



Rendite genial? Verlust total!

Was Sie über Online-Anlagebetrug wissen sollten

Ihre Polizei und die Schweizerische Kriminalprävention (SKP) – eine interkantonale Fachstelle der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)

Investieren Sie Ihr Geld mit Vernunft!

In Zeiten von Nullzinspolitik der Banken und allgemein unsicherer Wirtschafts- und Börsenlage ist es schwierig geworden, erworbenes Vermögen zu sichern, geschweige denn zu vermehren. Viele Anleger suchen deshalb verstärkt nach stabilen (z.B. Gold, Immobilien) und **neuartigen Anlageformen**, die auch in Krisenzeiten hohe Rendite versprechen, wie z.B. **Kryptowährungen**. Diese Situation wird gerne von Trickbetrügern ausgenutzt, die sich als progressive Finanzdienstleister ausgeben und verunsicherte Kleinanleger zu Investitionen verleiten, bei denen sie nichts gewinnen, aber alles verlieren können. Das nennt man **Online-Anlagebetrug** (engl. «investment fraud»), und wie er typischerweise abläuft, erfahren Sie in dieser Broschüre.



Phase 1: Anködern

Der Betrugsangriff startet normalerweise mit breit gestreuten **Werbeanzeigen** im Internet (Popups, Werbebanner, Spammails etc.) und in Online-Newsportalen, aber auch mit unangeforderten Telefonanrufen und Kontaktversuchen in den sozialen Netzwerken und sogar auf Online-Dating-Plattformen. Manchmal kommt der vermeintliche Insider-Tipp auch von einer Internetbekanntschaft, die Freundschaft oder gar Liebe vorgaukelt («pig butchering»).

Ziel der Betrüger/innen ist dabei zunächst nur, Sie grundsätzlich für die jeweilige neue Anlageform zu **interessieren** und dazu zu verleiten, Ihre **Kontaktdaten** zu hinterlassen. Dazu werden Sie – oftmals auch schon dann, wenn Sie auf Ihrer Online-Suche nach Anlagemöglichkeiten einschlägige Suchbegriffe eingeben – auf seriös wirkende (und suchmaschinenoptimierte!) Webseiten der Betrüger/innen gelenkt. Dort gaukelt man Ihnen überzeugende Argumente vor, zuweilen auch mit dem Hinweis auf prominente «Testimonials», die die angebotene Anlage angeblich ebenfalls mit Erfolg getätigten hätten.



Phase 2: Persönlicher Erstkontakt

Wenn Sie sich dann auf einer solchen Website registriert haben, erhalten Sie kurze Zeit später einen **Anruf eines/einer angeblichen Anlageberaters/Anlageberaterin**. Da Sie vermutlich noch skeptisch sind, wird diese/r nicht versuchen, Sie schon von Anfang an zu grösseren Investitionen zu überreden, sondern nur zu einer kleinen von vielleicht CHF 250 oder CHF 500, zum «Ausprobieren». Sie sollen das Gefühl haben, völlig frei zu entscheiden. Danach erhalten Sie einen Zugang zu Ihrem «Account» auf der Website, damit sie die angebliche Performance Ihrer Anlage verfolgen können, und werden wohl jedesmal, wenn Sie sich einloggen, feststellen, dass Ihr Geld sich vermehrt hat. **Das soll und wird Sie überzeugen, mehr zu investieren.**



Phase 3: Vertrauensbildung

Infolge der guten Performance schwindet Ihre Skepsis, und Sie freuen sich vielleicht sogar, wenn Ihr/e Berater/in Sie das nächste Mal anruft. Das ist auch im Sinne der Betrüger/innen, denn Sie sollen immer mehr das Gefühl bekommen, bei Ihren weiteren Investitionen ganz **persönlich betreut** zu werden. Die Betrüger/Betrügerinnen beherrschen das sogenannte «Social Engineering», sie wissen also, mit welchen zwischenmenschlichen Techniken sie ihr Opfer manipulieren können. Dabei werden Sie anfänglich wohl **nicht direkt unter Druck gesetzt**, sondern nur indirekt durch angeblich nur **begrenzt verfügbare** oder **zeitlich limitierte Angebote**. Ausserdem dient das neue Vertrauensverhältnis dazu, Sie gegen ehemalige Finanzpartner Ihres Vertrauens (z.B. Ihre Hausbank) abzuschirmen. Die Betrüger/innen eröffnen dann z.B. bei echten Händlern von Kryptowährungen ein Konto (Wallet) in Ihrem Namen und mit Ihrer Legitimation, doch die Zugriffsrechte darüber haben nicht Sie allein (wenn überhaupt), immer aber die Betrüger/innen. Es kommt sogar vor, dass sich die Täter/innen über Fernwartungssoftware den Zugang zu Ihrem Computer erschleichen und dann mit Ihrem e-Banking Überweisungen tätigen.



