Avoid Cryptocurrency Scams

Be on the lookout for:

- Guarantees of large returns on investments.
- Fake testimonials—even celebrity endorsements and testimonials are easily faked. Be sure to conduct thorough research before purchasing cryptocurrency or using an exchange.
- Promises of free money—either in cash or cryptocurrency. Free money promises are a huge red flag.
- Big claims of benefits with no details or explanations.
- Blackmail attempts—scammers will often send emails saying they have embarrassing or compromising material to share about a victim and threaten to make it public unless a cryptocurrency payment is made. Don't do it—report the extortion to the FBI immediately.
- Social media messages—if you receive a text, tweet, call, email or social media message prompting you to send cryptocurrency, it's a scam.

Report Crypto Scams

Floridians can report cryptocurrency scams to the Attorney General's Office by calling **1-866-9-NO-SCAM** or visiting **MyFloridaLegal.com**.

Florida Attorney General's Office
Scams at a Glance:

Cryptocurrency Scams

Visit MyFloridaLegal.com to find consumer tips or to file a complaint. By remaining vigilant and informed, savvy consumers can help us build a Stronger, Safer Florida.

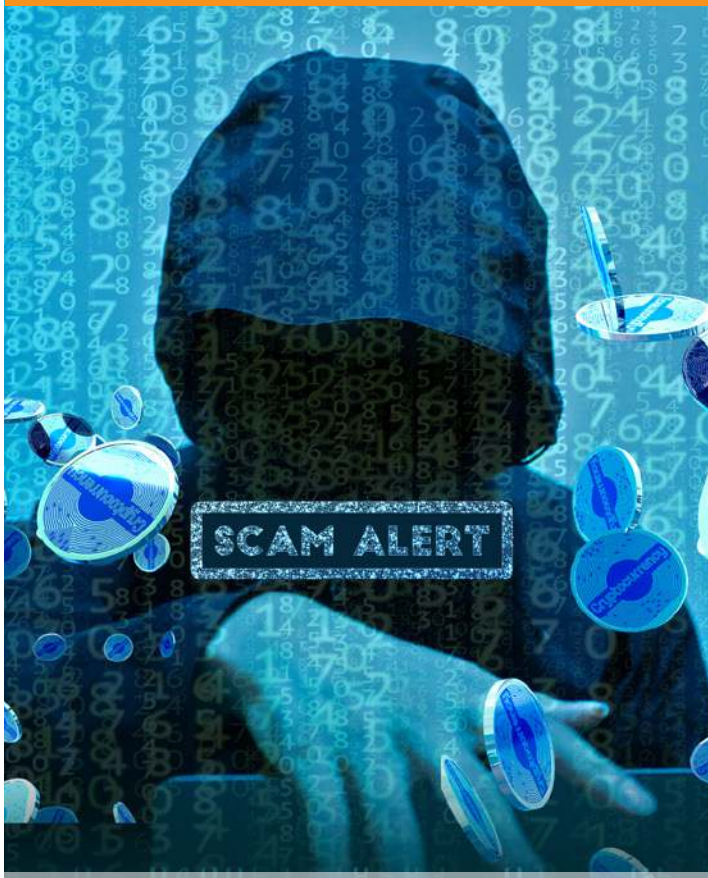
Report fraud by calling
1-866-9-NO-SCAM
(1-866-966-7226)

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Attorney General Ashley Moody
Office of the Attorney General
PL-01 The Capitol
Tallahassee, Florida 32399
MyFloridaLegal.com

