Investor.gov
U.S. SECURITIES AND EXCHANGE COMMISSION

Protect Your Money
How to Avoid Investment Scams

New and developing technologies – from social media to mobile trading apps to artificial intelligence – increasingly influence how we invest. While these technologies can provide many benefits to investors, they also create opportunities for scammers. Here are some red flags of investment fraud to keep an eye out for:

- **Promises of High Investment Returns with Little or No Risk**
  Scammers often promise to help you get rich – with little or no risk. They can make an investment scam seem appealing with fancy websites, videos, or images of lavish lifestyles. But there's no such thing as high guaranteed investment returns, and every investment involves risk.

- **Pressure to Act Now**
  Fraudsters may create a false sense of urgency to pressure you to invest. They may claim the deal is only available to a limited number of investors, or give you a short deadline to invest. They may claim to have inside information and tell you to act before others find out. Take your time to research on Investor.gov before deciding to invest.

- **Fear of Missing Out or FOMO**
  Scammers may pitch an investment as a "can't miss" opportunity. They may say that a lot of people are investing to pressure you to jump on the bandwagon. They also may try to tap into your desire to get in on the ground floor of the latest technology, product, or growth industry, like crypto assets or artificial intelligence (AI).

PRO TIP: Ask questions and research investment opportunities so you know what you're investing your hard-earned money into.

- **Building Trust**
  Relationship investment scams often start with a social media message or wrong number text message. Scammers hide their true identities and attempt to build trust slowly over time. Once the scammer develops a relationship with you, they may offer bogus investing recommendations or convince you to "invest" your money and then scam you. For example, you may think you're buying into a crypto asset investment when you're actually just sending money directly to fraudsters' wallets. No matter how trustworthy someone might seem, don't make investment decisions based on the advice of anyone who makes unsolicited contact with you online or through a messaging app or text message.

- **Using a Common Bond**
  Scam artists may claim to have something in common with you in the hopes you'll invest with them. They may be or claim to be a member of your same faith community or racial or ethnic group. Similarly, a scammer may convince someone in a group you trust to invest in a scam. Don't let your guard down because someone you have a common bond with told you about the investment opportunity—research the investment and the person offering it before you invest.

- **Impersonating Investment Professionals**
  Sometimes scammers impersonate registered investment professionals. They may set up an account name, profile, or handle designed to mimic a particular real individual. They may create a webpage that uses the real firm's logo, links to the firm's actual website, or uses the name of an actual person who works for the firm. Verify that you are communicating with an investment professional and not an imposter.

PRO TIP: Conduct a background check of any investment professional on Investor.gov to make sure they are currently licensed or registered. Find their contact information through Form CRS.

- **Fake Testimonials or Credentials**
  Some scammers pay people to post fake online reviews or appear in videos falsely claiming they got rich from an investment. Scammers may make up or exaggerate their credentials, claiming to have experience or a certification. Don't invest with someone just because the person claims to have an impressive background or track record.

- **Celebrity Endorsements**
  Celebrities can be lured into participating in an investment scam or the celebrity may not have actually endorsed the investment. Even if the celebrity endorsement and the investment opportunity are genuine, the investment may not be a good one for you.

- **Suspicious Payment Methods**
  If you are required to pay for the investment in one of the following ways, be wary of fraud:
  - Using a credit card, gift card, overseas wire transfer, Peer-to-Peer Payment App (P2P) or crypto assets;
  - Wiring money or writing a check to an individual;
  - Sending money to a different company than one you thought you were investing with;
  - Sending payment to a suspicious address (a P.O. Box or virtual address); or
  - Noting that the payment is for a purpose unrelated to the investment (for example, luxury watches, goods, or furniture).

Protect Your Personal Information. If a stranger contacts you through social media, text message, or phone call with an investment opportunity, do not share any information relating to your personal finances or identity. Do not share your bank or brokerage account information, tax forms, credit card numbers, Social Security number, passport information, driver's license information, birthdate, or utility bill details. Scammers may use this information to steal your money or identity.

Do not provide your phone number or email address to someone you don't know. They could be a scammer who may sell your contact information to other fraudsters.

WHERE CAN I GET MORE INFORMATION?

- Visit **Investor.gov** to learn more.
- If you have a complaint or question about your investments, visit **help.sec.gov**.
- If you suspect securities fraud, report it to the SEC at **sec.gov/tcr**.

PAID FOR BY THE U.S. SEC
PUB # 192 (3/2026)