10 SIGNS OF A SCAM CRYPTO OR FOREX TRADING WEBSITE

The vast majority of frauds involving cryptocurrency or foreign currency trading, also known as forex, begin on social media or through messaging apps. If someone contacts you out of the blue, or you meet someone online who introduces you to a trading website you've never heard of before, chances are it's a fraud.

It doesn't matter how much scam trading websites claim you will earn, or how easy or risk-free they say it will be, you will lose any money you give them. Besides trolling for victims on social media or messaging apps, here are 10 other telltale signs an online trading platform is a fraud:

1. It isn't registered to trade forex, futures, or options.

Many scam websites offer a mix of crypto assets, forex trading, binary options, futures, or other derivatives. But in order to solicit U.S. customers, entities that trade forex or derivatives must register with the CFTC and be members of the National Futures Association. You can **check registrations at nfa.futures.org/basicnet**.

2. Trades crypto, but not registered as a money service business.

Cryptocurrency trading platforms are considered money service businesses (MSBs) by the U.S. Treasury and must register with the Financial Crimes Enforcement Network (FinCEN). Many states also have requirements for cryptocurrency trading websites to register. To see if a site is registered, **visit fincen.gov/msb-registrant-search**. Registration alone won't protect you from fraud, but most scams involve unregistered entities, people, and products.

3. No physical address, it's clearly fake, or offshore.

If a centralized cryptocurrency or forex trading platform doesn't display a company address, it means the site's owners don't want you to know where they are. If there is an address, **run a street-view map search** to see if the address is real and looks like a legitimate place of business. Avoid companies that don't have a U.S. headquarters. If the trading platform is offshore, you may have little or no protections if something were to go wrong.

4. There is no customer service phone line.

Just like missing addresses, no customer service phone number is a sure indicator of a scam trading platform. Fraudulent trading websites might display messaging-app phone numbers, but these are easy to fake and easy to change. It's also common for scam sites to only offer live chat (often a chat-bot), email addresses, or "contact us" web forms. But when scams are exposed, the websites disappear, along with any way of communicating with them.

5. The website's age doesn't match its claims.

Look up domain registrations at lookup.icann.org. The search results will tell you when the web address was created. If the company claims to have been around for several years, but the domain registration is only a few weeks old, you'll know it's a scam. Other trading websites may claim to have millions of customers or conduct billions of dollars in trades, but such claims would be highly unlikely if the site were only weeks or months old. Also, be suspicious of websites that look or sound similar to other well-known brands, or that don't end with dot-com.

6. The website won't accept transfers from your bank.

Scam trading platforms won't connect to legitimate financial institutions because they'll be discovered as frauds. Instead, the scammers will walk you through how to convert dollars to cryptocurrency on a legitimate trading platform first, and then ask you to transfer the crypto to them. Remember, blockchain transactions don't have anti-fraud security systems like ACH bank transfers or credit card purchases. Instead, they obscure the scammers' true identities and are irreversible. By the time you discover your money's been stolen, it's too late.

7. Investment returns are based on how much you invest.

Many fraudulent trading sites offer "investment plans" that promise returns of 50, 75, 100, 200 percent or more depending on how much you give them. When it comes to investing in crypto assets, there are no risk-free investments or guaranteed returns. These kinds of plan upgrades are ploys to coax victims out of more money.

8. Broken links, poor spelling, and bad grammar.

Scam sites generally have short life spans. As soon as a fraud is discovered, the website will disappear only to pop up again under a different brand and web address. This means scam sites are often put together in a hurry. Criminals will often use translation software to run their scams in multiple countries. Be suspicious if you spot misspelled words, obvious grammatical errors, odd syntax, or other such mistakes. Likewise, broken links and pages "under construction," are common on scam sites.

9. Winner of so many awards you've never heard of.

Scam sites like to try to build credibility by showing off awards and trophies that read "Best Site," "Customer Satisfaction," or something equally generic. If you've never heard of the awards and it's not clear who gave them, don't trust them.

10. Raving testimonials.

Fake testimonials are another way scam websites try to build trust. Be critical of customer reviews that appear on the website. Instead, run a search using the site's domain name along with the words "scam," "fraud," or "reviews" to see if previous users have posted warnings. Also, check websites that detect or track frauds, like **cftc.gov/redlist**.

Report suspicious sites:

Visit **cftc.gov/redlist** to report unregistered websites offering forex or derivatives trading.

To report fraud, contact:

- The CFTC at **cftc.gov/complaint**
- The FBI's Internet Crime Complaint Center at **IC3.gov**
- The Securities and Exchange Commission at **https://www.sec.gov/tcr**
- The Federal Trade Commission at **reportfraud.ftc.gov**
- Your state regulator, attorney general, and local law enforcement

Learn more at: **cftc.gov/LearnAndProtect**

Commodity Futures Trading Commission
1155 21st Street NW
Washington, DC, 20581
cftc.gov | 866-FON-CFTC (866-366-2382)

education@cftc.gov @CFTC @CFTCgov youtube.com/CFTC