POLICE SCOTLAND
POILEAS ALBA

Cybercrime Harm Prevention Team

Cryptocurrency Scam Guidance

Police Scotland

18.06.24

What is Cryptocurrency?

Cryptocurrencies were invented as a result of decades-long research into digital currency. The most significant milestone was the creation of Bitcoin by an anonymous person or group known as Satoshi Nakamoto. In 2008, Nakamoto published the Bitcoin whitepaper, proposing a peer-to-peer electronic cash system that didn't rely on a central authority. Bitcoin was designed to be scarce, mimicking the properties of gold, and introduced a novel confirmation system called Proof-of-Work (PoW) to validate transactions on a public ledger known as the blockchain.

These digital currencies are known for their market volatility so the value of investors' assets can go up and down quickly. Criminals can take advantage of the unregulated nature of cryptocurrencies to scam consumers. Cryptocurrency is also the most common form of payment for illicit purchases on dark-web markets and criminal forums.

There are different types of cryptocurrencies – Bitcoin, Ethereum, USDC, USDT, BNB to name a few. In the same way that Pound Sterling, Dollars and Euros are all financial currency, cryptocurrencies differ in value.

Cryptocurrency investments are often made via currency exchange platforms. Like traditional exchanges, these websites facilitate the buying, selling or exchange of cryptocurrencies for fiat currencies like GBP or US dollars.

Criminals benefit from the lack of technical knowledge surrounding cryptocurrency transactions, pressuring people to make decisions without due diligence or consideration.

People who have been scammed often don't realise for some time. Sometimes, criminals would deliberately send a small profit to the victim, to demonstrate 'profit', only to encourage them to invest more, and faster. Victims often may make multiple or regular payments to the criminals and only realise they have been scammed when trying to withdraw their money from the investment scheme.

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

How do people use cryptocurrency?

People use cryptocurrency for many reasons – for quick 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. Due to the anonymity of transactions, cryptocurrency is also the most common form of payment for illicit purchases on dark-web markets and criminal forums.

How do you get cryptocurrency?

You can buy cryptocurrency through a cryptocurrency exchange, an app, or a website. Some people earn cryptocurrency through a complex process called 'mining' which requires advanced computer equipment to solve highly complicated mathematical calculations. Due to the limited amount of Bitcoins

available to mine, any realistic chance of becoming the first miner to solve an equation and receive a reward, would require an industrial-size set-up. Some countries, such as China and Russia have whole complexes called cryptocurrency mining farms.

The National Cyber Security Centre (NCSC) published figures which showed that as of March 2022, 11 million cryptocurrency phishing scams were reported which resulted in 78,000 scams being removed.

Who is behind this crime?

This type of crime can be carried out by lone individuals or organised crime groups, often based overseas. For perpetrators it's a low risk/high reward 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 message received via social media or dating apps. The scammer would then make the victim an offer, typically to become a cryptocurrency investor, that lures them to a fraudulent website to learn more about the apparent opportunity. Once on the website, the victim is encouraged to invest and make money quickly. The website might even have celebrity endorsements or testimonials that are fake, or offer “investment packages” that are “on sale”, to further create a sense of urgency and rush trading.

Once the victim completes the transactions, the criminals often advise that a profit is made, and to withdraw it, the victim has to “pay tax” and other fees, etc, turning the conversation into a never-ending loop of excuses and an offer that never comes to fruition. When the victim declines to invest, the criminals disappear, changing what was likely a disposable mobile number or closing down the fake social media accounts they used, before moving on to another victim. It is not unheard that the criminals would, at a later date, contact the victim again, pretending to be from a cryptocurrency recovery company, having knowledge of the scam and offering to recover the victim’s funds for a fee.

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 a fake celebrity advertising, encouraging cryptocurrency investments and trading. When the victim clicks on the advert, it redirects to a website that was set-up by the criminals. The website would often contain a form, where the victim is asked to enter their personal details. The criminals then reach out, pretending to be “portfolio managers” or part of the celebrity’s team.

Remember, the government does not regulate cryptocurrencies and it’s also not yet widely accepted by businesses so you should exercise caution whenever you receive emails or see adverts for crypto payments.

Financially motivated extortion scams

Financially motivated extortion is when the victim receives a message that someone possesses compromising information about you – be it photos, videos, confidential data etc. – and they request payment in cryptocurrency, or threaten to release the compromising material on the Internet or send it

to the victim's social media contacts. It is important that your social media profiles are not publicly available, so only people you know and trust have access to your friends' list and personal information.

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 reviews might be artificially generated by bots, programmed to post comments and make you believe that the advert is genuine.

Alternatively, the post or message might be from a friend whose account got hacked.

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 victim's 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 by offering buyers a chance to sign up for “early release” of ICO that will grow in value. 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 are told that you need to make payment to cover various fees or taxes before being able to withdraw any funds
- You are told to install remote desktop access software. This will allow the criminals to see everything you are doing, and potentially take over control of your device.
- They guide you to create an online account and move funds from your traditional account to this one, then they guide you on how to create a cryptocurrency account and move the funds once more

- If you met on social media, they will try to move the conversation to another encrypted channel of communication, to make it difficult to locate

How to secure your cryptocurrency wallet

Be careful with online services – Exercise caution when considering online services for storing your funds. 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.

Encrypt your wallet – Encrypting 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 'passw0rd'). To create a memorable password that's also hard for someone else to guess, you can combine three random words to create a single password (for example cupfishbiro)

- Do not use the same password for any other account

Offline wallet for savings – An offline wallet, also known 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.

Keep your software up to date – Ensuring your Bitcoin software 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.

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 withdrawal. 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 CORRESPONDANCE

Further help and support

Cryptocurrency related investment scams are prevalent 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**:**

- Victim Support Scotland - Fraud
- Financial Conduct Authority – Cryptocurrency Investment Scams
- Information for victims of financial crime
- Crimestoppers in Scotland | Crimestoppers (crimestoppers-uk.org)
- Police 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