.

Unter dem Begriff Phishing, abgeleitet vom englischen „Fishing“ für „Angeln“, versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, an persönliche Daten eines Internet-Benutzers zu gelangen oder ihn zur Ausführung einer schädlichen Aktion zu bewegen, beispielsweise über Bankkonten, Konten bei Kryptobörsen oder Blockchain-Wallets.

Die wichtigsten Tipps der Polizei gegen Smishing:

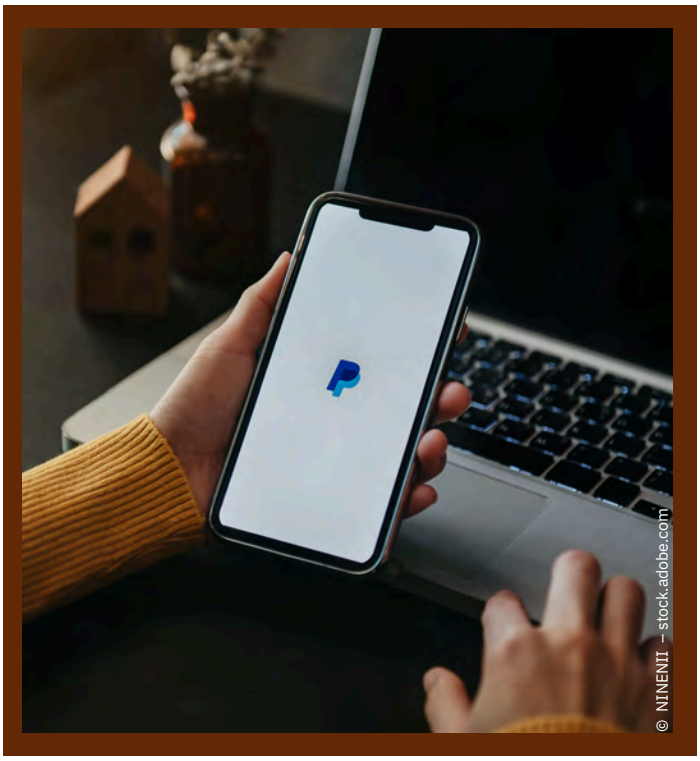
- Löschen Sie Nachrichten unbekannter Herkunft; sperren Sie die Absender. Klicken Sie keinesfalls deren Links an oder installieren Sie Apps. Laden Sie nur Apps aus bekannten Stores herunter.
- Um möglicher Abzocke vorzubeugen, lassen Sie sich bei Ihrem Mobilfunkanbieter eine Drittanbietersperre einrichten.
- Übermitteln Sie niemals online (über soziale Netzwerke, Smartphone usw.) persönliche Daten.

Was tun, wenn schon etwas passiert ist?

- Schalten Sie Ihr Handy in den Flugmodus, damit es keine SMS versenden und Befehle von außen empfangen kann.
- Sichern Sie in einem Backup Ihre Daten, Bilder und Videos.
- Stellen Sie dann Ihr Smartphone auf Werkseinstellungen zurück. So werden alle Apps und Daten gelöscht, die beim Handykauf noch nicht vorhanden waren.
- Ändern Sie alle Ihre Passwörter.
- Informieren Sie Ihren Mobilfunk-Betreiber über das Problem. Fragen Sie, ob schon Kosten entstanden sind. Informieren Sie Ihre nächstgelegene Polizeidienststelle.

4. Die Betrugsmethode Brandphishing am Beispiel PayPal

Zur Praxis von Hackern gehört mittlerweile auch der Missbrauch großer Markennamen. Um ihre Opfer in Phishing-Mails auf eine sichere Fährte zu locken, geben sie vor, Rechnungen oder Zahlungsaufforderungen von bekannten Konzernen zu stellen. Diese Methode wird als Brandphishing bezeichnet. Nun zeigt sich, dass der Zahlungsdienstleister PayPal nicht von dieser Taktik verschont blieb. Die Sicherheits-forscher von Avanan, die im letzten Jahr von Check Point übernommen wurden, haben beobachtet, dass Hacker den Treuhänder nutzen, um bösartige Rechnungen zu versenden und Zahlungen anzufordern.



Die Kriminellen senden die E-Mail sogar von der PayPal-Domäne aus und verwenden dafür ein kostenloses PayPal-Konto.

Der E-Mail-Text täuscht dabei bekannte Markennamen, im untenstehenden Beispiel den von Norton AntiVirus, vor. Technisch funktioniert der Trick, da PayPal in den meisten E-Mail-Prüfsystemen als legitime Website aufgeführt ist und die E-Mail ungefiltert weitergeleitet wird.

Phishing als Vorstufe zu einem gefährlichen Identitätsmissbrauch

Diese Angriffsweise ist doppelt gefährlich, weil der Nutzer erstens die angegebene Telefonnummer anrufen soll, um ihn im zweiten Schritt zu verleiten, die Rechnung zu bezahlen. Die Täter haben dann Kontaktdaten ihrer Opfer herausgefunden, die für einen zukünftigen Identitätsmissbrauch verwendet werden können. Das kann jeden Endbenutzer treffen. Avanan hat PayPal nach dieser Entdeckung umgehend über den Angriff informiert.

