

Money Mules und Finanzagenten

Wenn das eigene Konto zum Tatwerkzeug wird

Beschreibung

Money Mules sind Personen, die ihr Bankkonto, einen Zahlungsaccount oder eine Krypto-Wallet nutzen beziehungsweise zur Verfügung stellen, um Vermögenswerte für andere zu empfangen und weiterzuleiten. Kriminelle setzen solche Konten und Wallets als Zwischenstationen ein. Dadurch schaffen sie Abstand zur Straftat und erschweren die Nachverfolgung. Die Gelder können unter anderem aus Phishing, Kontoübernahmen, Online- und Investmentbetrug, CEO-Fraud, Romance Scam, Zahlungsbetrug und organisierter Kriminalität stammen.

Typische Anwerbung und Vorgehensweise

- **Falsche Jobangebote:** Homeoffice und hohe Provisionen werden versprochen. Tatsächlich sollen fremde Gelder über das Privatkonto laufen.
- **Freundschaftsdienst oder Notlage:** Eine Person behauptet, ihr Konto nicht nutzen zu können, und bittet um Empfang, Weiterleitung oder Barbehebung von Geld.
- **Romance Scam:** Nach dem Aufbau einer emotionalen Beziehung soll das Opfer Geld empfangen, weiterleiten oder in Kryptowerte tauschen.
- **Schnelles Geld:** Über soziale Medien wird eine Provision für die Kontonutzung, einen Krypto-Transfer oder eine Bargeldübergabe angeboten.

Typische Warnsignale

- Provision allein für die Nutzung des eigenen Kontos
- Sofortige Weiterleitung, Aufteilung, Barbehebung oder Krypto-Umwandlung
- Konto- oder Wallet-Eröffnung beziehungsweise Weitergabe von Bank- oder Krypto-Zugängen für andere
- Zeitdruck, Verschwiegenheit oder Aufforderung zu falschen Angaben gegenüber der Bank

Rechtliche Einordnung in Österreich

§ 165 StGB erfasst unter anderem das vorsätzliche Umwandeln oder Übertragen von Vermögensbestandteilen aus krimineller Tätigkeit zum Zweck der Verschleierung. Der Grundstrafrahmen beträgt sechs Monate bis fünf Jahre, in schweren Fällen ein bis zehn Jahre. Ob eine angeworbene Person strafbar ist, hängt von ihrer konkreten Handlung sowie den gesetzlich erforderlichen Wissens- und Vorsatzelementen ab.

Wichtig: Diese Information ersetzt keine rechtliche Beurteilung des Einzelfalls.

Maßnahmen im Verdachts oder Schadensfall

- **Transaktionen stoppen:** Keine weiteren Überweisungen, Abhebungen oder Krypto-Umwandlungen durchführen.
- **Bank informieren:** Zahlungseingänge, Empfänger und Anwerbung offenlegen; Rücküberweisungen zuerst abstimmen.
- **Anzeige erstatten:** Bei jeder Polizeidienststelle; bei einer bevorstehenden Übergabe sofort die Polizei verständigen.
- **Beweise sichern:** Chats, Profile, Kontaktdaten, IBAN, Belege, Screenshots sowie Krypto-Transaktionsdaten speichern.
- **Zugänge schützen:** Passwörter ändern und gefährdete Karten, Konten oder Wallets sperren lassen.

Präventionsempfehlungen der Polizei

- ✓ Hinterfragen Sie Angebote, bei denen Sie für den Empfang oder die Weiterleitung fremder Gelder bezahlt werden.
- ✓ Prüfen Sie Arbeitgeber und Kontaktpersonen über selbst recherchierte Kontaktdaten.
- ✓ Stellen Sie Ihr Konto niemals für fremde Zahlungsströme zur Verfügung – auch nicht einmalig.
- ✓ Bestätigen Sie nur Transaktionen, deren Empfänger, Betrag und Zweck Ihnen bekannt sind.
- ✗ Geben Sie Bank- oder Krypto-Zugänge niemals weiter und eröffnen Sie keine Konten oder Wallets für andere.

Weiterführende Links

FMA – Money Mules

www.fma.gv.at/fma-klaert-auf-money-mules-wenn-dein-konto-zum-tatwerkzeug-wird

Bundeskriminalamt – Geldwäscherei

www.bundeskriminalamt.at/308/start.html