Q1 2026

Fraudulent contact and scam awareness

As we move into the first quarter of the new year, this is a time when many people review finances, set new goals, and make important decisions, and scammers know it.

They often exploit this period with convincing approaches that target both your information and your money. We're here to help you stay aware of the techniques which criminals use.

With threats such as social engineering, SIM swaps, HMRC scams and online identity theft becoming more sophisticated, staying cautious and informed is essential. Read on to find out more about these scams.

Key tips

In order to reduce the risk of being a victim of cybercrime, here are some key tips which we strongly encourage:

- Ensure that you keep your devices up to date with the latest version releases and security updates.
- Where your device allows, please make sure that you have malware protection installed.
- Avoid storing passwords on your devices in locations that are trivial to access should your device be compromised – use a password manager.
- Ensure you use strong passwords and in the event of your passwords being compromised (e.g. through a data leak or being hacked). Change the password immediately.
- Pay attention to warnings from your bank – The Confirmation of Payee service is designed to make sure you're sending the payment to the right person or business.

HMRC scams

Scams can occur at any time of the year when individuals are particularly attentive to their tax affairs.

Criminals often impersonate HM Revenue & Customs (HMRC) to deceive people into sharing sensitive information or paying fake tax debts, often through emails, texts, and websites that look genuine. This activity usually increases in January, when fraudsters exploit the upcoming 31 January tax return deadline by sending threatening messages claiming your return has failed, must be resubmitted urgently, or that you owe tax immediately.

Always be cautious when asked for bank details or your National Insurance number. HMRC will not request this information by phone or email unless you have contacted them first.

SIM swap fraud

SIM swap fraud occurs when a criminal tricks your mobile provider into moving your number onto a SIM card they control.

Unauthorised SIM swaps increased tenfold in 2024, according to CIFAS. Once a fraudster takes control of your number, they can intercept calls and texts, including security codes and allowing them to reset passwords and access your email, banking, and steal your money before you realise.

If you suddenly lose service or suspect your SIM has been taken over, contact your mobile provider immediately and alert your bank so they can monitor for suspicious activity.

To protect yourself, add extra security to your mobile account by setting a PIN for SIM changes, use authentication methods that don't depend on SMS such as an authenticator app, and stay alert for unexpected changes to your mobile service so you can act quickly if anything seems unusual.

Multi-factor authentication (MFA)

Action Fraud recommends MFA on all important accounts. This includes Transact Online (TOL). MFA, which became compulsory in December 2025, makes it harder for fraudsters to access your accounts and money, even if your username and password are compromised. We strongly suggest using an authenticator app (like Google Authenticator or Microsoft Authenticator) as the second step, as it generates time-sensitive codes for added security.

A guide on setting up MFA is available on our website and TOL.

Pump and dump scams

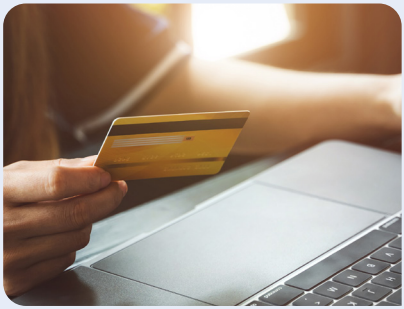
Pump and dump scams are a dangerous form of investment fraud that can cause heavy financial losses in a short space of time.

Fraudsters artificially inflate the value of a little-known share or cryptocurrency by spreading false or misleading claims. Once enough people buy in and the price is "pumped" up, the criminals quickly sell their holdings. The value then collapses almost instantly, leaving victims with significantly devalued shares, while the fraudsters walk away with the profit.

Criminals exploit people searching online for terms like "pension liberation" who are looking for ways to release funds, by creating fake websites and convincing adverts on social media or forums. Victims who show interest are contacted on messaging platforms like Whatsapp or Telegram. These scams can appear genuine, but they're designed to empty your savings. If it looks too good to be true, it probably is. We strongly recommend that you take financial advice before committing to any investment.

Authorised Push Payment (APP) fraud

APP fraud occurs when a victim is tricked into authorising a payment to a fraudster.



Scammers often impersonate trusted organisations; such as banks, government bodies, or even close friends or family, using phone calls, emails, or messages on social media. They pressure the victim into making a payment, often urgently, by claiming it's for a legitimate reason, such as settling a debt, paying for a service, or securing an investment opportunity.

This type of scam can be very convincing, as the fraudster uses tactics like spoofing phone numbers or email addresses to make their communications appear genuine. Victims may not realise they've been scammed until after the payment has been made, as the transaction is authorised by the victim themselves.

Anyone can be targeted by APP fraud, but those who are less familiar with financial transactions online, or who are under emotional or financial stress, are at greater risk. The financial loss can be devastating, as once the payment is made, it is often difficult to recover the funds as the victim authorised the payment.

Services and information

If you are contacted by someone claiming to be from your bank, stop, hang up and **dial 159**: the hotline designed to fight fraud. When you call 159, you'll get through to your bank directly and securely.

If you believe you've been targeted by scammers, report it to Action Fraud on **0300 123 2040** or at ***www.actionfraud.police.uk***, where you can also find more information on scams. If you're in Scotland, please report it to Police Scotland directly by calling 101.

Get more tips at ***www.takefive-stopfraud.org.uk*** and ***http://bit.ly/4i0ogxJ***

Sending money to Transact

Please avoid sending cheques or bankers drafts because they can be intercepted in the post on their way to us. The safest ways to make deposits into your Transact portfolio are through Transact Online (TOL: ***www.transact-online.co.uk***), using an active **direct debit** linked to the wrapper you wish to make the deposit into, or via **bank transfer**.

If you wish to send money via bank transfer

Our bank details are below:

Account Name: Transact Client Account

Name of Bank: NatWest

Account Number: 36298921

Sort Code: 60-00-01

You will need to use your **9-digit Portfolio Number** as the payment reference, so we can match the deposit to your portfolio. Please inform us that you have sent a deposit by logging into TOL, go to ***Transactions > Deposit*** or ***Deposit Then Buy*** pages and then follow the steps. That way we can allocate the deposit to the wrapper of your choice automatically and execute any investment purchases you have requested upon receipt of the deposit.

To make a deposit by Direct Debit

Log into TOL and go to ***Transactions > Deposit*** and select the **'Direct Debit'** option. Remember to select the wrapper you are making the deposit into.

If you have any concerns about your portfolio or feel as if any of the content in this guidance relates to you, then please contact your adviser or your Client Service team who will be able to help.

M291 (14) December 2025