Um sich vor diesen Angriffen zu schützen, raten die Sicherheitsforscher den Nutzern:

- Bevor man einen unbekannten Dienst anruft, sollte man nach der Nummer im Internet suchen, denn diese wird dort vielleicht als betrügerisch geführt.
- Prüfung aller Konten, um festzustellen, ob tatsächlich Gebühren angefallen sind.
- Es lohnt sich, erweiterte Sicherheitsmaßnahmen zu implementieren, wie Multi-Faktor-Authentifizierung, um den Zugang zu Konten zu erschweren.
- Bei Zweifeln an der Legitimität einer E-Mail sollte stets die IT-Abteilung informiert werden.

Meine Empfehlung: Der beste Schutz gegen Phishing-Versuche ist ein aufmerksamer Nutzer mit einem kritischen Blick. Daneben zeigen diese Entwicklungen, wie sinnvoll es ist, in den Megatrend der Cybersecurity zu investieren, über Cybersecurity-Aktien bzw. ausgesuchte Cybersecurity-ETFs.

5. Die Polizei, Ihr Krypto-Helfer!

Im Bereich der Online-Kriminalität verfolge ich fortlaufend aktuelle Warnungen der Aufsichtsbehörden, wie der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), der Finanzmarktaufsicht in Österreich und Liechtenstein (FMA) sowie der Eidgenössischen Finanzmarktaufsicht (FINMA) aus der Schweiz.

Ebenso Meldungen seitens der Polizeibehörden und Kriminalämter. Hier treffe ich immer wieder Betrügereien im Zusammenhang mit Krypto-währungen, selbst von kleineren Polizei-dienststellen. So hat das Polizeipräsidium Westpfalz in diesem Zusammenhang eine Information und Warnung veröffentlicht unter dem kreativen Titel:

„Betrüger lieben Krypto-Währungen…“

Statt des erhofften „schnellen Geldes“ hat ein Mann aus dem Landkreis Kusel einen riesigen Verlust gemacht. Der 30-Jährige investierte in sogenannte Krypto-Währungen und fiel dabei auf unseriöse Geschäftemacher herein. Dadurch verlor er einen sechsstelligen Euro-Betrag.

Wie der Mann nun bei der Polizei anzeigte, war er über eine Plattform in den sozialen Medien von einer Frau angeschrieben worden, die ihm empfahl, in Krypto-Währungen zu investieren. Der 30-Jährige ließ sich „bequatschen“ und lud sich eine spezielle App auf sein Handy. Dann lieh er sich Geld von Familie und Freunden, nahm auch einen Kredit auf und startete seine „Investitionen“.

Einzahlen problemlos möglich – Auszahlungen nicht!

Als er sich nach drei Monaten nun Geld ausbezahlen beziehungsweise zurücktransferieren lassen wollte, war dies nicht möglich. Daraufhin wandte er sich an die Polizei. Vermutlich ist der 30-Jährige von Anlagebetrügern hereingelegt worden. Die Ermittlungen laufen.

In diesem Zusammenhang noch einmal der dringende Appell der Polizei: Bleiben Sie wachsam, wenn Ihnen die Werbung im Internet und in den sozialen Medien „schnelles und leicht verdientes Geld“ verspricht. Nicht selten handelt es sich um unseriöse Lockangebote. Auf speziellen Plattformen wird den Anlegern häufig anhand von illustren Zahlen vorgegaukelt, wie rasant sich ihre Investitionen entwickeln. Aber wenn sich jemand seinen vermeintlichen „Gewinn“ auszahlen lassen möchte, bricht der Kontakt ab. Deshalb gilt bei solchen dubiosen Angeboten erhöhte Vorsicht!

Über Love Scamming zum Krypto-Betrug!

Der obige Fall ist nach meiner Einschätzung nicht primär ein klassischer Krypto-Betrug, sondern dürfte weit mehr in das Segment „Love Scamming“ fallen. Mit dem englischsprachigen Begriff „Love Scamming“ oder auch „Romance Scam“ wird eine Form des Internetbetrugs bezeichnet, bei der gefälschte Profile in Singlebörsen und auf sozialen Medien dazu benutzt werden, den Opfern Verliebtheit vorzugaukeln mit dem Ziel, eine finanzielle Zuwendung zu erschleichen.

Meine Empfehlung: Dennoch gilt auch hier natürlich: Augen auf im Online-Verkehr und Achtung vor den digitalen Neppern, Schleppern und Bauernfängern! In jeglichen Betrugs- bzw. Schadensfällen sollte umgehend eine Strafanzeige bei einer Polizeidienststelle gestellt werden.

6. Reich mit Kryptos? Network-Marketing und Schneeballsysteme!

Falls Sie nicht nur ein Produkt kaufen, sondern auch neue Kunden anwerben sollen, dann sind Sie in der Regel im Bereich des Strukturvertriebes, Network-Marketings oder Multi-Level-Marketings (MLM). Der Grat zwischen Seriosität und Abzocke ist dabei sehr schmal.

Die Finanzmarktaufsicht Österreich FMA hat hierzu aktuell in ihren Verbraucher-Informationen in der Rubrik „Reden wir über Geld“ hervorragende Grundlageninformationen veröffentlicht, die ich gerne unterstütze, da auch mein Kampf seit Jahren den digitalen Neppern, Schleppern, Bauernfängern und MLM-Drückern gilt.

Sie haben ein verlockendes Angebot auf Facebook erhalten?

Die Person, die Sie kontaktiert hat, ist jung und dynamisch. Sie sehen Bilder von Fernreisen, Luxusautos und teuren Uhren. Ihr Profil wurde entdeckt, man hat „Ihr Potenzial erkannt“ und möchte Sie unbedingt im Team haben. Auch Sie sollen mit wenig Arbeit reich werden können, indem Sie z.B. Abos für Finanzschulungen vertreiben.