4

Phase 4: Nachschuss

Wenn Sie dann eine Zeitlang Ihre Gewinnsteigerungen beobachtet haben und aus irgendeinem Grund einen Teil des Geldes abheben wollen, werden Sie feststellen, dass nur geringfügige Beträge – oder sogar überhaupt keine – ausbezahlt werden. Ihr/e Berater/in wird Ihnen z.B. erklären, es habe einen **plötzlichen Crash** gegeben oder Sie müssten zuvor eine **hohe Steuerabgabe** entrichten. Er/sie wird jetzt – diesmal womöglich auch mit direktem Druck bis hin zur Drohung – versuchen, Sie vom speziellen Charakter der Investition zu überzeugen, der es erfordere, noch mehr Geld nachzuschiessen, um die Gewinne zu sichern. Eventuell wird auch ein angeblicher Vorgesetzter oder sogar der **«Chef»** des Unternehmens ins Feld geführt, der mittels seiner behaupteten Autorität beruhigend auf Sie einzuwirken versucht und Ihnen weiterhin finanzielle Erfolge in Aussicht stellt, wenn Sie nur bei der Stange blieben. Wenn Sie immer noch aussteigen wollen, wird Ihnen möglicherweise auch noch eine **Versicherung gegen Verluste** angeboten; diese hätten Sie angeblich von vornherein abschliessen können, aber aus Kulanz werde man das für Sie auch rückwirkend ermöglichen. Das ist alles nicht wahr. Schliesslich dämmert Ihnen, dass Sie einem Betrug zum Opfer gefallen sein könnten. Sie klammern sich aber irrationalerweise umso mehr an Ihre/n vertraute/n Berater/in: Am Ende behauptet diese/r möglicherweise, er/sie könne doch noch einen Weg finden, Ihren Einsatz wieder herauszuholen, dafür sei aber eine **Vorabzahlung von Bank-, Rechts- oder Notargebühren** erforderlich ...



5

Phase 5: Verlust-Realisierung

Was auch immer Sie versucht haben: **Sie erhalten kein Geld zurück** (– ausser evtl. in der Anfangsphase und auch dann nur kleinere Beträge, um Sie in Sicherheit zu wiegen und weiter zu ködern). Jetzt ist Ihnen definitiv klar, dass Sie Opfer eines Betrugs geworden sind.



Was Sie tun sollten, bevor Sie in neue Anlageformen investieren:

- Vor allem bei hohen Renditeversprechen und komplexen Anlagebereichen wie Kryptowährungen, Forex-Trading und angeblichem Handel mit binären Optionen ist Vorsicht geboten. Nehmen Sie sich Zeit und informieren Sie sich an möglichst vielen verschiedenen Stellen. Lassen Sie sich nie unter Druck setzen, weder von Berater(inne)n, noch von angeblich limitierten Angeboten.
- Lassen Sie sich von unrealistischen Versprechen nicht blenden. Kein seriöser Finanzdienstleister verspricht überdurchschnittliche Gewinne in kurzer Zeit.
- Überprüfen Sie, ob der Anbieter/die Anbieterin eine Bewilligung der FINMA (www.finma.ch → FINMA Public → Bewilligte Unternehmen) hat oder in der FINMA-Warnliste (www.finma.ch → FINMA Public → Warnungen) aufgeführt ist. Stossen Sie auf zweifelhafte Angebote, sollten Sie diese der FINMA mittels Meldeformular (www.finma.ch → FINMA Public → Meldung erstatten) melden. Solche Hinweise ermöglichen es der FINMA, unerlaubt tätige Anbieter zu entdecken und aus dem Verkehr zu ziehen.
- Überprüfen Sie, ob die Plattform auf der Warnliste von Cybercrimepolice aufgeführt ist: cybercrimepolice.ch → Warnliste
- Überprüfen Sie den Handelsregisterauszug von Schweizer Anbietern unter www.zefix.ch.
- Recherchieren Sie im Internet nach dem Angebot, auch in Verbindung mit Wörtern wie «Betrug». Tauchen nur schon vereinzelt Betrugswarnungen auf, lassen Sie die Finger davon.
- Wenden Sie sich an Ihren Kundenberater/Ihre Kundenberaterin Ihrer Hausbank und an Experten/Expertinnen Ihres Vertrauens für eine fachmännische Einschätzung.

Was Sie tun sollten, wenn Sie Opfer eines Online-Anlagebetrugs geworden sind:

- Informieren Sie umgehend Ihre Polizei und erstatten Sie Anzeige!
- Informieren Sie sofort Ihre Hausbank, dass die in Frage kommenden Überweisungen betrügerisch waren. Allenfalls können so Geldbeträge noch auf dem Weg zur Täterschaft gestoppt werden.
- Überweisen Sie nie Geld an angebliche Privatdetektive, Rechtsanwälte oder Staatsanwälte, die vorgeben, sich um Ihren Verlust kümmern zu wollen. Diese gehören mit grösster Wahrscheinlichkeit zur selben Betrügerbande.

Generell gilt:

- Schnelles Geld ohne Verlustrisiko ist eine Illusion!
- Niemand verrät «Geheimtipps» öffentlich im Internet. Wer für einen Geheimtipp Werbung machen muss, hat keinen.
- Niemand teilt vielversprechende Anlagestrategien – auch nicht versehentlich.
- Anlagetipps, welche mit prominenten Persönlichkeiten beworben werden, sind in aller Regel gefälscht. Das gilt auch für angebliche News-Beiträge, Interviews oder Medienkonferenzen. Die Prominenten haben meistens keine Ahnung, dass sie als Köder für Online-Anlagebetrug dienen sollen.
- Vertrauen Sie nie jemandem Geld an, den Sie nur virtuell kennen.
- Investieren Sie nie, ohne das Angebot vorgängig ausgiebig zu recherchieren und zu prüfen.
- «Nicht gutes Geld dem schlechten nachwerfen!»: Drohende Totalverluste können nicht abgewendet werden, indem man immer neues Geld nachschießt.



Weitere Informationen:
← online-anlagebetrug.ch
www.ebas.ch/investment-fraud →





Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch

August 2025

Dieses Faltblatt entstand in Zusammenarbeit mit
der **Hochschule Luzern** und «eBanking – aber sicher!».

www.ebas.ch | www.ebankingabersicher.ch

Lucerne University of
Applied Sciences and Arts

eBanking aber sicher!

**HOCHSCHULE
LUZERN**

Informatik
FH Zentralschweiz