CYBERTRADING-BETRUG: CHECKLISTE FÜR DEN ERNSTFALL

Beim Anlagebetrug im Internet werden finanziell interessierte Personen gezielt durch manipulierte Werbeanzeigen angelockt, um sich auf vermeintlich lukrative und schnelle Investitionsgeschäfte einzulassen.

SO GEHEN TÄTERINNEN UND TÄTER VOR

Für das Anwerben potenzieller Opfer werden Werbeanzeigen im Internet oder in sozialen Netzwerken geschaltet. Die Anzeigen versprechen erfolgreiche Kapitalanlagen, häufig gekoppelt mit besonders hohen Renditeversprechen. Unter Zuhilfenahme von Deepfakes werden auch Prominente eingeblendet, die dazu auffordern, in Aktien oder Kryptowährungen zu investieren.

Die Täter nutzen dabei oft eigens für diese Masche erstellte gefälschte Anlageplattformen für Online-Investments. Diese lassen auf den ersten Blick keinen Zweifel an Seriosität und Echtheit zu. Die dort eingesetzte Software ermöglicht es den Tätern, den Verlauf der Aktienkurse zu ihren Gunsten zu beeinflussen. Ein echter Handel findet nicht statt, sondern wird vorgetäuscht. Das investierte Geld wird durch die Täter nicht angelegt, es verschwindet in deren kriminellen Netzwerken.

HINWEIS

Der Modus Operandi beim Cyber-Trading-Fraud entwickelt sich fortlaufend weiter – die Täter verwenden immer wieder neue Methodiken, beispielsweise zur Verschleierung der Geldflüsse (meist Krypto-Transaktionen).

SIE INTERESSIEREN SICH FÜR CYBERTRADING...

... dann sollten Sie darauf achten:

- ✓ **Zu schön, um wahr zu sein:** Werbeanzeigen oder (überhöhte) Gewinnversprechen in den sozialen Medien.
- ✓ **Ihr „Anlageberater“** meldet sich außergewöhnlich schnell persönlich.
- ✓ Sie werden um **Fernzugriff** auf Ihren Rechner gebeten.
- ✓ Sie sollen Geld auf **Auslandskonten** überweisen, oft auch nur **geringe Einzahlungen** wie 250 €.
- ✓ Der Eindruck von **Dringlichkeit und Zeitdruck** wird vermittelt: limitierte Gelegenheit oder Last-Chance.
- ✓ **Oft erhalten Sie anfangs auch Auszahlungen**, die Ihr Vertrauen in die Seriosität der Plattform erhöhen sollen.
- ✓ Eine **Auszahlung des Gewinns** wird danach an **Nachzahlungen** gebunden. Oft wird zur erneuten Investition gedrängt, um das Geld „zurückzuholen“.

Wir wollen, dass Sie sicher leben. Ihre Polizei

SO SCHÜTZEN SIE SICH VOR CYBERTRADING-BETRUG

- Misstrauen bei hohen Gewinnversprechen mit geringem Risiko. Bei Werbeanzeigen auf Websites, bei Social-Media-Beiträgen, Spam-Mails oder Messenger-Diensten. Seien Sie vorsichtig bei reißerischen Angeboten oder angeblichen Geheimtipps.

- Überprüfen der Seriosität der angeblichen Trading-Plattformen. Informieren Sie sich und recherchieren Sie, bevor Sie investieren. Kontrollieren Sie hierbei Impressum, Adresse und Ansprechpartner.

  Hier finden Sie seriöse Informationen:
  - bei der BaFin
  - auf den Seiten der Verbraucherzentrale
  - auf Warnlisten (Vorsicht, nicht alle sind gelistet, da ständig neue Plattformen entstehen.)
  - Bei ihrer Bank

- Keine sensiblen Daten an ungeprüfte Seiten weitergeben. Schützen Sie Ihre Zugangsdaten, Ausweisdokumente und Zahlungsinformationen.

- Keinen Fernzugriff zulassen. Auch wenn es als ein vermeintlich nettes Unterstützungsangebot getarnt ist.

- Nicht unter Druck setzen lassen. Tätigen Sie keine Überweisung auf unbekannte Konten. Nehmen Sie sich immer die Zeit zu prüfen, ob es sich um seriöse Anbieter handelt.

Mehr Informationen zu Cybertrading-, Kredit- und Anlage Betrug:
www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/cybertrading-betrug/

Wir wollen, dass Sie sicher leben. Ihre Polizei