Achtung! Fügen Sie sich, Ihrer Familie und Ihren Freunden keinen Schaden zu, indem Sie deren Vertrauen ausnützen!

Typische Merkmale von Network-Marketing im finanznahen Bereich:

- Die Aussicht, sehr viel Geld verdienen zu können
- Sie müssen ein hohes Einstiegsinvestment tätigen
- Der Aufstieg im System wird als sehr einfach dargestellt
- Sie werden aufgefordert, Freunde und Bekannte anzuwerben

Achten Sie auf diese Warnsignale

- Große Veranstaltungen und Feste in Top-Locations
- Betonung des Gemeinschaftsgefühls
- Darstellung des Systems als neue Bewegung
- Belohnungssysteme wie Reisen, Autoprogramme usw.
- Beratung durch branchenfremde Personen mit geringen Kenntnissen ohne entsprechende Ausbildung
- Es werden keine realen Produkte, sondern Webinare oder Trading-Signale auf WhatsApp vertrieben
- Das Produkt tritt eher in den Hintergrund – die Position in der Verkaufspyramide (Pyramiden-, Ponzi- oder Schneeball-Systeme) steht im Vordergrund

Empfehlung: Stellen Sie sich stets die entscheidende Frage!

Fragen Sie sich bitte immer, ob Sie das Produkt auch ohne das ganze System des Netzwerk-Marketings dahinter kaufen würden. Ist das Produkt für sich allein tatsächlich werthaltig?

Die Abgrenzung zum illegalen Schneeballsystem

Der Unterschied zum illegalen Schneeballsystem ist, dass Sie für den Eintritt in das System Zahlungen leisten müssen, ohne dafür eine echte Gegenleistung zu erhalten. Das neu investierte Geld wird auf andere Mitglieder in höheren Hierarchiestufen verteilt.

Die Rolle der Finanzmarktaufsichtsbehörde FMA in Österreich

Die FMA hat nur dann Handlungsmöglichkeiten, wenn es sich bei den Produkten um Finanzinstrumente handelt oder wenn eine Anlageberatung stattfindet, ohne dass die erforderliche Konzession vorhanden ist. Bei den allermeisten Modellen handelt es sich um keine konzessionspflichtigen Dienstleistungen – trotzdem ist Vorsicht geboten. Lassen Sie sich nicht abzocken!

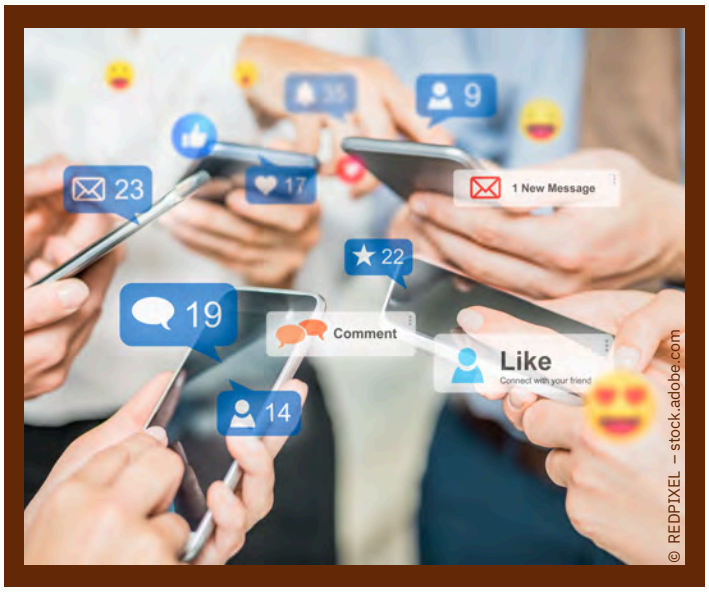
Fazit: Wann ist ein bestimmtes System legal oder illegal?

- **Legal und seriös:** Werthaltige Produkte werden direkt vertrieben
- **Legal und unseriös:** Produkte würden ohne das System nicht gekauft werden
- **Illegal:** keine realen Produkte oder Werte

7. Vorsicht bei Krypto-Tipps aus den sozialen Medien!

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat vor Kurzem eine ebenso wichtige wie richtige allgemeine Warnmeldung im Bereich „Verbraucherschutz“ veröffentlicht, mit Blick auf dubiose Investment-Tipps aus den sozialen Medien:

Viele Verbraucher treffen ihre Anlageentscheidung anhand von Informationen, die sie in den sozialen Medien finden. Die BaFin informiert über den Umgang mit sozialen Netzwerken bei der Geldanlage – und erläutert, wann bei Anlegerinnen und Anlegern die Alarmglocken angehen sollten.



Dubiose Internet-Tipps gehen von Edelmetallen bis Kryptowährungen

Welche Finanzprodukte sollte man kaufen, um möglichst hohe Renditen zu erzielen? Welches Start-up wird der neue Börsenstar? Bei welchen Kryptowährungen werden sich die Preise vervielfachen? Welche Edelmetalle gehören in jedes Portfolio?

Diverse Plattformen wie YouTube, Facebook, Twitter, Instagram, Telegram, Reddit, TikTok und Pinterest bieten Anlaufstellen für Finanzthemen und schnelle Antworten auf die beschriebenen Fragen.

