POLICE SCOTLAND
POILEAS ALBA

Cryptocurrency Scam Guidance

Cybercrime Harm Prevention

Police Scotland
04.03.25

What is Cryptocurrency?

Cryptocurrencies are digital currencies or digital money. They don't exist physically like the coins and cash, but instead they're completely virtual. Although they are virtual, cryptocurrencies do hold value. They can be stored in a 'digital wallet' on a smartphone or computer, and owners can send them to people to buy things.

The exchange of these digital currencies are known as 'peer-to-peer' transactions, which simply means there are no banks, or other third parties involved. Instead, every transaction ever made is recorded on a huge database known as a blockchain - think about it like a massive spreadsheet.

Each transaction made is represented by a block which is added to the larger chain, hence the name blockchain, and all the transactions remain in the blockchain forever. A blockchain isn't based in a central location, but is distributed among a large network of computers which is kept secure at all times through complex systems. This makes it virtually impossible for anyone to tamper with a blockchain and ensures all transactions and users are protected.

Cryptocurrencies 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. They benefit from the volatility of the cryptocurrency markets by pressuring people to make investment decisions without due diligence or consideration.

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

How do people use cryptocurrency?

People use cryptocurrency to make payments, to avoid transaction fees that traditional banks charge or because it offers some anonymity. Others hold cryptocurrency as an investment, hoping the value goes up.

How do you get cryptocurrency?

You can buy cryptocurrency through an exchange, an app, a website, or a cryptocurrency ATM. Some people earn cryptocurrency through a complex process called ‘mining’ which requires advanced computer equipment to solve highly complicated mathematical calculations.

Who is behind cryptocurrency scams?

These types of crime can be carried out by lone individuals or organised crime groups, often 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 is gambling that enough people will respond so that their scam is profitable.

Examples of Cryptocurrency Frauds

Investment or business opportunity frauds

Investment or business opportunity frauds often begin with an unsolicited offer, typically to become a cryptocurrency investor, that lures you to a fraudulent website to learn more about the apparent opportunity. Once on the site, you’re encouraged to invest and make money quickly. The website might even have celebrity endorsements or testimonials that are fake.

Once you complete your transaction the offer never comes to fruition and you don’t see your money again.

Imposter or impersonation scams

An imposter or impersonation scam is when a cybercriminal poses as a trusted source to convince victims to complete a cryptocurrency transaction. This might be under the guise of government authorities, credit card providers, banks, a service provider or even a fake celebrity and they will often reach out via email and request you complete payment via cryptocurrency.

Remember, the government does not regulate cryptocurrency and it’s also not yet widely accepted by businesses so you should exercise caution whenever you receive email requests for crypto payments.

Blackmail or extortion scams

Blackmail or extortion is when you receive a message that someone has compromising information about you – be it photos, videos, confidential data etc. – and they request you pay them money or else they'll release it.

Social media cryptocurrency scams

Often, this is via a false social media post or advertisement requesting payment in cryptocurrency. You might even see other users responding to the post or leaving reviews.

In reality, these could be artificially generated trying to lure you into a social media scam. The post or message might be from a friend whose account got hacked. Alternatively, social media influencers might tout new and potentially fake crypto and encourage users to sign up or send them payments that might multiply.

Giveaway cryptocurrency scams

Giveaway scams are when cybercriminals lure victims into sending them money while promising they'll multiply the payment.

For example, this could occur if a fake celebrity social media account posts that if followers send them a certain amount of cryptocurrency, they will send back twice the amount. In reality, followers will send money directly to scammers, never to see their investment again.

Romance cryptocurrency scams

Cybercriminals play the part of an online love interest and gain a victims trust before asking them to send money. Once the victim does, the cybercriminal takes the money.

Romance cryptocurrency scams follow the same approach, but the funds are requested in cryptocurrency and are much more difficult to reverse.

Fraudulent initial coin offerings (ICO)

Scammers have found ways to make money by creating fake cryptocurrencies or hyping an existing currency by offering buyers a chance to get in on the ground floor of an ICO. Once they have enough investors, they will disappear with all of the 'invested' funds, leaving investors with nothing.

How to spot a Cryptocurrency Fraud?

