

Investment scam criminals will usually get in touch after you've shown interest in their fake firm on social media or through a Google search, but they can also cold call people out of the blue. The criminal appears professional and may offer investments in things like cryptocurrencies, carbon credits, property, land, gold, or wine. Here are the warning signs to look for that can help you to spot a possible investment scam.

- 1** An unsolicited email, private message or cold call offering any form of investment. Cold calling to sell you shares or investments is illegal.
- 2** 'Limited time only' offers that don't give you enough time to consider the investment.
- 3** Company names which sound familiar or have a slight variation to a legitimate company that's registered with the Financial Conduct Authority ('clone' companies).
- 4** A pushy and persistent sales technique.
- 5** A company, or a broker, that pushes you to keep your investment secret, even from your bank. This is to avoid detection.

## How to protect yourself from investment and cryptocurrency scams

- ✓ **Make the right checks** – firms providing regulated financial services must be authorised by the FCA. You can check whether they are authorised on the FCA Register.
- ✓ **Avoid clones** (fake companies that look genuine) - use the contact details on the FCA Register, not the contact details you've found on an online advert, or that the firm gives you when they make contact.
- ✓ **Don't assume it's real** – professional-looking websites, adverts or social media posts don't always mean that an investment opportunity is genuine. Criminals can use the names of well-known brands or people to make their scams appear legitimate.
- ✓ **Stay in control** – avoid uninvited investment offers, whether made on social media or over the phone. If you're thinking about making an investment, thoroughly research the company first and consider getting independent advice.
- ✓ **Never** download software or apps that allow someone remote access to any of your devices, including your computer, laptop, tablet or phone.
- ✓ **Don't allow** anyone to set up a cryptocurrency wallet, upload ID documents or manage investments on your behalf remotely.



**Remember: If something sounds too good to be true, it's probably a scam.**

### Be ScamSmart

The FCA has created their [ScamSmart online tool](#) to help consumers identify if their investment is a scam or not. Answer 4 questions with drop downs for multiple choice and get a clear picture on the potential investment and the potential risks.