There are lots of scams out there:

In this issue we're looking at **Bank scams** which come in many guises. Many of these scams are run by offshore organisations which makes it more difficult for the authorities.

- **Phone scams,** also called Vishing, are where the target receives a call from a fraudster pretending to be a member of the target's bank staff. They'll try to persuade the target that they have been a victim of fraud. They then either try to get financial details (account and card details, four digit pins and passwords) so that they can access the account, or they try to get the target to transfer money to a 'safe' account or hand cash to a courier.

  To give the target confidence they'll suggest calling the bank back to verify the call – **beware** the 'phone line can remain open for up to two minutes so the fraudsters remain on the line and play a dialling tone to trick the target.

  If you get one of these calls **don't give out any details, don't transfer any money, don't give cash to a courier**, wait 10 or 15 minutes and ring your bank on the number the bank publishes. Ideally ring from another 'phone (for example your mobile 'phone).

- **Email scams** are from fraudsters who send convincing emails pretending to be from your bank or a trusted organisation such as HMRC or the Financial Conduct Authority. The bank scam emails often say there's a problem with your account, and ask you to update your bank details, either by replying to the email or by clicking on a link. **Don't reply or click the link,** telephone your bank on a number you trust if you feel you should contact them.

- **Postal scams** offer something that sounds attractive; however, it doesn't exist. The catch? You'll have to pay upfront to receive this once in a lifetime offer. The most common scams are for competitions, fake foreign lotteries and clairvoyants.

  To make it worse, if you fall for one of these scams, its likely that you'll be targeted again, as victims' details sold on to other fraudsters on so-called 'suckers lists'.

  Don't be rushed in sending money off to someone you don't know. Talk to your family or friends. There are lots of nasty people out there. Sadly many people who fall for these cons don't want to believe that they're being conned.

If you think you've given a fraudster your bank details, contact your bank immediately.

Explain what has happened giving as much detail as possible. Your bank will tell you what you need to do. Make sure you contact them on the number that you use for telephone banking.

Find out more at the Which? website: https://www.which.co.uk/consumer-rights/advice/i-think-i-may-have-given-a-fraudster-my-bank-details?utm_source=whichcouk&utm_medium=email&utm_campaign=scamalert280520#reporting-fraud