Dabei sind in sozialen Netzwerken durchaus gute Informationsangebote rund um die Geldanlage und Ratschläge mit seriösem Hintergrund zu finden. Allerdings kursieren dort auch unzählige falsche oder nur teilweise richtige Darstellungen. Oft sind Anlagetipps daher nicht verlässlich. Denn nicht alle Tippgeberinnen und Tippgeber kennen sich ausreichend mit Finanzthemen aus. Bei manchen von ihnen ist die Motivation zudem unredlich. Wer solchen Tipps blind folgt, riskiert also Kapitaleinbußen bis hin zum Totalverlust.

Wenn Sie Ratschläge und Angebote aus sozialen Netzwerken bei Ihrer Geldanlage nutzen, sollten Sie äußerst wachsam sein und folgende Prinzipien beachten:

Prüfen Sie, mit wem Sie es zu tun haben!

In den sozialen Medien sind neben echten Kennerinnen und Kennern viele selbsternannte Experten unterwegs. Auch unter den Financial Influencern (kurz: FinFluencer), die regelmäßig und in hoher Frequenz Informationen und Anlagetipps posten. Wer in den sozialen Medien seriös in Fragen der Geldanlage aktiv ist, erläutert in der Regel, wer er ist und worauf sich sein Fachwissen begründet. Sind die Akteure seriös, können Sie deren Angaben in vielen Fällen anhand anderer Quellen überprüfen. Wenn aus einem Post die Identität des Verfassers nicht zweifelsfrei hervorgeht und Sie zudem nicht erkennen können, welchen (beruflichen) Hintergrund derjenige hat, sollten Sie sich auf die Angaben keinesfalls verlassen.

Lassen Sie sich nicht von (scheinbar) hohen Zustimmungswerten blenden!

Viele Follower, viele Likes und viele positive Kommentare sind kein Gütesiegel. Sie sagen wenig bis nichts über die Seriosität oder Qualität eines Auftritts aus. Denn es ist leicht, diese Werte zu manipulieren. Scheinbar positive Kommentare oder Hinweise auf vermeintliche Anlageerfolge können frei erfunden und im Auftrag des Verfassers platziert worden sein. Überprüfbar sind solche Beiträge in der Regel nicht.

Machen Sie sich ein vollständiges Bild von dem angepriesenen Investment!

Alle Geldanlagen bieten Chancen und sind zugleich mit Risiken verbunden. Beides müssen Sie gegeneinander abwägen und mit Blick auf Ihre individuellen Anlageziele bewerten. Ob die in einem Post dargestellten Chancen und Risiken vollständig sind und zutreffen, ist oft nur schwer zu bewerten. Nutzen Sie deshalb immer mehrere Quellen, um sich ein vollständiges Bild vom angepriesenen Investment zu machen. Teil Ihrer Recherche sollten auch unabhängige Quellen sein, wie etwa die Verbraucherzentralen. Seien Sie äußerst skeptisch, wenn in sozialen Medien nur oder überwiegend Erfolgsaussichten dargestellt werden und keine Risiken.

Lassen Sie sich nicht unter Zeitdruck setzen!

Anlagetipps sind oft aggressiv formuliert und erwecken den Eindruck, dass Sie schnell reagieren müss(t)en. Damit will man sich die Sorge von Anlegern zunutze machen, Gewinne zu verpassen (fear of missing out – FOMO), und sie in eine unüberlegte Anlageentscheidung drängen. Lassen Sie sich nicht drängen. Prüfen Sie den Anlagetipp in jedem Fall so sorgfältig, dass Sie die Chancen und Risiken vollständig überblicken und auch verstehen.

Hinterfragen Sie die finanziellen Motive des Tippgebers!

Anlagetipps in sozialen Netzwerken sind meist kostenlos. Das bedeutet, dass sich Akteure wie FinFluencer aus anderen Quellen finanzieren. In der Regel erhalten sie eine Vermittlungsprovision von dem Unternehmen, über dessen Anlageprodukte sie berichten. Dies lösen Sie selbst aus, indem Sie bestimmte Text- und Bilderbereiche anklicken und direkt auf andere Internetseiten geführt werden. Das Problem: Für Sie als Nutzerin oder Nutzer ist dies oft nicht ohne Weiteres erkennbar. Behalten Sie daher im Hinterkopf, dass es solche Vergütungsmodelle gibt, die eine starke Motivation des Tippgebers (MLM-Systeme) sein können.

Seien Sie bei sehr hohen Gewinnversprechen besonders skeptisch!

Das „sichere, schnelle Geld“ gibt es nicht. Werden Ihnen außergewöhnliche Gewinne in Aussicht gestellt? Dann können Sie sicher sein, dass auch das Risiko außergewöhnlich hoch ist. Hinter solchen Tipps verbergen sich meist hochspekulative Anlageprodukte, bei denen Sie viel – oder sogar Ihr gesamtes – Kapital verlieren. Oft steckt sogar Betrug dahinter. Soziale Medien machen es einfach, Falschinformationen zu verbreiten, und locken damit auch Kriminelle an.

Seien Sie vorsichtig, wenn Sie für Anlagetipps auf private Messenger-Dienste wechseln sollen!

Besondere Skepsis ist geboten, wenn Sie in öffentlichen Foren aufgefordert werden, für Anlagetipps auf private Messenger-Dienste zu wechseln. Damit geben Sie nämlich Ihre privaten Kontaktdaten preis. Danach dürften Sie einige ungebetene, unerlaubte Anrufe erhalten, bei denen Ihnen Anlageprodukte angeboten werden und in vielen Fällen Anrufer auch einen hohen Handlungsdruck erzeugen.

Informieren Sie sich über Betrugsmaschen in sozialen Medien!

