Market Talks
EDUCATION CENTER

CRYPTO · BEGINNER · LESSON 14 OF 15

Scams, Rug Pulls and Red Flags

How the most common crypto scams work, from rug pulls and pump and dumps to fake investment platforms, impersonators and wallet drainers, and the warning signs they share

11 min read · 8 quiz questions with answer key

CRYPTO · BEGINNER · LESSON 14 OF 15

Scams, Rug Pulls and Red Flags

IN ONE SENTENCE

Crypto scams take billions of dollars every year. Most of them follow a small number of patterns, and once you can recognise the patterns, the warning signs become much easier to see.

Why scams are a big part of crypto

Crypto transactions are fast, global and cannot be reversed. There is no bank to call and ask for a refund, and no central desk that can freeze a payment that has already left your wallet. These same features that make crypto useful also make it attractive to scammers.

The numbers are large. Blockchain analysis firm Chainalysis estimated that crypto scams took **more than $17 billion** in 2025, a record. In the United States alone, the FBI's Internet Crime Complaint Center (IC3) received crypto-related complaints with reported losses of about **$11.4 billion** in 2025, up 22% from the year before. About $7.2 billion of that came from fake investment schemes.

Scams are also getting more professional. Chainalysis found that impersonation scams grew by more than 1,400% in 2025, and the average amount taken per payment rose from about $782 to about $2,764. Many operations now use AI to write messages, translate conversations and create fake videos.



Figure 1. Crypto scams reached record levels in 2025. Figures are estimates from Chainalysis and complaints reported to the FBI.

Rug pulls and honeypots

A **rug pull** happens when the people behind a token or project suddenly take the money and disappear, "pulling the rug" from under the buyers. It is most common with new tokens on decentralized exchanges, where anyone can create a token and a trading pool in minutes (Lessons 7 and 9).

Common versions include:

- **Liquidity pull:** the creators remove the funds from the trading pool. With nothing left to trade against, the token's price collapses to almost zero.
- **Team dump:** the creators hold a large share of the supply and sell it all into the market at once.
- **Honeypot:** the token's smart contract is written so that people can buy but cannot sell. The price chart only goes up, because no one except the creators is able to sell.



Figure 2. A simplified view of the Squid Game token rug pull. Holders could not sell while the price rose, then the creators drained the pool.

EXAMPLE: THE SQUID GAME TOKEN, 2021

In late 2021 an unofficial token named after the popular TV series appeared on PancakeSwap, a decentralized exchange. Its price rose by tens of thousands of percent in a few days and passed **$2,850** on 1 November 2021. Buyers soon found they could not sell it. Then the creators sold their holdings and drained the pool, and within minutes the price fell to about **$0.002**. The creators left with roughly $3.38 million. The show's makers had nothing to do with it.

Pump and dumps

In a **pump and dump**, a group buys a small, thinly traded coin quietly, then promotes it loudly through social media posts, paid influencers or chat groups. As new buyers rush in, the price jumps.

The organisers then sell ("dump") their coins to these late buyers, and the price falls back, often below where it started.

Pump and dumps work because small coins have very little liquidity (Lesson 8), so a modest amount of buying can move the price a lot. A sudden flood of posts all saying the same thing about an unknown coin, often with countdowns and price targets, is a typical sign.

Fake investment platforms and "pig butchering"

The largest category of losses comes from fake investment schemes. One well known form is called **pig butchering**, a translation of a Chinese phrase used by the scammers themselves: they "fatten up" the victim with trust before "slaughtering" them.

It usually starts with a message that looks harmless: a "wrong number" text, a dating app match or a new contact on social media. Over weeks the scammer builds a friendship or romance. Eventually they mention that they make good money trading crypto, and offer to show you how.

The victim is guided to a trading website or app that looks professional but is fake. The balance on the screen grows quickly, and small early withdrawals may even work, which builds trust. Deposits get bigger. When the victim tries to take out a large amount, the platform suddenly demands a "tax", "fee" or "unlock deposit" first. After that is paid, the platform and the friend disappear.

