Aegisum | Education

Common Crypto Scams

Cryptocurrency offers exciting opportunities, but with its rise, scams have become more prevalent. Billions of dollars have been lost to fraudulent schemes, leaving victims with little to no recourse.
Scammers exploit hype, fear, and greed, using sophisticated tactics to deceive even experienced users. By understanding the most common crypto scams, you can protect yourself and your assets.

1 Pump-and-Dump Schemes: The Classic Market Manipulation

Pump-and-dump scams artificially inflate a cryptocurrency's price to lure in unsuspecting buyers. Once prices peak, scammers sell off their holdings, causing a sudden crash. How it works:

Scammers create hype around a low-volume coin, often in private Telegram or Discord groups.
Coordinated buys push the price up, attracting FOMO-driven investors.
Once the price peaks, insiders sell, crashing the market and leaving new investors with losses.
How to avoid it:

BE SKEPTICAL of coins suddenly trending with no fundamental reason.

CHECK trading volume—low liquidity coins are easier to manipulate.

AVOID "signals" groups promising guaranteed profits.

Fake ICOs: The Illusion of a Groundbreaking Project 2

Initial Coin Offerings (ICOs) raise funds for new blockchain projects, but scammers often create fake ICOs to steal investor funds. Red flags of a fake ICO:

No clear roadmap, whitepaper, or working product.

Anonymous or unverifiable team members.

Unrealistic promises like "guaranteed 100x returns."

Pressure tactics: "Limited-time investment opportunities."

How to Avoid It:

- **RESEARCH** the team—legitimate projects have verifiable developers.
- **CHECK** for transparent tokenomics and a working product.
- **AVOID** projects with no independent audits or reviews.

3 Imposter Scams: Fake Celebrities, Influencers, and Support Teams

Scammers create fake accounts pretending to be Elon Musk, Vitalik Buterin, or other well-known figures to trick users into sending crypto.
Common imposter scams:

Twitter & YouTube Giveaways: "Send 1 ETH, get 2 ETH back!" (Always fake.)

Fake Customer Support: Scammers pretend to be support agents, asking for private keys or seed phrases.

WhatsApp & Telegram Messages: Unsolicited messages from "investment managers" promising huge returns.

How to Avoid It:

- **VERIFY** accounts (official influencers have blue checkmarks).
- **NEVER** send crypto to random "giveaways."
- **REAL** support will never ask for your private key.

Rug Pulls: When DeFi Projects Disappear Overnight 4

A rug pull happens when a DeFi project's developers abandon it after collecting investor funds, leaving worthless tokens behind. How to spot a rugpull:

Anonymous Team: No public information about the developers.

No Code Audits: Lack of third-party security verification.

Centralized Token Control: Devs can dump tokens at any time.

High APYs & Rewards: "Earn 10,000% interest!" (If it sounds too good to be true, it is.)

How to Avoid It:

- **CHECK** the project's liquidity lock. If liquidity isn't locked, the devs can pull funds anytime.
- **AVOID** anonymous or unverifiable teams.
- **LOOK** for real-world utility and partnerships.

5 Social Engineering: When Scammers Exploit Human Psychology

Unlike technical hacks, social engineering scams manipulate people into revealing sensitive information. Common Social Engineering Tactics:

Phishing Emails: Fake emails pretending to be from an exchange or wallet provider.

Phone Scams: Callers posing as "customer support" asking for sensitive details.

Fake Urgency: Messages claiming "your account is compromised" to trick you into clicking malicious links.

How to Avoid It:

- **ALWAYS** verify URLs and email addresses before entering login credentials.
- **ENABLE** Two-Factor Authentication (2FA) to prevent unauthorized access.
- **NEVER** share private keys or seed phrases, even with "support."

Conclusion: Stay Skeptical, Stay Safe

Crypto scams continue to evolve, but knowledge is your best defense. By staying informed and skeptical of too-good-to-be-true offers, you can avoid falling victim to fraud.

Final Tip: Always **do your own research** (DYOR) before investing or trading. Trust no one with your private keys.

All rights reserved. AEGISUM ©2025