LLOYDS BANK

PRESS RELEASE

Lloyds Bank issues urgent warning over rising threat of crypto scams

- **Crypto scams have surged by 23% this year as fraudsters target younger investors**
- **Victims losing £10,741 on average, more than any other type of scam**
- **Two-thirds of investment scams now estimated to start on social media**
- **Findings highlight importance of investing through trusted, genuine companies**

A growing number of British investors risk being defrauded by a wave of fake adverts posted on social media, according to a new a warning issued by Lloyds Bank.

The number of cryptocurrency investment scams reported[1] by victims so far this year has risen by 23%, compared to the same period in 2022.

The average amount lost by each victim of a crypto investment scam is £10,741 (up from £7,010 last year). This is more than any other type of consumer fraud (such as romance scams or purchase scams).

Remarkably, the analysis found that 66% of all investment scams start on social media – with Instagram and Facebook the most common sources. This includes a mix of bogus ads, fake celebrity endorsements, and targeting through direct messages.

The scourge of crypto scams

The organised criminal gangs behind scams are constantly evolving their tactics to exploit new trends and trick more victims into parting with their cash.

Over recent years they've widened their net to target younger investors, who are often tempted by the supposed 'get rich quick' promise of cryptocurrency trading.

The most common age range for crypto scam victims is 25 to 34 year olds, who make up a quarter of all cases.

Would-be crypto investors typically make an average of three payments before they realise they have been scammed, taking around 100 days from the date of the first transaction before they report it to their bank. By this point, the money is usually long gone, and impossible for the bank to reclaim.

Revolut is the most common recipient of Faster Payments made by crypto investment scam victims at Lloyds Banking Group (though is not always the end destination of the funds, which may then be sent on elsewhere).

The warning signs of a crypto scam

While even genuine investment in cryptocurrencies is highly risky – with the FCA stating people should be prepared to lose all their money[2] – ultimately that is an individual choice for each investor.

But it's important to remember that fraudsters will go to great lengths to convince investors that they are the real deal. This can include setting up fake companies, social media profiles and websites to clone real firms. They may even produce investment literature that looks professional.

There are two main ways that fraudsters snare the cash of would-be investors through crypto scams:

The illusion

This is where there is no genuine investment platform or cryptocurrency involved. The fraudster, typically posing as an 'investment manager', promises that any payments made by the victim will be invested on their behalf, often with the promise of huge returns.

Sometimes the victim will be shown a fake investment account, suggesting that the funds are already making a profit, or a small amount of money will be transferred back into their bank account.

However, both tricks are just a way of duping the victim into thinking the investment is real and encouraging them to part with even more money.

There is no investment account, no genuine crypto holding, and once the fraudster has taken as much money as they can, they will simply disappear.

The takeover

In some cases there will be an actual investment account held in the victim's own name and registered with a legitimate platform, such as Coinbase or Binance.

Either the victim will be shown how to set this up, or it will be opened on their behalf, as many trading platforms carry out limited checks when opening new accounts.

Once funds have been deposited, victims may be tricked into handing over their account login details, or passing control of their digital wallet over to the fraudster.

They might also be directed to transfer cryptocurrency from within their own account to another digital wallet, which is under the control of the fraudster.

Crypto payments and other types of scam

It's important to remember that cryptocurrency payments can also form part of other types of scam, such as romance scams or impersonation scams. If someone asks for a payment using cryptocurrency, that should immediately set alarm bells ringing.

Liz Ziegler, Fraud Prevention Director, Lloyds Bank, said:

"Investing can be a great way to make money, but you need to make sure your money is going to a trusted, genuine company. Crypto is a highly risky asset class and remains largely unregulated, which makes it an attractive area for fraudsters to exploit. If something goes wrong, you're unlikely to get your money back.

"Predictably, social media platforms are the main breeding ground for this type of scam, with a mix of bogus ads, fake endorsements and cloned accounts being key to fraudsters' methods. It's time these tech firms took responsibility for protecting their customers, stopping scams at source and contributing to refunds when their platforms are used to defraud innocent victims."

Top tips to stay safe from crypto investment scams:

- **Beware of social media:** Fraudsters often put adverts for scam crypto investments on social media. They can also send offers by direct message. They will promise returns that you can't get elsewhere or make claims about 'guaranteed' profits. If you're contacted out of the blue about an investment, it's likely a scam.

- **Make sure it's genuine:** Fraudsters can easily set up fake companies, social media profiles and websites to clone real firms. Use the FCA website to find genuine contact details for a company and check for warnings about fake firms. Always do your own research or seek professional financial advice.

- **Check for warnings:** Marketing of crypto is now regulated, which should make it easier to spot genuine crypto ads. According to the FCA, whenever you invest in crypto you should see prominent warnings about the risk of losing your money, and you shouldn't be offered any free gifts to join or refer a friend bonuses.

- **Keep it to yourself:** Never share the log in details for your investment account or your private cryptocurrency keys with anyone else. A legitimate firm would never ask you for this. Remember if you transfer funds to another account that isn't in your name, you have lost control of your money.

- **Protect how you pay:** If you pay by bank transfer and it's a scam, it's very hard to get your money back. Fraudsters might ask you to pay an account in a different name to the company you are meant to invest with. If the names don't match, it's a sign of a scam. Paying by card always offers the greatest protection.

Notes to editors

Methodology

1) Figures based on analysis of relevant investment scams reported by Lloyds Banking Group customers (including Lloyds Bank, Halifax and Bank of Scotland) between January and September 2023 compared with the equivalent period last year (January and September 2022). Source data based on transaction details and the testimony of victims at the point they reported the scam to the bank, including where cryptocurrency was stated as the investment category. Figures should be regarded as indicative of key trends.

Additional sources

2) Financial Conduct Authority: Investing in crypto | FCA

Media contacts:

Gregor Low: gregor.low@lloydsbanking.com / 07500 078 879

Lynsey Cheshire Willis: lynsey.cheshire-willis@lloydsbanking.com / 07595 124 294