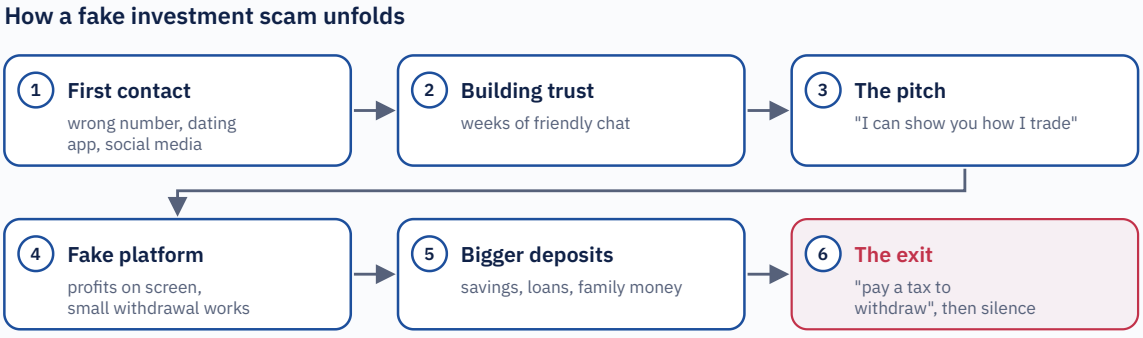


Figure 3. The typical stages of a pig butchering scam. Trust is built slowly, and the losses come at the end.

EXAMPLE: HOW IT LOOKS FROM THE INSIDE

Laura gets a text from Michael: "Hi David, are we still on for golf Saturday?" She replies that he has the wrong number. Michael apologises, and they start chatting. Six weeks later he shows her screenshots of his trading profits and helps her open an account on a platform he uses. Her first $1,000 grows to $1,600 on screen, and a $200 withdrawal arrives in her wallet. She deposits $25,000. When she asks to withdraw, support says she must first pay a 20% "tax" on her profits. The numbers on the screen were never real.

Impersonators, fake support and recovery scams

Many scams work by pretending to be someone you trust:

- **Fake support:** after you post a question in a public forum or chat group, someone sends a private message claiming to be from the exchange or wallet's support team. Real support teams do not start private chats and never ask for a seed phrase or password.
- **Fake exchange or government contact:** a call, email or text says your account is at risk and you must move your funds to a "safe" wallet right away.
- **Fake celebrities and giveaways:** a video or post shows a famous person promising to send back double any crypto you send. AI-generated deepfake videos now make these look convincing. No real giveaway works this way.
- **Recovery scams:** after someone loses money, a "recovery expert" or fake law firm offers to get it back for an upfront fee. These target people who have already been scammed once.

Wallet drainers, approvals and fake airdrops

Some scams do not need you to send anything. Instead, they trick you into giving a malicious smart contract permission to move your tokens.

When you use a DeFi app, your wallet often asks you to **approve** a contract to spend a certain token for you (Lesson 12). A fake website, often promoted as a free **airdrop**, a mint or a reward claim, asks you to connect your wallet and sign. What you actually sign is an approval, sometimes for an unlimited amount, that lets the scammer's contract take your tokens. This kind of tool is called a **wallet drainer**.

Other common tricks include fake wallet apps and browser extensions that steal the seed phrase as you type it, look-alike website addresses, and address poisoning (Lesson 10). Anyone who has your **seed phrase** has full control of your wallet, as covered in Blockchain Lesson 9. Old approvals stay active until they are removed, and tools such as Revoke.cash and some block explorers show which approvals a wallet has given.

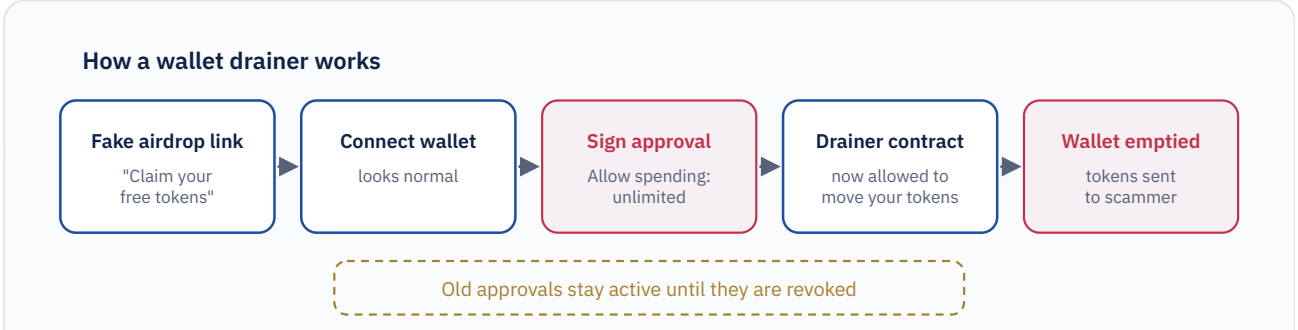


Figure 4. A wallet drainer does not ask you to send funds. It asks you to sign a permission that lets it take them.

