Crypto Scam Radar Checklist

Use this simple checklist to spot scams, avoid manipulation, and stay safe.

If you check even one major red flag, stop immediately.

SECTION 1

⚠ High-Risk Red Flags (Instant “No”)

These are deal-breakers. If any appear, it’s a scam.

- [ ] **Guaranteed or “risk-free” returns**
  “10% daily profit” / “we guarantee doubling your money”.
- [ ] **Pressure or urgency**
  “last chance,” “act now,” “don’t miss out”.
- [ ] **Requests for your recovery phrase or private key**
  No legitimate service will ever ask for this.
- [ ] **Someone offering to “help” with wallet setup or recovery**
- [ ] **A stranger asking you to install software or remote-access tools**
- [ ] **Unregulated platform asking you to deposit first**
- [ ] **Romantic interest + investment advice**
  The “pig butchering” pattern.
- [ ] **Promises of “insider access,” “exclusive signals,” or “secret strategies.”**
- [ ] **Platforms requiring you to recruit others to earn money.**

SECTION 2

Suspicious Behaviors & Patterns

Not always scams alone, but dangerous if combined.

- [ ] Team members are anonymous or unverifiable.
- [ ] Website has spelling errors or inconsistencies.
- [ ] Token has no real use case explained in plain language.
- [ ] Overemphasis on a “roadmap” but no working product.
- [ ] The community is aggressive or overly defensive.

- [ ] Returns depend on new users joining.
- [ ] Social media engagement seems artificially inflated.
- [ ] No clear explanation of how the platform makes money.
- [ ] The product sounds too complex to be explained simply.
- [ ] The domain name looks suspicious or slightly misspelled.

SECTION 3

Messages / DMs / Emails to Ignore Automatically

If a message feels like any of these, treat it as spam or a scam attempt.

"Hello sir/ma'am, I'm from customer support..."

"Your wallet has a problem — click to fix."

"I noticed you are having issues; I can help."

"Claim your free airdrop now."

"Verify your wallet by entering your seed phrase."

"Our group has insider crypto signals — join us."

"I made huge profits; let me show you how."

"Send me a small amount to prove your wallet is active."

SECTION 4

Safe-Behavior Reminders

A short list of protective habits you can practice every time.

- [ ] Use only official websites and verified apps.
- [ ] Double-check URLs slowly before logging in.
- [ ] Never share your recovery phrase.
- [ ] Never let anyone access your computer remotely.
- [ ] Enable 2FA (authenticator app preferred).
- [ ] Use strong, unique passwords.
- [ ] Always test with small amounts first.
- [ ] Avoid making decisions when emotional (fear or excitement).
- [ ] Research platforms before depositing funds.

SECTION 5

What To Do When in Doubt

A gentle sequence you can follow anytime something feels off.

- Stop.
- Don’t send anything.
- Don’t reply to messages.
- Close the window or app.
- Search for verified reviews or warnings.
- Ask someone knowledgeable (or wait until you’ve cooled off).
- Trust hesitation — it’s a sign of awareness, not ignorance.

“A scam depends on urgency. Safety depends on slowing down.”

Mind Treks
Built by learners. Not sellers.