Oppenheimer & Co. Inc.
Spencer Nurse
Managing Director - Investments
500 108th Ave. NE
Suite 2100
Bellevue, WA 98004
425-709-0540
800-531-3110
spencer.nurse@opco.com
https://www.oppenheimer.com/spencernurse/

Watch Out for Crypto Scams

All investing involves risk, including the possible loss of principal, and there is no guarantee that any investment strategy will be successful.

Cryptocurrencies are not traditional investments; they are highly speculative instruments, carry a significant amount of risk, and are not suitable for all investors.

Cryptocurrencies are not typically subject to the same reporting and data integrity requirements that apply to more traditional investment products. The IRS is treating cryptocurrency as an asset subject to capital gains taxation rather than as a currency.

As interest in cryptocurrency takes off, scammers have come out in droves to cash in. According to the Federal Trade Commission (FTC), more than 46,000 people reported losing over $1 billion in crypto scams from January 2021 through March 2022. Losses in 2021 were nearly 60 times the losses in 2018.[1]

Many scams aren't unique to cryptocurrency. They are variations of financial scams that have been around for years, but still manage to ensnare many new victims. Crypto scams may be especially lucrative and easy to perpetrate because of investor inexperience, exploitable platforms and software, and the constant influx of new currencies and opportunities.

Most of the safeguards that help protect other financial systems aren't in place with crypto, and currently there is very little regulation or legal recourse. To make matters worse, crypocurrency transactions aren't reversible. If you decide to invest in cryptocurrency, it's extremely important to try to protect yourself against scams and the possibility that both your money and your identity could be stolen. Here are some red flags to watch out for.

An amazing opportunity

Words like "guaranteed" or "once in a lifetime" should set off alarm bells that the opportunity is too good to be true. It might be offered by someone you met online — often through social media — or through a dating app or site (a classic "romance scam"). Over time, you grow to trust this person, and eventually you're told you can get big returns by investing in a cryptocurrency opportunity. You send money, and at first you seem to get a windfall — on paper. But your account isn't real. Before you know it, you've lost everything, and the person you trusted disappears.

Sometimes a real person you trust unwittingly pulls you into a scam like this. Without realizing it, a family member, friend, or colleague has been set up by a scammer to bring other victims into the fold. Once many people have sent in money, the scammer vanishes with everyone's funds.

Extensive promotion

Some scams try to capitalize on investor desire to get in on the ground floor of a new crypto project. One scam called the "rug pull" may start with a fraudulent developer who easily and cheaply creates tokens or coins and initially sells them at a low value on a decentralized platform. After the developer hypes up the opportunity to make it look legitimate, people begin to buy and the value goes up sharply, but ultimately the developer "pulls the rug out" by abandoning the project and running off with the funds. The tokens or coins are now worthless.

A related scheme called "pump and dump" involves insiders who quickly pump up a new or low-value cryptocurrency asset by heavily promoting it. Then, as outside buyers jump on board and drive prices higher and higher, insiders sell/dump their holdings at peak value, leaving outside buyers scrambling to minimize their losses by selling as the value plummets.

Perpetrators use popular channels and messaging apps to promote themselves and their opportunities, and sometimes hire social media influencers who receive financial incentives for marketing a product. Many perpetrators use screen names to remain anonymous, while others promote themselves to build credibility within crypto communities.

Scammers may advertise giveaways on social media, promising that if you enter and send cryptocurrency to a certain address, you'll get a great prize or multiply the amount you send in. These heavily promoted scams are often supposedly sponsored by celebrities or famous crypto or tech gurus. Unfortunately, your money will be the only thing given away.

There's a problem with your account

Perhaps you receive an email or see an onscreen pop-up telling you there is an issue with your account, such as a security problem or an unauthorized purchase. Although it seems to come from a reputable source like your bank or a business, it links to a page set up by a scammer to steal your

Don't be ashamed to admit if you become the victim of a scam — you're not alone. Unfortunately, if you lose money, it's unlikely that you'll get it back. But there are steps you should take that may help catch the perpetrators and keep others from losing money. The FTC suggests that you report fraud and other suspicious activity to the following:

- ***FTC at ReportFraud.ftc.gov***
- ***Commodity Futures Trading Commission (CFTC) at CFTC.gov/complaint***
- ***U.S. Securities and Exchange Commission (SEC) at sec.gov/tcr***
- ***Internet Crime Complaint Center (IC3) at ic3.gov***
- ***Cryptocurrency exchange company you used to send the money***

credentials or financial information. Or you receive a call or find a number online for a "customer support center" that will direct you to a person who will download malware onto your computer under the guise of helping you resolve your issue.

Phishing attacks are very common, and scammers are counting on the fact that people unfamiliar with buying and selling crypto will easily fall for them. Never give anyone remote access to your computer or give out personal information, including passwords, keys, or two-factor security codes that could give hackers access to your digital crypto wallet. Legitimate sites will not ask you for this information.

Don't click on a link you randomly receive (even if it seems to come from a business or person you know) and scrutinize a website address that you are accessing directly to make sure it is the right one before entering your credentials. And never log into a cryptocurrency exchange unless you are certain you are on the correct site. Counterfeit trading platforms mimic the appearance of legitimate sites and use misleading domain names.

Must pay with cryptocurrency

If an institution is credible, there's no reason that it will only accept cryptocurrency and not traditional forms of payment. Scammers may impersonate others, including government agencies, charities, well-known businesses, and utility companies, or even pose as someone you know. A scammer may ask for payment in Bitcoin and make it easier for you to send it by providing a quick response (QR) code that can be scanned at a Bitcoin ATM. The Bitcoin comes out of your digital wallet and goes directly to the scammer.

Threatening messages

A scammer might try to blackmail you by sending an email or a message that threatens to reveal compromising information such as photos, videos, or personal data unless you pay them in cryptocurrency. This is known as an extortion scam. Report this to the authorities and don't pay anything.

Ten tips to help protect your money

- Learn about crypto and stay up-to-date on evolving scams.
- Don't fall victim to the fear of missing out. When you think you need to act quickly, you may ignore warning signs.
- Ignore social media ads for cryptocurrency. They are often used to promote fraudulent investment opportunities.
- Don't be fooled by buzz around an opportunity; it does not mean it's legitimate. Scammers rely on hype to pump up perceived value that most people will never benefit from — watch out for skyrocketing value that seems to come out of nowhere.
- Research crypto promoters and backers and check their track records.
- Type in the URL of a reputable site directly and double check it before logging in. Google searches may lead to fake copycat sites because scammers pay to come up at the top of search results.
- Know how to spot fake apps. Read app reviews, number of downloads, and research the developer. Watch out for spelling and grammar mistakes.
- Never share your recovery phrase (seed phrase) or private keys (long letter and number codes) that can unlock your crypto wallet.
- Use layered security such as strong, unique passwords and two-factor authentication to help protect your accounts and your computer, smartphone, and other technology you use.
- Never invest more than you are willing to lose.

1) Federal Trade Commission, June 2022