The red flags most scams share

The stories change, but the warning signs repeat:

- **Guaranteed or very high returns**, such as "2% a day" or "no risk".
- **Urgency and pressure:** act now, the offer ends tonight, your account will be closed.
- **Requests for your seed phrase or private key**, for any reason.
- **Unsolicited contact** that slowly turns to investing.
- **A platform that is not well known**, recommended by a new online friend, or an app not found through official sources.
- **Withdrawals that need a fee first.**
- **"Send crypto to get double back".**
- **Tokens you cannot sell**, an anonymous team holding most of the supply, or unlocked liquidity.

One red flag is not proof of a scam, but several together are a strong warning.

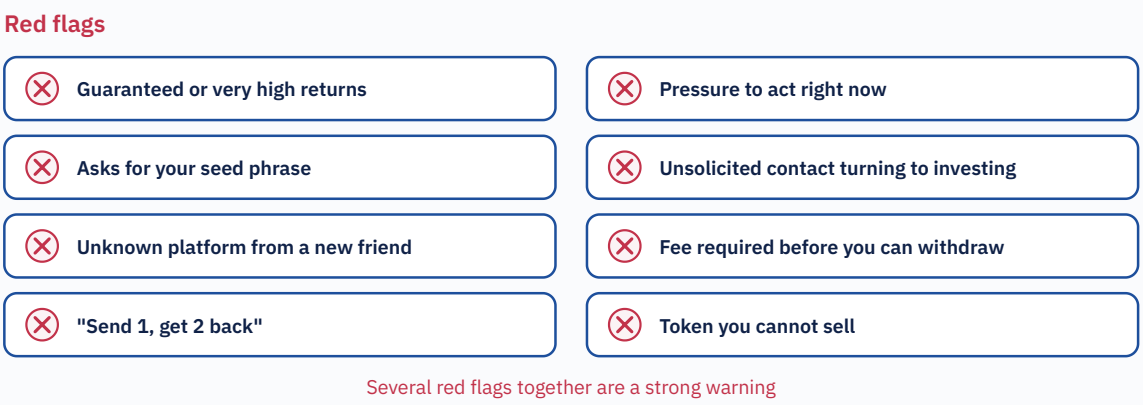


Figure 5. Common warning signs shared by most crypto scams.

What happens after a scam

Because blockchain transfers are final, money sent to a scammer is very rarely recovered. Sometimes, if the funds reach a regulated exchange quickly, that exchange can freeze them, and stablecoin issuers such as Tether and Circle have frozen stolen funds in some cases.

Steps that authorities such as the FBI describe include reporting the scam to the police and, in the US, to IC3; telling the exchange or platform that was used; keeping records such as transaction hashes, wallet addresses, messages and website links; and removing any wallet approvals that were given. Many people also move remaining funds to a new wallet with a new seed phrase if they think the old one has been exposed.

Authorities also warn that people who report a loss are often contacted afterwards by recovery scammers, so the second loss can follow the first.

Why this matters for traders

- **Fast gains attract scams.** New tokens with huge daily gains are exactly where rug pulls, honeypots and pump and dumps happen. Checking whether a token can be sold, who holds the supply and whether liquidity is locked is part of the basic research many traders do.
- **"Copy my trades" offers.** Groups that promise private trading tips or account management in exchange for deposits are a common entry point for fake platforms.
- **Approvals pile up.** Active DeFi users can build up many old token approvals over time. Each one is a possible risk if the contract is ever compromised.
- **The same security habits protect trading accounts.** Exchange accounts are a target too: phishing emails, fake login pages and SIM swaps aim to take over accounts and withdraw funds. Lesson 15 covers the basic protections exchanges offer.

Key terms

Rug pull	When a project's creators suddenly take the money, for example by removing liquidity or dumping their tokens, leaving the token almost worthless.
Honeypot	A token whose smart contract allows buying but blocks selling for everyone except the creators.
Pump and dump	A scheme where organisers buy a small coin, hype it to push the price up, then sell to the late buyers.
Pig butchering	A long scam in which the scammer builds trust over weeks, then leads the victim to deposit large sums on a fake investment platform.
Phishing	Fake messages, emails or websites that copy a real service to trick people into giving away passwords, codes or seed phrases.
Wallet drainer	Malicious code on a fake website that tricks users into signing approvals or transactions that move their tokens to the scammer.
Token approval	A permission you sign that lets a smart contract spend a certain token from your wallet, up to a set amount or without limit.

Deepfake	A fake video or audio clip, usually made with AI, that shows a real person saying something they never said.
Recovery scam	A follow-up scam that targets people who have already lost money, promising to get it back for an upfront fee.