Um nicht Opfer von kriminellen Machenschaften zu werden, sollten Sie verschiedene Betrugsmaschen kennen:

Über Anlagetipps oder Kontaktaufnahme in den sozialen Medien versuchen Kriminelle, Anlegerinnen und Anleger zum Beispiel auf unseriöse, nicht lizenzierte Online-Plattformen zu locken. Nicht immer geht es dabei von Anfang an um Geldanlage. Oft werden Anleger zum Beispiel über Anfragen in Chat-Boxen und Dating-Plattformen oder per Freundschaftsanfrage kontaktiert und erst später auf unseriöse Online-Plattformen gelenkt.

Dort wird ihnen – häufig durch technische Tricks – vorgegaukelt, dass das Geld, das man dort einzahle, investiert werde und Gewinne erziele. In Wirklichkeit sind aber keine Gewinne möglich, denn die überwiesenen Beträge fließen nicht in eine Kapitalanlage. Betroffen davon sind häufig Investments in Kryptowerte wie beispielsweise Bitcoin oder Ether, aber auch Geschäfte mit finanziellen Differenzkontrakten (Contract for Difference – CFDs).

Werden Sie Opfer eines solchen Betrugs, wird es Ihnen nur sehr schwer gelingen, die Verantwortlichen zu identifizieren. Die stehlen nämlich oft eine Identität und verstecken sich dahinter. Auf den Plattformen der häufig außerhalb der Europäischen Union (EU) ansässigen Anbieter täuschen die Betrüger oft vor, die Genehmigung einer Aufsichtsbehörde zu haben. Bisweilen gibt es diese Behörden, manchmal werden welche erfunden. Oft wird auch so getan, als stehe man in Verbindung zu Unternehmen mit bekannten Markennamen oder man gibt vor, die Plattform sei für öffentliche Stellen wie Ministerien und Polizei tätig.

Für Sie im Vorhinein kaum zu erkennen: Manipulation von Kursen und Preisen!

Immer wieder beeinflussen unlautere Akteure in den sozialen Medien Kurse und Preise von Finanzinstrumenten wie Aktien. Sie versuchen, etwa durch falsche oder irreführende Anlagetipps, Nachfrage nach Aktien zu erzeugen oder zu erhöhen, ohne dabei offenzulegen, dass sie diese Anlageprodukte selbst halten und daher selbst von Kursgewinnen stark profitieren. Sie verbreiten diese unseriösen Anlagetipps in der Absicht, ihr Investment nach dem durch sie herbeigeführten Kursanstieg gewinnbringend wieder abzustoßen. Dadurch fällt der Kurs in der Regel wieder, und alle anderen Anleger verlieren Geld.

Gut zu wissen: Informationen zu aktuellen Betrugsmaschen rund um Anlagetipps in den sozialen Medien finden Sie auch auf verschiedenen Webseiten der Polizei und der Verbraucherzentralen.

Was tun, wenn Sie Opfer krimineller Handlungen in den sozialen Medien geworden sind?

Wenn Sie Opfer einer Straftat in den sozialen Medien geworden sind, sollten Sie unverzüglich Anzeige bei der Polizei oder Staatsanwaltschaft erstatten. Wenn Sie Zweifel haben, können Sie sich auch an die BaFin selbst wenden.

8. Geld verdienen als Crypto-Assistent? Nein!

Der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sind auch vermehrt Fälle bekannt geworden, in denen Unternehmen Verbrauchern auf unlautere Weise Jobs im „Treuhandservice“ anbieten. Die BaFin weist darauf hin, dass sie – entgegen den Angaben in den Stellenbeschreibungen – Treuhandkonten weder registriert noch verwaltet. Mit den Stellenangeboten wird versucht, Verbraucher anzuwerben, die gegen Entgelt über ihr Girokonto im Auftrag des Unternehmens Geldbeträge annehmen und weiterleiten sollen.

Die Unternehmen stellen sich im Internet und in der persönlichen Kommunikation sehr professionell dar und missbrauchen mitunter die Identität anderer Unternehmen. Bei ihrem angeblichen Job im Treuhandservice sollen Verbraucher die Rolle von Finanzagenten übernehmen. Ihre Aufgabe besteht darin, für die Einzahlung oder Überweisung von Geldern angeblicher Kunden des Anbieters ihr eigenes Girokonto zur Verfügung zu stellen und dem Anbieter die Kontodaten mitzuteilen. Anschließend sollen sie das Geld weiterleiten – entsprechend den Weisungen des Anbieters.

Allerdings können sich Verbraucher, die im Treuhandservice agieren, strafbar machen. Denkbar ist insbesondere eine leichtfertige Geldwäsche. Da für die Tätigkeit ein Entgelt vorgesehen ist, können die Verbraucher als Finanzagenten zudem strafrechtlich verfolgt werden, weil sie unerlaubt Zahlungsdienste erbringen. Außerdem könnte es den Verbrauchern passieren, dass die Personen, von denen das eingezahlte oder überwiesene Geld stammt, bei ihnen Rückzahlungsansprüche geltend machen. Die Anbieter solcher Stellen verwenden verschiedene Bezeichnungen.

