

So verlieren Sie Ihre Kryptowährung nicht

Eine Checkliste: was Sie nie tun sollten, wie Sie sich schützen und was zu tun ist, wenn es schon passiert ist.

Das sollten Sie nie tun

- 1 Geben Sie niemandem Ihre Wiederherstellungsphrase (12–24 Wörter) oder Ihren privaten Schlüssel.** Keine Börse, kein Support und keine Polizei fragt danach. Wer danach fragt, will stehlen.
- 2 Investieren Sie nie über jemanden, den Sie online kennengelernt haben:** in einer Dating-App, auf Telegram, WhatsApp oder Facebook. So beginnen die meisten Betrugsfälle, auch nach Monaten des Schreibens.
- 3 Glauben Sie keinem garantierten Gewinn.** „2 % pro Tag“, „ohne Risiko“, „nur heute“ bedeuten immer Betrug.
- 4 Zahlen Sie nie, um Ihr eigenes Geld abzuheben.** Wird vor der Auszahlung eine „Gebühr“, „Steuer“ oder „Versicherung“ verlangt, ist das Geld bereits weg.
- 5 Installieren Sie keine Fernzugriffs-Apps** (AnyDesk, TeamViewer und ähnliche), nur weil jemand darum bittet.
- 6 Antworten Sie keinem „Support“, der Sie zuerst anschreibt.** Echte Admins und Börsenmitarbeiter schreiben nicht zuerst.
- 7 Ein Anruf von Ihrer „Bank“, „Börse“ oder „der Polizei“?** Legen Sie auf und rufen Sie selbst die offizielle Nummer an.
- 8 Bestätigen Sie in Ihrer Wallet nichts, was Sie nicht verstehen.** Ein einziges „Approve“ oder „Sign“ auf einer gefälschten Seite kann die ganze Wallet leeren.
- 9 Prüfen Sie die ganze Empfängeradresse, nicht nur Anfang und Ende.** Kopieren Sie Adressen nicht aus dem Transaktionsverlauf: Betrüger schleusen dort sehr ähnliche Adressen ein.
- 10 Vertrauen Sie keinen „Rückholddiensten“, die Ihnen Ihr Geld garantiert zurückholen wollen oder Krypto im Voraus verlangen.** Das ist der zweite Betrug nach dem ersten.

So schützen Sie sich

- Tippen Sie die Adresse der Börse selbst ein oder öffnen Sie sie über ein Lesezeichen. In Google-Ergebnissen und Anzeigen tauchen gefälschte Seiten auf.
- Nutzen Sie eine Börse mit Zulassung in der EU. Schalten Sie die Zwei-Faktor-Bestätigung per Authenticator-App ein, nicht per SMS.
- Aktivieren Sie bei Ihrer Börse die Liste erlaubter Auszahlungsadressen: Dann kann Geld nur an Adressen gehen, die Sie freigegeben haben.
- Bewahren Sie größere Beträge auf einer Hardware-Wallet auf, die Sie nur direkt beim Hersteller gekauft haben.
- Prüfen Sie ab und zu, welchen Seiten Ihre Wallet Berechtigungen gegeben hat, und widerrufen Sie die unnötigen (zum Beispiel mit revoke.cash).

Wenn es schon passiert ist

- 1 Zahlen Sie nichts mehr** und brechen Sie den Kontakt zu den Betrügern ab.
- 2 Sichern Sie Beweise:** Transaktions-IDs (TxID), Adressen, Beträge, Zeitpunkte und Screenshots der Chats und der Website.
- 3 Melden Sie es sofort** Ihrer Börse und der Polizei. Die ersten Stunden zählen am meisten: Solange das Geld noch auf einer Börse liegt, kann es eingefroren werden.
- 4 Wenn Sie verfolgen lassen wollen, wohin das Geld gegangen ist,** und Beweise für Polizei und Börse brauchen: trailforensics.com.

Trail Forensics fragt nie nach Wiederherstellungsphrasen, Passwörtern oder Wallet-Zugang und garantiert nicht, dass Geld zurückgegeben wird.