Key takeaways

1. Crypto payments are fast and final, which makes them attractive to scammers. Chainalysis estimated more than $17 billion in scam losses in 2025.
2. Rug pulls, honeypots and pump and dumps are most common with new, small tokens. The Squid Game token fell from above $2,850 to almost zero in minutes.
3. Fake investment platforms, often reached through a long online friendship, cause the largest losses. Fake balances and small early withdrawals build trust.
4. Impersonators pose as support staff, exchanges, officials and celebrities. Real support never asks for a seed phrase.
5. Wallet drainers use signed approvals instead of asking you to send funds. Old approvals stay active until removed.
6. Guaranteed returns, urgency, requests for a seed phrase and fees to withdraw are the most common red flags.

Test yourself

Circle one answer for each question. The answer key with explanations is on the next page. You can also take this quiz online at markettalks.info and see your score instantly.

1. Why are crypto payments attractive to scammers?

- A) They are always anonymous and invisible
- B) They are fast, global and cannot be reversed
- C) Exchanges guarantee scammers' profits
- D) They can only be sent at night

2. What is a honeypot token?

A. A token backed by real honey
B. A token that pays high staking rewards
C. A token whose contract lets people buy but not sell
D. A stablecoin pegged to gold

3. What happened to the Squid Game token in November 2021?

A. It was listed on every major exchange
B. Its creators drained the pool and the price fell from above $2,850 to about $0.002
C. The TV show's makers bought all the supply
D. It became a stablecoin

4. In a pump and dump, who usually loses money?

A. The organisers who bought first
B. Late buyers who joined because of the hype
C. The blockchain's validators
D. Nobody, it is risk-free

5. In a pig butchering scam, why do small early withdrawals often work?

A. Because the platform is real
B. To build trust before larger deposits
C. Because of blockchain rules
D. Because the bank forces it

6. Someone in a private message says they are from your wallet's support team and asks for your seed phrase to fix a problem. What is this?

A. Normal support procedure
B. A required security check
C. A typical impersonation scam
D. A software update

7. How does a wallet drainer usually take tokens?

A. By guessing your password
B. By getting you to sign an approval or transaction on a fake site
C. By hacking the whole blockchain
D. By changing the token's price

8. Which of these is a common warning sign of a scam?

A. A platform asking for a fee before you can withdraw
B. Being able to sell a token at any time
C. A well known exchange with public audits
D. A price that moves both up and down

Answer key

1 B

They are fast, global and cannot be reversed

Once a transfer is confirmed it cannot be reversed by a bank or payment company, and funds can cross borders in minutes.

2 C

A token whose contract lets people buy but not sell

The contract blocks selling for normal holders, so the price only appears to go up until the creators cash out.

3 B

Its creators drained the pool and the price fell from above $2,850 to about $0.002

Buyers could not sell, then the creators sold and took the liquidity, and the price collapsed within minutes.

4 B

Late buyers who joined because of the hype

Organisers buy early and sell to the people who arrive after the promotion, leaving them holding a falling coin.

5 B

To build trust before larger deposits

Letting a small amount out makes the fake platform look real, so the victim feels safe depositing much more.

6 C

A typical impersonation scam

Anyone with your seed phrase controls your wallet. Real support teams never ask for it.

7 B

By getting you to sign an approval or transaction on a fake site

The user signs a permission, often presented as claiming an airdrop, that lets the scammer's contract move the tokens.

8 A

A platform asking for a fee before you can withdraw

Demanding a tax, fee or deposit before releasing a withdrawal is a classic sign of a fake platform.

SOURCES

- Decrypt, AI and impersonation drove crypto scam losses to a record $17 billion in 2025 (Chainalysis): https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance, FBI reports 22% rise in crypto fraud losses in 2025: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html
- Cointelegraph, Squid Game inspired crypto scam collapses as price crashes from $2.8K to zero: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-zero

- Cointelegraph, Users not able to sell Squid Game token: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

CONTINUE LEARNING

Up next: Lesson 15 How to Actually Get Started: Exchanges, KYC and Wallets

This lesson is part of the Crypto course at the MARKET TALKS Education Center. Beginner lessons are free, each with a quiz and a downloadable PDF. Intermediate and Advanced lessons are for members.

Education Center
Lessons from first principles to advanced topics

Markets Analysis
Technical and fundamental analysis on major markets

Reports
Bitcoin, Gold, Silver, SPX and more

markettalks.info

Telegram @MARKET_TALKS

For education only. Nothing in this document is financial advice. © 2026 MARKET TALKS. You are welcome to share this PDF unchanged.