







SPOTLIGHT: Cryptocurrency Scams



While there are legit uses for digital currency, cryptocurrency (crypto) is a popular payment method used by scammers. Crypto is not backed by the government and is not insured like money deposited into a bank. Investments and payments involving crypto do not come with the same legal protections if something goes wrong. It's like sending someone cash and payments typically are not reversible.

While the stories scammers use may vary, the **red flags of a crypto scam** remain the same:

-  **Scammers try to gain your trust** by pretending to be from a well-known business, law enforcement or another government agency.
-  **There's a problem or a prize.** You missed jury duty, your bank account is in danger, there's a great investment opportunity or you won the lottery!
-  **You must act NOW!** Scammers want you to act before you have time to think. They often stay on the phone with you for hours and walk you through the payment process from withdrawal of cash to deposit into the ATM. Their goal is to prevent you from talking to someone you trust about what's going on.
-  **Only scammers insist you can only pay with crypto.** No legitimate business or government agency is going to demand payment in crypto.

How to Avoid Crypto ATM Scams

Scammers may call or send you messages pretending to be financial institutions, government agencies or real businesses. The claims often involve bank accounts that are frozen, a missed court date or that you owe money.

- **Never withdraw cash in response to an unexpected call or message.** Only scammers will tell you to do that. They often instruct you to lie to bank employees about why you're making the withdrawal.
- **Don't believe claims** that you need to use a cryptocurrency ATM to protect your money or fix a problem.
- **If you think there's a real problem, verify the story.** Use a phone number, website or app you know is real. Don't use the contact info provided by the caller or that's in the message.



Think something is suspicious?

Stop and talk to a friend, family member or neighbor about what happened.

Consumers can report scams to SCDCA by either calling (800) 922-1594 or visiting consumer.sc.gov and click the How Do I... button, then Report a Scam.

Common Crypto Scams



Investment Scams

These fake investment opportunities often promise huge returns. An online love interest may encourage you to invest or you may be contacted by an “investment manager” out of the blue.

- **Research before you invest.** Do an online search of the name of a digital currency, the investment company, and agent involved.
- **Stick to investment apps in your device’s official app store.** Do not use unfamiliar sources to download apps or software.
- **Be wary of promises of big returns.** No investment is guaranteed to make money.
- **Don’t mix** online dating and investment advice.

Imposter and Giveaway Scams

Online videos, social media posts or direct messages may claim to be from a celebrity, influencer or well-known businessperson. Scammers promise to match or multiply the money you send them. In the end, all they do is steal it.

- **Search online** for the celebrity’s name plus the word “scam” to see if others are getting the same messages.
- **If you see a video, post or message claiming to be a celebrity asking for crypto,** report it to the social media platform you’re using.
- **Never send money to someone that you haven’t met** in real life.

Phishing Scams

Crypto payments aren’t the only targets for scammers. They also want access to crypto wallets. Scammers use a variety of schemes to trick people into clicking on links to fraudulent websites that ask for credentials to access their wallet.

- **Do not click on links or call numbers** listed in an unexpected message.
- **Do not reply to messages** asking for login credentials or account details.
- **Think the message may be legit? Do not use the contact info in the message.** Look up customer support numbers or website addresses yourself.

Blackmail Scams

Scammers may send emails, text messages or even mail to your home claiming that they have embarrassing or compromising photos or videos of you. The claims are often vague with an intention to scare the victim into providing cryptocurrency payments. If you receive these types of messages, contact the FBI immediately by going to [fbi.gov/contact-us](https://www.fbi.gov/contact-us).