DIE BELIEBTESTEN INVESTOR-REPORTS

Weitere Gratis-Reports per Klick

Schwarze Liste 2025

Jetzt kostenlos herunterladen

Aktien unter 10 Euro

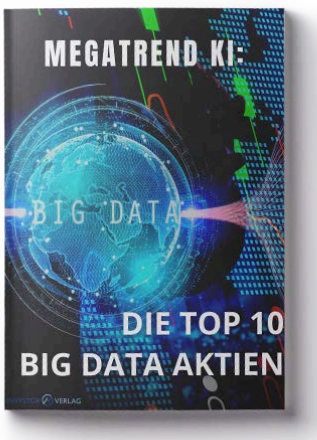
Jetzt kostenlos herunterladen

Krypto-X: Diese 3 Kryptos explodieren

Jetzt kostenlos herunterladen

Megatrends 2025

Jetzt kostenlos herunterladen



Megatrend KI: Die Top 10 Big-Data-Aktien

Jetzt kostenlos herunterladen

Die 10 goldenen Trading-Regeln

Jetzt kostenlos herunterladen

Folgende Job-Beschreibungen sind der BaFin aktuell bekannt:

- Treuhandmanager
- Treuhandassistent
- Transferverwalter
- Transaktionsverwalter
- Kundendienstmitarbeiter im Finanzsektor
- Wertverwalter
- Helfer Geldtransfer
- Helfer Transfermanagement
- Assistent im Währungshandel
- Supportmanager
- Support Mitarbeiter im Asset Management
- Client Trade Analyst
- Anlageverwalter
- Client Trading Analyst
- Crypto-Assistent

Die Tätigkeiten werden dabei im Homeoffice angeboten. Die Betrugsmuster und Stellenbezeichnungen ändern sich ständig. Verbraucher sollten daher überaus wachsam sein, zumal die kriminellen Absichten hinter solchen Angeboten oft nicht leicht zu erkennen sind. Den betroffenen Verbraucherinnen und Verbrauchern empfiehlt die BaFin, die Strafverfolgungsbehörden – Polizei oder Staatsanwaltschaft – zu informieren.

9. Ponzi und Scam: 8 Punkte, wie Sie Betrugs-Systeme erkennen!

Leider stehen die ersten Fragen von neuen Lesern meiner Wirtschaftsdienste „Kapitalschutz vertraulich“ und „KRYPTO-X“, die mich erreichen, sehr häufig im Zusammenhang mit fehlgeschlagenen, betrügerischen „Online-Investments“.
Nachfolgend meine wichtigsten Empfehlungen, die Sie prüfen sollten, bevor Sie eine Investition in einen Krypto-Anbieter bzw. ein Krypto-, Trading- oder generell Online-Investment-System tätigen.

1. Impressum?

Ist ein rechtskonformes Impressum auf der Internetseite vorhanden, mit entsprechender Datenschutzerklärung (DSGVO) und Allgemeinen Geschäftsbedingungen (AGB)?

2. Zulassungen?

Sind bei Trading-, Brokerage- und Investment-Systemen entsprechende Zulassungen der Finanzaufsichtsbehörden (BaFin, FMA, FINMA) vorhanden?

3. Handelsregister?

Ist das entsprechende Unternehmen mit seinem Gewerbe überhaupt im Handelsregister eingetragen und der Gerichtsstand somit korrekt angegeben, ebenso wie verantwortliche Personen? Ist ein Firmensitz im Ausland – beispielsweise in Übersee – plausibel (Haftung, Regulierung, Steuern) oder verbirgt sich dahinter lediglich ein Briefkasten?

4. Team-Zusammensetzung?

Gibt es ein Team, das auf der Internetseite transparent dargestellt ist, und haben die Mitglieder auch die Kompetenz, das beschriebene Geschäftsmodell umzusetzen? Sind die angegebenen Teammitglieder überhaupt reale Personen? Hier hilft eine Suche nach den Namen bei Business-Plattformen wie LinkedIn oder XING, bzw. Twitter.

5. Google-Recherche?

Gibt es bereits Warnungen zum jeweiligen Anbieter im Internet, sei es von Aufsichtsbehörden, Erfahrungsberichten von Kunden oder journalistischen Recherchen? Sind die handelnden Personen bereits einmal negativ in Erscheinung getreten?

Beispielsweise mache ich stets die Erfahrung, dass bei jüngeren MLM-Systemen wie EXW Wallet, BitClub Network, WeGoCrypto WGC, Arbitracoin, Aequatorcoin, Infinity Economics (XIN), Smart Trade Coin, Pulse Empire, Top10Coins, Plus Token, Karatbank Coin, Tycoon69, BCB4U, MCV-CAP, Minerva Trading Bot, Kryptogold, Lopoca, Cloud Token oder Glamjet zahlreiche MLM-Provisions-Vertriebler in der Vergangenheit bereits mutmaßliche Mega-Betrugsprogramme wie OneCoin, Cryp Trade Capital, Optioment, USI-Tech oder Questra vermittelt haben.

6. Geschäftsmodell?

Ist das Businesskonzept des Anbieters überhaupt plausibel? Ist bei einer beworbenen Kryptowährung bzw. einem Token überhaupt eine dezentrale, einsehbare Blockchain vorhanden? Ist das nicht der Fall, ist die Wahrscheinlichkeit eines Shitcoin- bzw. SCAM-Investments annähernd 100%.

7. Renditeversprechen?

Sind Gewinnprognosen überhaupt realistisch und gibt es eventuell sogar Renditeversprechen?

