

Krypto-Seed-Checkliste:

Trage deine Seed-Phrase **niemals** online ein. Keine Webseite, keine App und kein Support braucht diese Wörter.

- Ich habe meine Seed-Phrase niemals online eingegeben.
- Ich habe keine Fotos oder Screenshots meiner Seed-Phrase erstellt.
- Meine Seed-Phrase liegt nicht in Google Drive, iCloud, Dropbox, E-Mail, Notizen-App oder Passwortmanager.
- Ich habe die Seed-Phrase offline auf Papier oder besser auf Metall gesichert.
- Ich habe mindestens ein Backup an einem sicheren, getrennten Ort.
- Niemand außer mir kennt die vollständige Seed-Phrase.
- Ich habe geprüft, dass alle Wörter korrekt und in richtiger Reihenfolge notiert sind.
- Ich habe niemals einem angeblichen Support-Mitarbeiter meine Seed-Phrase gegeben.
- Ich nutze für größere Beträge eine Hardware Wallet.
- Ich bewahre PIN, Passphrase und Seed-Phrase getrennt voneinander auf.

Hardware Wallet für mehr Sicherheit prüfen

Eine Hardware Wallet wie der Trezor Model T kann helfen, private Schlüssel offline zu halten. Wichtig bleibt trotzdem: Auch bei einer Hardware Wallet darfst du deine Seed-Phrase niemals auf einer Webseite eingeben.

Affiliate-Link: <https://bitcoinbasis.de/anbieter/trezor/model-t>

Was tun, wenn du deine Seed-Phrase bereits eingegeben hast?

1. Betrachte die alte Wallet als kompromittiert.
2. Erstelle auf einem sicheren Gerät eine komplett neue Wallet.
3. Notiere die neue Seed-Phrase offline und sicher.
4. Übertrage vorhandene Coins schnellstmöglich auf die neue Wallet.
5. Verwende die alte Wallet danach nicht weiter.
6. Prüfe Geräte und Browser auf verdächtige Erweiterungen oder Malware.

Wichtiger Hinweis

Diese Checkliste dient der allgemeinen Information und ersetzt keine individuelle Sicherheitsberatung. Gib deine Seed-Phrase niemals an Dritte weiter und trage sie niemals in Online-Formulare ein.