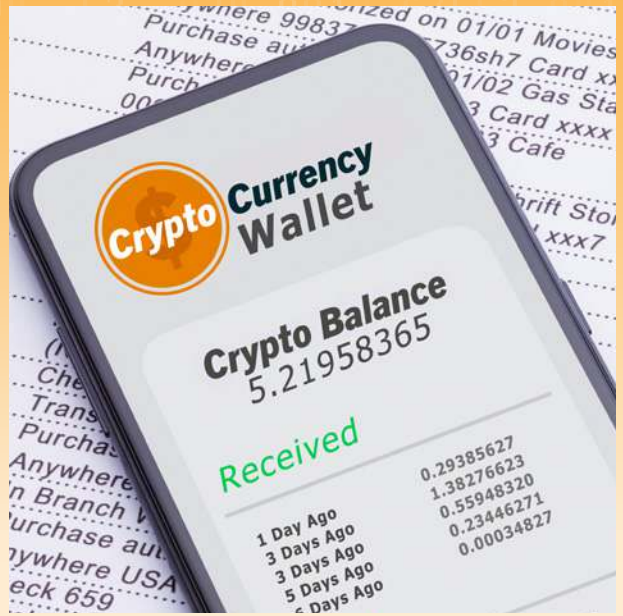
Scams at a Glance:

Cryptocurrency Scams



OFFICE OF
ATTORNEY GENERAL
ASHLEY MOODY
Stronger, Safer Florida

What is Cryptocurrency?



Cryptocurrency is a type of digital or virtual currency designed to be used over the internet by private exchanges. Being a virtual currency, there is no physical coin or bill, and consumers must use a service, called an exchange, if they wish to convert cryptocurrency to U.S. dollars or other fiat currency. Bitcoin and Ethereum are well-known cryptocurrencies, but there are many different types of cryptocurrencies, and new ones are continuously being created.

Cryptocurrency can be bought through an online exchange platform and stored in a cryptocurrency wallet, which can take many forms—from mobile apps, paper wallets, online wallets or a hardware wallet (which may look like a USB stick). Some investors earn cryptocurrency through a complex process called "mining," which uses computer equipment to assist in completing cryptocurrency transactions in exchange for a small amount of cryptocurrency.

Cryptocurrency may be used as payment in certain transactions, while others buy cryptocurrency as an investment, hoping the value increases.

Cryptocurrencies are typically offered by private exchanges and not backed by the federal government or a central bank. If cryptocurrency is stored with a third party that goes out of business or is hacked, the government has no obligation to help return the lost value. Unlike paying with a credit or debit card, if a consumer attempts to dispute a purchase, cryptocurrency exchanges typically do not have a process for returning lost funds.

Payments made with cryptocurrency are typically not reversible. Once a cryptocurrency transaction takes place, the buyer can usually only get the cryptocurrency back if the seller returns it.

Investors should know that taxes must be paid on gains made from cryptocurrency investments.

Scammers are always finding new ways to steal victims' money. Because cryptocurrencies have quickly become popular, scammers may prey on the unsuspecting.

Types of Cryptocurrency Scams

Investment and Business Opportunity Scams: Scammers may pose as a company promising consumers that they can earn a lot of money in a short time and asking consumers to pay in cryptocurrency for the right to recruit others into a program. Other scammers start with unsolicited offers from purported "investment managers" who promise to help the consumer increase their money if the consumer places the cryptocurrency they bought in a specific account. Once the victim logs in to this supposed "investment account," they find that they can't withdraw their money unless they pay fees.

Bait-and-Switch Investment Scheme: These schemes defraud victims by first helping them earn profits, then encouraging the victims to transfer funds to a fraudulent trading platform where the money is stolen. After convincing the victim to invest with the scammer, the scammer will typically prompt the victim to establish an account with a legitimate cryptocurrency exchange. Afterward, victims are directed to transfer earnings from the legitimate platform to another cryptocurrency website that is a fraudulent, imposter platform. These fraudulent websites may only operate for a short time and then victims are blocked from accessing the phony investment accounts.

Rug-Pulls: Scammers may create a new cryptocurrency and fraudulently encourage victims to purchase it as an investment despite having little actual value. As the price of that cryptocurrency increases, the scammers then sell their holdings and take a profit while victims are left with a cryptocurrency worth far less than what they invested.