Meine Empfehlung: Sobald im Krypto- oder Tradingbereich Renditen versprochen oder garantiert werden (z.B. Bitclub Network, Plus Token, EXW Wallet), gilt: **Finger weg!**

8. Basiert das Angebot auf einem MLM-System?

Sobald ein Krypto-Angebot oder eine Kryptowährung auf einem MLM-System (Multi-Level-Marketing, Network-Marketing NM) basiert und Provisionen für eine Vermittlung an Sponsoren bezahlt werden, gilt: **Finger weg!**

Neben meinen fundierten Empfehlungen befasse ich mich auch fortlaufend sehr intensiv mit schwarzen Schafen und unseriösen Krypto-, Mining- oder Trading-Anbietern. Diese missbrauchen den Krypto-Boom, um ihre – meist in betrügerischer Absicht konzipierten – Shitcoins oder angeblichen Krypto-Investment- (Scam) bzw. Schneeball-Systeme (Ponzi) gezielt und bewusst an unbedarfte Anleger zu verkaufen. Ich warne Sie regelmäßig vor dubiosen Anbietern und aktuellen Betrugsmaschen.

Im bereits eingetretenen Schadensfall

Sollte das Kind bereits in den Brunnen gefallen sein, sind die nachfolgenden Punkte ratsam:

1. Anzeige bei der Polizei erstatten

2. Nationale Aufsichtsbehörden informieren (BaFin, FMA, FINMA)

3. Beschreitung des Rechtsweges über einen spezialisierten Anwalt – Hier steht Ihnen unser Experten-Netzwerk zur Verfügung!

Meine Empfehlung: Nehmen Sie auch Ihren Vermittler/Sponsor in Haftung und verklagen Sie diesen. Prüfen Sie hierzu rechtliche Schritte über einen versierten Anwalt für Krypto- und Vertriebsrecht, bzw. Bank- und Kapitalmarktrecht.

10. Krypto als Rechtsgebiet

Bereits bekannt sind die Rechtsgebiete des Cyber Crime oder des Wirtschaftsstrafrechts. Doch es entwickelt sich auch ein neuer Bereich, der kriminelle Machenschaften und Kryptowährungen zusammenbringt: Crypto Crime. Hierbei wird nicht nur das Zivilrecht berührt, sondern auch das Strafrecht. Deswegen ist es sehr interessant einmal zu beleuchten, was es damit im Detail auf sich hat.

Schon seit einiger Zeit hat sich das Kryptorecht als neues Gebiet für juristische Beratungen herausgebildet.

Die renommierte Wirtschaftskanzlei SBS LEGAL Schulenberg & Partner aus Hamburg hat sich bereits sehr frühzeitig auf diese Themenfelder spezialisiert und liefert regelmäßig wichtige juristische Informationen rund um den Bitcoin und die Blockchain-Technologie. Die hochspezialisierten Rechtsanwälte beraten dabei zu allen Fragen des Kryptorechts im Zusammenhang mit Investments in Kryptowährungen.

Cyberkriminalität im Strafrecht

Cyberkriminalität beschäftigt Behörden überall auf der Welt. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten. Auf den ersten Blick würde es sehr gut passen, Crypto Crime ebenfalls darunter zu fassen. Denn auch hier geht es um Daten, z. B. solche auf der Blockchain.

Die Bereiche sind allerdings nicht völlig deckungsgleich. So betrifft Cyberkriminalität vor allem Straftaten wie Datenfälschung oder das Ausspähen von Daten.

Cyber Crime im Strafgesetzbuch (StGB)

- **202a StGB: Ausspähen von Daten**

Abs. 1: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

- **269 StGB: Fälschung beweiserheblicher Daten**

Abs. 1: Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Der Blick auf den noch so jungen Rechtsbereich des Crypto Crime

Wenn es um kriminelle Machenschaften in Bezug zu Kryptowährungen geht, sind etwas andere Straftaten relevant. Hier geht es um Geldwäsche und Betrug bis hin zu Diebstahl und Erpressung. Um Kryptokriminalität effektiv zu bekämpfen, müssen unterschiedliche Institutionen zusammenarbeiten. Regierungen, Strafverfolgungsbehörden und die Kryptowährungs-Industrie müssen sich gegenseitig unterstützen. Denn der Kryptobereich wächst schnell und die Technologien wandeln sich. Damit ändern sich auch die kriminellen Verhaltensweisen.

Besonders Geldwäsche kann hier erträglich sein. Im letzten Jahr betrug der Gesamtwert aller gewaschenen Krypto-währungen ca. 23,8 Mrd. USD. Das geht aus dem offiziellen Crypto Crime Report hervor, der jährlich von Chainalysis veröffentlicht wird. Dies entspricht einem Anstieg von 68 Prozent im Vergleich zum Vorjahr.

Bitcoin und Blockchain – Verruf durch Straftaten

Kryptokriminalität sorgte dafür, dass vor allem staatliche Behörden viele Kryptoanbieter genauer unter die Lupe nahmen. Bitcoin und die Blockchain sorgen für einen gewissen Grad an Misstrauen, eben weil der Betrugsmarkt so groß ist. So haben deutsche Ermittler erst vor Kurzem einen großen Geldwäschedienst für Kryptowährungen abgeschaltet. Ein weiteres Beispiel ist die milliardenschwere Krypto-Börse FTX, welche schon Insolvenz anmelden musste.

Hier ist unklar, ob es sich um ein Betrugssystem gehandelt hat. Jedenfalls haben Anleger Verluste in Milliardenhöhe erleiden müssen. Sogar für illegale Deals mit Drogen, Waffen und gestohlenen Daten wurden Bitcoins bereits zur Verschleierung genutzt. Zwar bleibt Bargeld das größere Risiko für illegale Geschäfte.

Doch Kryptokriminalität ist ein ernst zu nehmender Bereich.

Ist jede Straftat mit Krypto gleich Crypto Crime?

