Crypto Self-Defence Checklist

LEARNED THE HARD WAY

12 rules, each one paid for by a real heist. Tick them off.

- [ ] **Never run a "take-home task" on a work computer**
  A job test that asks you to download and run code is the oldest trick in this playbook. Use a throwaway machine or decline.
  `BINANCE 2026 · fake job interview, homework repo · $6.3B`

- [ ] **Verify the company before the interview**
  Look the recruiter and the company up outside the chat: website age, registered address, real employees. If it only exists in the conversation, stop.
  `BINANCE 2026 · "Project Director" for a company that did not exist`

- [ ] **Install developer tools only from the official source**
  Type the address yourself; don't follow search ads or links in DMs. Check the publisher and the checksum.
  `BINANCE 2026 · tampered installer while searching for an AI coding tool`

- [ ] **Don't sign what you can't read**
  If your wallet screen shows a wall of code instead of a clear amount and destination, don't approve it. "Blind signing" is how a vault gets handed over.
  `BYBIT 2025 · signers approved a disguised transaction · $1.5B`

- [ ] **Check the transaction on a second, independent device**
  The website can lie; your hardware wallet's own screen, or a separate decoder, is the second opinion.
  `BYBIT 2025 · tampered wallet interface showed a normal transfer`

- [ ] **Treat "approve" and "delegate" like handing over keys**
  Some signatures grant ongoing control, not a one-off payment, and can be hard to take back. Review and revoke old approvals regularly.
  `BINANCE 2026 · one signature delegated control of a hot wallet`

- [ ] **Use phishing-resistant sign-in (security keys)**
  Hardware security keys stop most stolen-password and fake-login attacks that SMS codes don't.
  `ALL CASES · stolen credentials were the way in`

- [ ] **Turn on withdrawal allow-lists and delays**
  On every exchange you use, lock withdrawals to saved addresses and add a time delay for new ones.
  `BINANCE 2026 · money kept leaving through pre-approved paths`

- [ ] **Don't keep everything in one place**
  Exchanges can pause withdrawals for days after a hack. Keep only what you trade on an exchange.
  `BINANCE & BYBIT · withdrawals paused or flooded after the hack`

- [ ] **Copy-paste is not verification**
  Check the first and last characters of every address you send to; malware swaps addresses in your clipboard.
  `COMMON · address-swapping malware`

- [ ] **Nobody can "recover" your stolen crypto for a fee**
  After every big hack, fake "recovery experts" flood the comments. Real investigators don't DM you first.
  `EVERY HACK · recovery scams follow the headlines`

- [ ] **Assume the attacker is patient**
  The big thefts were prepared for weeks or months before the money moved. Unusual requests are a signal, not noise.
  `BYBIT · 17 days inside · BINANCE · 5 months`

Not financial or legal advice. General security practice, illustrated with public reporting on the Bybit (Feb 2025) and Binance (Oct 2026) hacks. Sources and full reconstructions: youtube.com/@Casebuild.