

5 common scams you need to be aware of

In last month's article, you read about why it's often more difficult than you expect to identify scams. With the amount of money lost to fraud rising, being aware of common types of scams could mean you're in a better position to spot the warning signs.

According to [UK Finance](#) (15 June 2026), £1.28 billion was lost to fraud in 2025, an increase of 4% when compared with 2024. There were 4.06 million confirmed cases of fraud in 2025, which fall into two broad categories, both of which may affect individuals.

- *Unauthorised fraud:* This occurs when the account holder doesn't provide authorisation for the payment to proceed. Instead, it's carried out by a third party. For example, this could happen if a criminal accesses your bank details and is able to make fraudulent purchases.
- *Authorised fraud:* With authorised fraud, the victim is tricked into sending money to the scammer. They might believe they're sending money to their bank or are investing in a genuine opportunity.

Falling victim to a scam could harm your financial security. The long-term effects often go beyond finances too. Some victims may find the fraud has an emotional impact, such as affecting their confidence or ability to trust people.

Here are five common scams you should be aware of.

1. Phishing and smishing

Every day, you likely receive dozens of emails. You might quickly scan them before clicking on a link or downloading an attachment – something scammers seek to exploit through phishing scams.

With this type of scam, fraudsters send messages that appear to be from genuine organisations, such as a bank or retailer, to obtain your personal details or download a virus onto your computer.

Smishing works in a similar way but happens via a text message.

Before you click a link or download an attachment, consider whether it's a communication you were expecting and check who has sent it. If you've accidentally clicked on a phishing or smishing link, changing your login details or freezing your accounts as soon as you realise could prevent criminals from accessing your assets.

2. Investment scams

Investment scams can take many forms, from fake social media adverts to a phone call that appears to relate to a genuine investment opportunity.

According to figures from the [City of London Police](#) (7 April 2026), victims of investment fraud collectively lost £879.8 million in 2025 – the equivalent of £2.4 million a day. Criminals reportedly exploited economic uncertainty, unstable markets, and highly convincing online platforms to dupe their victims.

Sometimes fraudsters will deliver a return on your initial “investment” to tempt you to hand over larger sums.

If you’re contacted out of the blue about an investment, this should act as a warning bell. In addition, remember that it’s impossible to guarantee returns, and if the opportunity seems too good to be true, it probably is.

3. Pension scams

Pensions are often among the largest assets people own, and the rules around them can be confusing. Indeed, a survey carried out by the [Money and Pensions Service](#) (5 November 2025) found that 22.5 million UK adults do not understand enough about their pensions to make decisions about retirement.

As a result, pensions are attractive to fraudsters. By posing as a financial professional, they may convince people to hand over significant amounts that they’ve set aside for their retirement.

Pension scammers might offer a free pension review, claim they could help you secure higher investment returns, or suggest they could help you access your pension sooner to fund an early retirement.

Again, you should be cautious if you’re contacted out of the blue. Your financial planner could help you better understand your pension, making it easier to recognise bogus opportunities.

4. Romance fraud

The number of reported romance fraud cases has risen sharply. More than 10,700 cases were reported to [Report Fraud](#) (5 May 2026) in 2025, a rise of 29% when compared to the previous year. The average victim lost £9,500. In severe cases, individuals reported losing up to £1 million.

Often using online platforms to make initial contact, fraudsters will build a fake relationship before asking for money. As this type of scam often lasts months or years, victims may come to trust the fraudster and develop a genuine emotional connection with them. The scammer may further manipulate emotions by claiming the money is needed to cover medical expenses, support their family, or pay for plane tickets so they can meet in person.

The nature of this type of fraud often means it has devastating emotional consequences for victims as well as a financial impact.

5. Vishing

Finally, vishing is when a scammer phones you and pretends to be from your bank, building society, or government organisation. By gaining your trust, they may convince you to share personal details or transfer money.

Technology is making it easier for criminals to carry out convincing vishing scams. For example, number spoofing could make the caller ID appear genuine.

If you weren't expecting a call or something sets your alarm bells ringing, hang up. Use official websites to verify the contact details, then get in touch directly. A genuine professional will understand why you're being cautious.

The Financial Conduct Authority maintains the [Financial Services Register](#), which includes the contact details of authorised firms that you can use.

We could help you identify signs of a scam

Sometimes, a second pair of eyes can highlight a warning sign of a scam that you'd previously overlooked. If you receive financial communications that you're unsure about, we're here to help you.

Next month, read our blog to discover the essential tips that could help you avoid falling victim to a scam.

Please note: This article is for general information only and does not constitute advice. The information is aimed at individuals only.

All information is correct at the time of writing and is subject to change in the future.

TNS Financial Services Limited is an appointed representative of The Openwork Partnership, a trading style of Openwork Limited which is authorised and regulated by the Financial Conduct Authority.

TNS Financial Services Limited is registered in England 6957254. Registered Office: Resolution Close, Endeavour Park, Boston, Lincolnshire, PE21 7TT.

Approved by The Openwork Partnership on 09/09/2026.