Here are the main cryptocurrency warning signs to look out for:

- 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 you're 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 secure your cryptocurrency wallet

Be careful with online services – Exercise caution when considering online services for storing your funds. Exchanges and online wallets have suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank, therefore, it may be prudent to explore alternative cryptocurrency wallet options. Should you opt for such services, select them with meticulous care. Furthermore, employing two-factor authentication is strongly advised.

Small amounts for everyday uses – A cryptocurrency wallet is like a wallet with cash. Just as you wouldn't carry a large sum in your pocket, it's wise to apply the same principal to your cryptocurrency wallet.

Backup your wallet – Stored in a safe place, a backup of your wallet can protect you against computer failures, human errors, and theft of your mobile or computer.To safeguard your wallet:

- Backup Completely: Some wallets contain hidden private keys. Ensure your backup includes all private keys to recover your full funds.
- Encrypt Online Backups: Online backups are susceptible to theft. Protect your data with encryption, especially when exposed to the network.
- Diverse Storage: Avoid single points of failure by storing backups in multiple secure locations, such as USB keys, paper and CD's.
- Regular Backups: To include recent cryptocurrency addresses and changes, perform regular backups. In the future, many applications will transition to one-time backups for added convenience and security.

Encrypt your wallet – Encyrpting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software:

- Remember your password: Losing your password means losing your funds. Cryptocurrency offers limited recovery options, so store it securely. A paper copy in a secure location away from your device is a wise precaution.

- Strong password: Avoid using predictable passwords (such as dates, family and pet names)

- Avoid the most common passwords that criminals can easily guess (like Password123). To create a memorable password that is also hard for someone to guess, you can combine three random words to create a single password (for example cupfishbiro).

- Offline wallet for savings – An offline wallet, also know as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice.

  Here is an overview of some approaches:

- Hardware Wallets: Have a balance between high security and ease of use with hardware wallets. These dedicated devices offer robust protection against computer vulnerabilities and online threats. They are incapable of installing additional software and backup options ensure recovery in case of lost devices.

- Offline transaction signing: Employ two computers, one offline with the complete wallet and transaction-sigining capability, and one online with a watching wallet for unsigned transactions. This enables secure transaction issuance:
  - Create a new transaction on the online computer and save it to a USB key

- Sign the transaction with the offline computer
- Send the signed transaction using the online computer. In the event of network compromise, the online computer cannot withdraw funds

Keep your software up to date – Ensuring your Bitcoin softeware is up to date is pivotal. The latest version provides critical stability and security enhancements, preventing a range of issues and introducing valuable features, all while bolstering your wallets security. Equally vital is updating all other software on your computer or mobile to foster a secure wallet environment.

Multi-signature to protect against theft – Bitcoin offers a multi-signature capability, requiring several independent approvals for a transaction to be executed. It's valuable for organisations, granting access to treasury funds only when, for example, 3 out of 5 members authorise the withdrawl. Certain web wallets also offer multi-signature functionality, empowering users to maintain control over their assets and preventing theft by protecting against the compromise of a single device or server.

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.

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 the platform. Deactivating your account temporarily rather than shutting it down will mean the data is preserved and will help police to collect evidence. Also, keep an eye on all the accounts which you might have linked (i.e. other social media platforms, email etc.) 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, 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 – DO NOT DELETE ANY CORRESPONDENCE

Further help and support

Cryptocurrency related investment scams are prevelant across various social media platforms which can result in significant financial loss (i.e. lifesavings, pension etc.) and in turn have a negative impact on peoples futures and mental wellbeing.

The best way to protect yourself from crypto currency fraud is to be careful and selective about the websites you visit and whom you engage with online, especially when considering to invest large amounts of money. More information on where and how to invest in crypto currency can be found by visiting the Financial Conduct Authority website – Cryptoassets | FCA

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

Remember, if you are the victim of Fraud or any other crime please contact the Police by visiting our website or phoning 101.

Links

Support and Wellbeing**:**

- Home | SAMH
- Samaritans Scotland
- Breathing Space is a free confidential service for people in Scotland. Open up when you're feeling down - phone 0800 83 85 87
- Crimestoppers in Scotland | Crimestoppers (crimestoppers-uk.org)
- Victim Support Scotland

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