

Achtung: Anlagebetrug! So schützen Sie sich vor der großen Abzocke

19.11.2020

von



Altmann, Kathleen

Schlagworte

Anlegerschutz

Wertpapier

Rendite

Zinsen

Onlinebanking

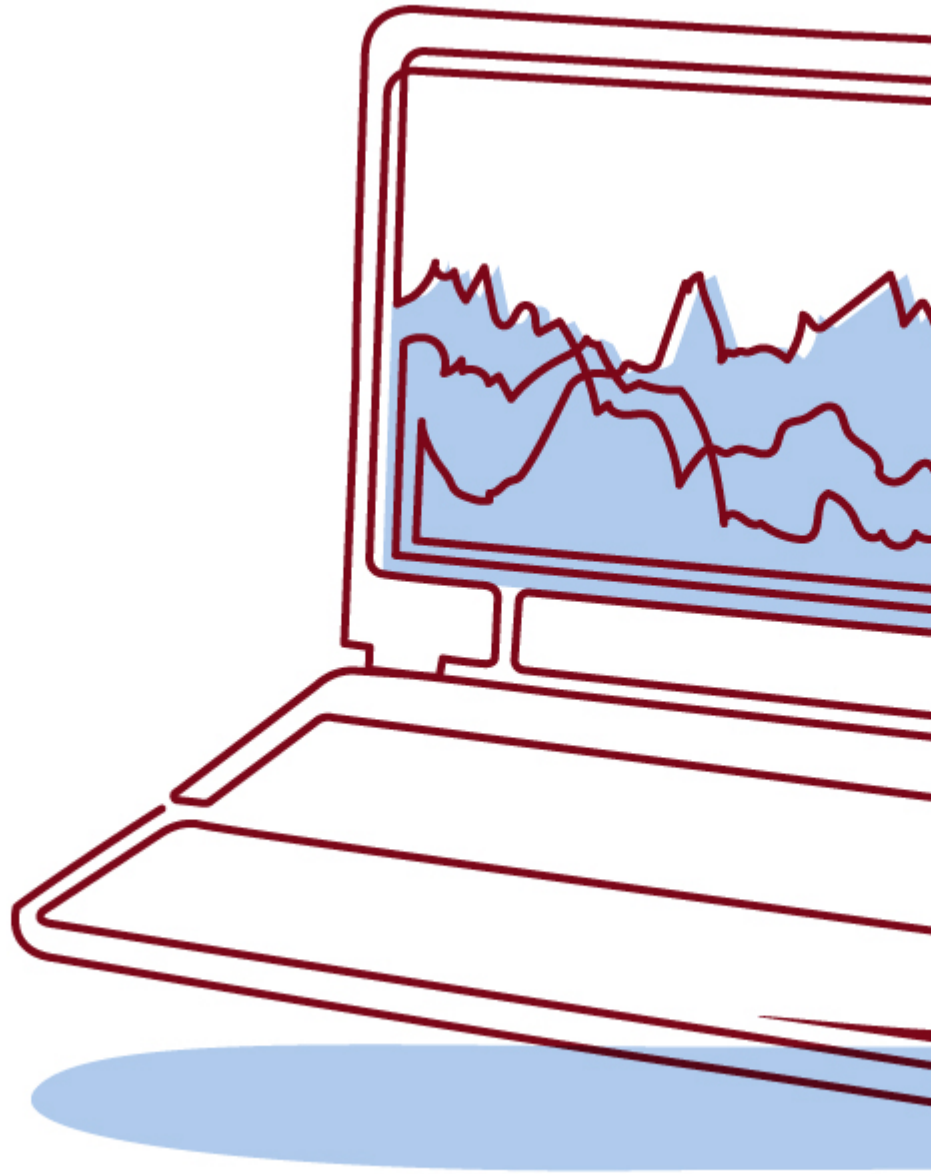
Cyberattacken

Kryptowährung

Geldanlage

Cyberkriminalität

Verbraucher



Wer im Internet nach lukrativen Geldanlagemöglichkeiten sucht, sollte Vorsicht walten lassen. Für einen nur kleinen Anlagebetrag wird teilweise eine hohe Rendite versprochen. Das mag auf den ersten Blick sehr verlockend klingen, vor allem bei den aktuell niedrigen Zinsen. Aber Vorsicht, hinter solchen Versprechen lauert oft ein Anlagebetrug!

Anleger werden geködert

Charakteristisch für diese Betrugsmasche ist der Ablauf in mehreren Phasen: In einer ersten Phase wird das potenzielle Opfer geködert. Dazu schalten Betrüger Werbung - etwa in bekannten Online-Magazinen oder in den Sozialen Medien. Das

weckt den Anschein der Seriosität. Allerdings werden die Werbeanzeigen häufig nicht ausreichend geprüft, da diese Anzeigenseiten meist an externe Dienstleister ausgelagert werden. Diese Anzeigen verlinken auf Webseiten mit einem seriös wirkenden Aufbau.

Das Ködern kann aber auch über Spam-Mails erfolgen. E-Mails werden so angelegt, dass sie gängige Spamfilter umgehen. Sie kürzen beispielsweise Schlagwörter wie Bitcoin ab oder versehen sie mit Sonderzeichen. Oft werden seriös klingende Formulierungen oder Schlagwörter benutzt, wie „Ihr Schweizer Finanzpartner“ oder „Sonderbericht“. Nicht selten wird auch auf betrügerische Weise mit bekannten Persönlichkeiten, Unternehmen oder Fernsehsendungen ohne deren Kenntnis geworben. Ziel der Betrüger in dieser ersten Phase ist es, dass sich die Opfer mit ihren Kontaktdaten, insbesondere ihren Rufnummern, auf einer gefakten Website registrieren.

