

Beware of cryptocurrency scams



Cryptocurrencies have seen a boom in recent years. Companies like Bitcoin have grown from relatively unknown, to a multi-trillion dollar market and this trajectory isn't likely to slow in 2023. Unfortunately this has unlocked opportunities for scammers to take advantage and capitalise on security weaknesses to initiate scams. These scams could be as simple as encouraging you to move money to a crypto asset account or offering fake investments.

What is cryptocurrency?

Cryptocurrency lives online as a digital asset that can be traded or exchanged to buy from people or companies. There are reputable traders out there who have access to professional trading tools and use an exchange that requires ID verification to open an account or 'wallet'.

What to watch out for

Being asked to give a different payment reason:

If someone wants you to move money for an investment but asks you to give your bank a different reason for a 'smoother' transaction, don't. Fraudsters know investment payments attract more scrutiny.



Downloading new software:

Fraudsters may ask you to download software. They'll use this as a way in to access your devices and move money without you knowing.



Celebrity endorsements:

Cyber criminals can sometimes impersonate famous people on social media or messaging apps to make their offer seem more real and appealing.



Short term returns as an incentive for larger investments:

The most high value cyber crimes can give you an initial short term return. Fraudsters use this to convince victims to invest more, but after sending larger payments they can suffer even greater losses.



Top tips to keep your money safe

-  **Do check credentials**
Before making any investment, always check if the company is regulated by the Financial Conduct Authority (FCA). If they're not, you won't be protected should anything go wrong.
-  **Do stay in control of your investments**
Never allow anyone to set up a cryptocurrency wallet, upload ID documents or manage investments for you.
-  **Do be wary of requests to download software**
Never download software from an unconfirmed source. It could be used to steal your personal details and take control of your bank accounts.
-  **Do background checks before investing**
If in doubt, do your research. Use well-known and reputable sources before you take action and check that they're verified.
-  **Do report concerns**
Please report any suspicious activity to your Relationship Manager. It builds awareness of new scams and cyber crimes, and could prevent future victims falling prey to the same.