What are the most prevalent crypto scams to be aware of?

Last Modified on 09/06/2026 1:32 am PDT

Cryptocurrency scams take many forms, and no single list captures every scheme or variation. Government agencies and cryptocurrency service providers regularly warn about investment fraud, fake trading platforms, task scams, phishing, wallet drainers, impersonation, and recovery scams. According to the FBI's 2025 IC3 Annual Report, cryptocurrency investment fraud produced the highest reported financial losses to Americans during 2025, with approximately $7.2 billion in reported losses. That figure reflects complaints submitted to IC3 and may not account for every incident.

Cryptocurrency investment scams may involve fake trading platforms, fraudulent investment groups, token promotions, purported AI-powered trading services, or other schemes that misrepresent how funds will be invested. Promoters may advertise guaranteed returns, minimal risk, exclusive access, or fabricated past performance through social media, messaging applications, advertisements, and group chats. Some platforms display fictitious profits or permit a small initial withdrawal to build confidence before encouraging larger deposits. The SEC's Investor.gov guidance identifies guaranteed returns, emerging-technology claims, manipulated token prices, and additional withdrawal fees as recurring warning signs.

Relationship-based investment scams—sometimes called "pig butchering" scams—are a particularly damaging form of cryptocurrency investment fraud. They commonly begin through an unsolicited text, social-media message, dating application, investment group, or apparently accidental contact. The person gradually builds trust through friendship, romance, or investment guidance before directing the target to a particular website or application. The SEC warns that these platforms may display fabricated trades, profits, and account balances. When the user attempts to withdraw, the platform may demand purported taxes, deposits, or regulatory fees. A displayed balance alone does not establish that the platform holds the assets it claims.

Job and task scams typically advertise easy remote work involving activities such as rating products, liking videos, processing orders, or "optimizing" applications. The platform may display commissions or allow a small payment to build confidence. It then requires the user to deposit personal funds—frequently cryptocurrency—to unlock additional tasks or withdraw supposed earnings. The Federal Trade Commission warns that legitimate employment should not require someone to deposit cryptocurrency to complete tasks or receive payment. Unexpected job offers and demands to "pay money to earn money" are significant warning signs.

Phishing and wallet-drainer schemes attempt to obtain login credentials, seed phrases, private keys, or wallet permissions. They may use fraudulent websites, search advertisements, browser extensions, airdrops, emails, or direct messages that imitate legitimate services. Some malicious decentralized applications attempt to persuade users to approve smart-contract permissions that can later be used to transfer tokens without obtaining the wallet's seed phrase. MetaMask identifies phishing websites, compromised recovery phrases, malicious approvals, malware, and fraudulent extensions as potential causes of unauthorized wallet transactions. Users should never disclose a seed phrase to someone offering support and should carefully review transaction details before signing. See our guide to avoiding crypto drainers and malicious smart contracts.

Impersonation scams may involve someone claiming to represent a cryptocurrency exchange, wallet provider, government agency, law-enforcement organization, celebrity, or established business. These messages often create urgency by alleging that an account has been compromised or that funds must be transferred to a "safe" wallet. The FBI warns that exchange impersonators may request login information, identification documents, or immediate action through a supplied link. Anyone receiving such a message should contact the organization through a

separately verified website or telephone number rather than relying on contact information supplied by the sender.

Cryptocurrency recovery scams target people who have already experienced a financial loss. A purported investigator, attorney, government representative, or recovery specialist may claim that funds have been located and can be released after an advance payment. Some scammers possess details about the original loss or impersonate real professionals to appear credible. The FBI has specifically warned about fictitious law firms and recovery providers using these tactics. Unsolicited contact, guaranteed recovery claims, unverifiable affiliations, requests for sensitive credentials, and unexplained advance payments are important warning signs. Learn more about evaluating cryptocurrency recovery firms.

Warning signs appearing across multiple crypto scams include guaranteed profits, pressure to act immediately, requests for secrecy, unsolicited investment advice, unverifiable credentials, demands to transfer cryptocurrency to an unfamiliar wallet, and additional payments required to access supposed funds or earnings. Before sending money, independently verify the individual, company, website, and investment opportunity. Users should not rely solely on social-media profiles, testimonials, professional-looking websites, app-store availability, or balances displayed on an unfamiliar platform as evidence of legitimacy.