Der erste Kontakt meist am Telefon

Ist das erreicht, ruft in der Regel ein „Berater“ oder „Finanzmakler“ den potenziellen Anleger an. Weil der sich vorher registriert hat, kann er den Anrufer zuordnen und schöpft daher meist keinen Verdacht. Es werden zum Beispiel Anlagen in Kryptowährungen, Gold oder auch in spezielle Wertpapiere empfohlen, mit denen auf Kursentwicklungen von Kryptowährungen, Aktien, Währungen, Rohstoffen gewettet wird (Optionen, Derivate). In welches Anlageprodukt investiert werden soll, kann der Anleger selbst entscheiden. Vereinbart werden anfänglich kleinere Anlagesummen von beispielsweise 250 oder 500 Euro.

Überweist der Anleger diesen Anlagebetrag, erhält er einen „Onlinebanking-Zugang“ für ein vermeintliches Wertpapierdepot. Hier wird ihm sein eingezahlter Geldbetrag angezeigt, und mit jeder neuen Anmeldung zudem, wie die Erträge angeblich inzwischen gestiegen sind. Das Geld ist aber in Wahrheit längst verloren.

Wie die Betrüger sich Vertrauen erschleichen

Diese Betrugsmasche ist deshalb so erfolgreich, weil das Opfer durch den angeblichen „Berater“ persönlich kontaktiert wird; dies schafft ein gewisses Maß an Vertrauen. Mit derselben Intention erzählt der „Berater“ oftmals bei den Anrufen erfundene Geschichten aus seinem eigenen Leben. Dem Anleger werden im Gespräch dann Informationen entlockt, die einen Rückschluss auf seine Liquidität zulassen. Dem Opfer wird dabei stets vorgegaukelt, alle Anlageentscheidung aus eigenen Stücken zu treffen. Gleichzeitig wird von Seiten der Betrüger mit der Aussage, die günstigen Angebote würden nur kurzfristig zur Verfügung stehen, Druck aufgebaut, möglichst schnell einen Abschluss zu tätigen.

Einmal betrogen, doppelt abgezockt

Ist das erst einmal geschehen, werden die Opfer überzeugt, weitere Überweisungen – meist mehrere Tausend Euro - zu tätigen. Häufig werden dafür durch die "Beratung" auch bestehende Anlagen gekündigt, um das einsetzbare Kapital zu erhöhen. Erst wenn sich der Anleger irgendwann einmal seine Gewinne auszahlen lassen will, wird ihm bewusst, dass er Opfer eines Betrug geworden und das eingesetzte Geld verloren ist.

Jetzt kommt ein weiteres Szenario hinzu: Der Betrüger kommt dem Wunsch des Opfers nach Auszahlung des Geldes vermeintlich nach. Allerdings sei es dafür notwendig, dass es einen weiteren Geldbetrag überweist. Die Gründe hierfür seien beispielsweise Steuern, Bonuszahlungen, Nachschusspflichten oder Versicherungsbeiträge. Auch dieses eingesetzte Geld ist unwiederbringlich verloren.

So können Sie sich und andere schützen

1. Klicken Sie keine Werbung an, die unseriöse Versprechungen macht

Achten Sie genau darauf, ob es sich um eine Anzeige handelt. Oft sind Anzeigen in der gleichen Typografie wie die Artikel des seriösen Online-Magazins verfasst. Verzichten Sie auf das Anklicken von dubiosen Anzeigen. Das gilt auch für die Sozialen Medien.

2. Überprüfen Sie die aufgerufene Webseite

Die Verlinkung führt zu einer Webseite, auf der man sich registrieren soll. Prüfen Sie diese Anmelde-Seite: Können Sie diese mit Freunden teilen? Wenn nicht, handelt es sich höchstwahrscheinlich um einen Betrugsversuch. Denn: Durch das Teilen würde die genaue Adresse der Webseite aufgedeckt.

3. Schützen Sie Ihre persönlichen Daten

Geben Sie fremden Personen keine persönlichen Daten preis. Erteilen Sie keine Berechtigung, sich auf ihren Computer einzuloggen, sollte man Ihnen Hilfe beim Zugang zu diesen Webseiten anbieten.

4. Vorsicht bei Schlagwörtern in E-Mails

Achten Sie auf Schlagwörter, die Vertrauen wecken sollen, wie „Ihr Schweizer Finanzpartner“, „Sonderbericht“. Verzichten Sie darauf, solche E-Mails zu öffnen.

5. Achten Sie auf Layout und Schreibweise

In einigen Spam-Mails wird das bekannte Erscheinungsbild von bekannten Fernsehsendern genutzt, um einen seriösen Eindruck zu vermitteln. Achten Sie hier auf abweichende Schreibweisen oder einzelne Buchstaben, die zum Beispiel durch Zahlen ersetzt werden.

6. Ein gesundes Misstrauen hilft

Lautet das Angebot „Kleiner Anlagebetrag, große Rendite“, handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch. Ein gesundes Misstrauen hilft auch anderen: Sprechen Sie daher auch mit Ihrer Familie und Freunden über diese Betrugsmethode.

7. Erstellen Sie Anzeige bei der Polizei

Haben Sie einen Verdacht oder sind Sie tatsächlich Opfer einer Betrugsmasche geworden, erstatten Sie Anzeige bei der Polizei. Sie helfen Sie damit, den Betrügern auf die Schliche zu kommen und vor allem bewahren Sie andere Anleger vor einem finanziellen Verlust.

Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und das Bundeskriminalamt (BKA) haben Verbraucher schon früh auf die Gefahren im Online-Handel mit bestimmten spekulativen Finanzinstrumenten hingewiesen.