



**POLICE**  
**SCOTLAND**  
**POILEAS ALBA**

# Cybercrime Harm Prevention Team

## Cryptocurrency Scam Guidance

## OFFICIAL



Cryptocurrency related investment scams continue to be prevalent across various social media platforms, which can result in significant financial loss (i.e. lifesavings, pension etc.) and in some cases may lead to increased risk of causing mental health issues such as depression and anxiety.

During lockdown cases of cryptocurrency investment scams increased. It is believed that the number of victims falling for this may be significantly higher as it is suspected many cases go unreported to Police.

The best way to protect victims is to encourage them to be careful and selective about the websites they visit and whom you engage with online, especially when considering to invest large amounts of money - [Cryptoassets | FCA](#)

Below are some details of the potential signs of this type of crime, along with advice and support that is available to those who may have been affected.



## **What is Cryptocurrency?**

Cryptocurrencies are digital currencies that are known for their market volatility so the value of investor's assets go up and down quickly. Criminals can take advantage of the unregulated nature of cryptocurrencies to scam consumers. Cryptocurrency can be traded or exchanged online to buy from people or companies who accept this form of payment.

Cryptocurrency investments are often made via currency exchange platforms. These are websites where you can buy, sell or exchange cryptocurrencies for other digital currency or traditional currency like GBP or US dollars.

Criminals benefit from the volatility of the cryptocurrency markets, pressuring people to make decisions without due diligence or consideration.

Some people who have been scammed don't realise for some time. They may make multiple or regular payments to the criminal and only realise when they try to withdraw their money from the 'scheme'.

If something goes wrong with a cryptocurrency investment you are unlikely to get your money back, because they mostly aren't covered by the UK's Financial Services Compensation Scheme.

The National Cyber Security Centre (NCSC) published figures which showed that as of March 2022, 11 million phishing scams were reported which resulted in 78,000 scams being removed – Fake cryptocurrency investment lures make up more than half of all online scams detected.



## **Who is behind this crime?**

This type of crime can be carried out by lone individuals or organised crime groups who are maybe based overseas. For perpetrators it's a low risk way to make money, and they can reach a wide range of individuals easily online. The perpetrator(s) is gambling that enough people will respond so that their scam is profitable.

## **Examples of Cryptocurrency Scams**

### *Celebrity Endorsements*

Arun saw a 'celebrity endorsed' social media post advertising the promise of big returns on Bitcoin. He contacted the company and following a phone call with a "trader" was convinced to make a payment of £300. After logging into his trading account on the website, he saw his investment increase. Arun continued to invest more money following pressure from another "trader" from the company and was persuaded to take out a loan sourced by the criminal. Arun only realised it was a scam when he was unable to access his account to withdraw his money or contact the company.

### *Mining scheme scam*

Emma had owned cryptocurrency for a few years and the value of her investment had gone up and down. Some of Emma's friends got into crypto mining, and they said it was a great opportunity to make passive income on the side, without much effort or knowledge.

Having joined a mining group on social media to find out more, Emma was contacted by a 'successful cryptocurrency trader' who offered her fixed returns for an investment in a mining programme. Emma transferred some of her cryptocurrency to the trader, but she realised she had fallen for a scam when the trader became uncontactable.

## **OFFICIAL**

### *New coin scam*

Jadon had heard loads about cryptocurrency traders putting money into Bitcoin years ago and making a fortune. The influencers he followed on social media encouraged everyone to get involved. He went online to do some research and concluded he needed to invest in a new coin to make the most money.

Jadon saw an advert for a new coin and found it on a brokerage site. The advert said he could triple his money in months and that the makers of the coin had an office in London. Jadon put most of his savings into the coin as he wanted to maximise his returns, and he was told he wouldn't lose anything as he was buying in at the start. It only dawned on Jadon that he had been a victim of a scam when his account stopped working and he was asked to make another payment to access his funds.

## **How to spot a Cryptocurrency Scam?**

- You see adverts on social media, sometimes celebrity endorsed, offering unrealistic returns on investments
- You're contacted by phone, email or social media about an opportunity using aggressive techniques and incentives to buy before certain deadlines
- You're told your buying in at the perfect time. You may be offered a high return on your investment with apparently little or no risk
- You're pressurised into making a decision with no time for consideration
- You're told the investment opportunity is exclusive to you

## **How to protect yourself?**

- **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 individuals to make their scams appear legitimate.
- **Don't be rushed or pressured into making a decision** – A genuine bank or financial organisation won't force you to part with your money on the spot. Always be wary if you're pressured to invest quickly or promised returns that sound too good to be true.
- **Stay in control** – Avoid uninvited investment offers, especially those over cold calls. If you're thinking about making an investment, get independent advice and thoroughly research the company first.

## OFFICIAL

### Advice for victims of investment scams;

If you or someone you know has been a victim of an investment scam, don't feel embarrassed, help and support is available.

1. **Contact the Police immediately.** The police will take your case seriously, will deal with it in confidence.
2. **Contact your Bank immediately.** Ensure all pending/future transactions are cancelled.
3. **Report to Financial Conduct Authority (FCA).** Phone their Consumer Helpline on 0800 111 6768 or using their [report form](#).
4. **Don't communicate further with the criminals.** Take screen shots of all your communication. If they contacted you via Social Media, suspend your account (but don't delete it) and use the online reporting process to report the matter to Instagram, Facebook etc. Deactivating your account temporarily rather than shutting it down will mean the data are preserved and will help police to collect evidence. Also, keep an eye on all the accounts which you might have linked in case the criminals try to contact you via one of those. If you were contacted by email, you can forward the email to the NCSC's Suspicious Email Reporting Service (SERS) on [report@phishing.gov.uk](mailto:report@phishing.gov.uk), and then delete it.
5. **Preserve evidence.** Make a note of all details provided by the offenders, for example; the email address, number or social media account that you have been contacted from; the Western Union or MoneyGram Money Transfer Control Number (MTCN); any bank account details; cryptocurrency wallet, etc.
6. **Block and report.** Report them to the platform they have contacted you on and block the individual on the platform / in your contacts.
7. **Don't panic.** It can be a very distressing situation for some people but there is lots of help, advice and guidance out there.

## OFFICIAL

DO NOT DELETE ANY CORRESPONDANCE

### Further help and support

If this has happened to you or someone you know please talk to a family member, friend, colleague or line-manager that you trust. Please check out our useful links section with more support channels available along with guidance and links to trusted partner agencies.

### Links

Support and Wellbeing:

- [Home | SAMH](#)

Further information, advice and guidance:

- [Report a scam email - NCSC.GOV.UK](#)
- [Report a scam website - NCSC.GOV.UK](#)
- [Report a scam advert - NCSC.GOV.UK](#)
- [Report a scam to us | FCA](#)
- [Financial Conduct Authority | FCA](#)
- [Victim Support Scotland](#)