Die Bestimmung des Crypto Crime-Sektors ist nicht einfach. Denn bei einer Vielzahl von Straftaten können Kryptowährungen eine Rolle spielen. So könnte bei manchen Straftaten einfach Bitcoin als Währungsersatz dienen oder selbst das Tatobjekt sein. Doch nur weil jemand Bitcoins stiehlt, handelt es sich nicht gleich um Kryptokriminalität.

Ebenso verhält es sich damit, wenn Hacker auf einem fremden Computer ein Programm zum Mining von Krypto-Tokens installieren. Der Computer wird dann ohne Zustimmung des Nutzers dazu benutzt, die Hacker zu bereichern. Dies ist jedoch dem etablierten Cyber Crime zuzuordnen.

Crypto Crime: Zahlreiche neue Rechtsfragen erfordern Experten für Kryptorecht!

Es wurden bereits große rechtliche Schritte getätigt, um Anleger vor Crypto Crime zu schützen. Seit 2020 fallen beispielsweise Krypto-Verwahrstellen und weitere Finanzdienstleister im Krypto-Finanzsektor unter das Kreditwesengesetz und das Geldwäschegesetz. Damit sind gewisse Sorgfaltspflichten verbunden, die den Markt sicherer machen sollen.

Auch wenn nicht jede Straftat mit Kryptowährungen gleich Crypto Crime bedeutet, lohnt sich ein eigener rechtlicher Bereich. Denn es stellt sich eine Vielzahl unerforschter Rechtsfragen im Falle von Kryptokriminalität. Darüber hinaus ist im Steuerrecht häufig unklar, wie man Gewinne durch Kryptowährungen korrekt versteuern muss. Auch diese rechtliche Unklarheit bietet Raum für Kriminalität.

Wie macht man sich am Kapitalmarkt strafbar, wenn man Kryptokurse manipuliert? Oder wann findet deutsches Strafrecht überhaupt Anwendung, wenn Kryptogeschäfte international abgewickelt werden? Für diese und andere Rechtsfragen lohnt sich eine anwaltliche Beratung im Kryptorecht. In diesem Bereich gibt es für mich im deutschsprachigen Raum und im internationalen Kontext keine besseren Rechtsexperten als die hochspezialisierten Anwälte von SBS LEGAL, sowie die Steuerexperten von SBS TAX!

Kontaktdaten

SBS LEGAL Rechtsanwälte
SBS TAX Steuerberater
Tel.: 0049(0)40-7344 086-0
www.sbs-legal.de

Impressum

Investor Verlag, ein Unternehmensbereich der
FID Verlag GmbH
Koblenzer Str. 99
D-53177 Bonn,

Handelsregister: HRB 7435
Registergericht: Amtsgericht Bonn

Geschäftsführer
Richard Rentrop

Kontakt
Telefon: 0228 – 9 55 04 30
(Kundendienst)
Telefax: 0228 – 36 96 499
E-Mail: kundenservice@investor-verlag.de
Internet: https://www.investor-verlag.de

Redaktionell Verantwortlicher
Redakteur: Markus Miller (V.i.S.d.P.)
Herausgeber: Marc Brede
Koblenzer Str. 99
D-53177 Bonn

Bildnachweis
Adobe Stock, https://stock.adobe.com/de/

Disclaimer

Zur Sicherung der journalistischen Unabhängigkeit der FID Verlag GmbH handeln alle Mitarbeiter und Redakteure nach den Publizistischen Grundsätzen des Deutschen Presserates (Pressekodex) sowie nach den Journalistischen Verhaltensgrundsätzen und Empfehlungen des Deutschen Presserats zur Wirtschafts- und Finanzmarktberichterstattung (Verhaltensgrundsätze). Der Pressekodex enthält Richtlinien für die publizistische Arbeit nach den Empfehlungen des Deutschen Presserats. Die Verhaltensgrundsätze berücksichtigen die gesetzlichen Regelungen der Marktmissbrauchsverordnung (MAR) zum Verbot von Insidergeschäften und von Marktmanipulation und konkretisieren den Pressekodex im Hinblick auf die Erstellung, Weitergabe und Veröffentlichung von Anlageempfehlungen oder Anlagestrategieempfehlungen journalistischen Publikationen. Sie treten an die Stelle der entsprechenden Vorschriften der Marktmissbrauchsverordnung bzw. des Wertpapierhandelsgesetzes.

Sofern nicht anders angegeben, stammen historische Unternehmens- sowie Konsenszahlen aus dem OCT Aktien Screener, der seine Daten über Morningstar, FactSet und die Börse Stuttgart bezieht.

Ergänzende Informationen zum Autor und den von ihm verwendeten Analysemethoden finden Sie **hier**.

Der Verfasser und/oder eine an der Erstellung der Publikation mitwirkende natürliche oder juristische Person, und/oder deren Angehörige oder verbundene Unternehmen halten möglicherweise Long- oder Short-Positionen betreffend die im Report genannten Finanzinstrumente. „Long-Position“ bedeutet eine Investition, mit der von steigenden Kursen des Finanzinstruments profitiert wird, wohingegen bei „Short-Positionen“ von sinkenden Kursen profitiert wird. Diese Personengruppe unterliegt den strengen Compliance-Richtlinien des Verlages. Nur unter den darin gemachten Auflagen ist es diesen Personen erlaubt, die empfohlenen Werte selbst zu handeln.

Risikohinweis: Unseren Risikohinweis finden Sie **hier**.

Redaktionsschluss: 21. November 2024, 17:00