Q4 2025

Fraudulent contact and scam awareness

As we enter the final quarter and the festive season, it's important to stay vigilant.

Scammers often take advantage of holiday promotions and busy schedules to target individuals and businesses. Staying informed is your first line of defense, and we're here to equip you with the tools and knowledge to keep yourself protected.

With more of our lives happening digitally, tactics like social engineering and identity theft are costing billions each year. Staying alert is essential.

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.
- 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.

Account safety

Action Fraud urges the use of strong passwords and **multi-factor authentication (MFA)** on all your important accounts, including Transact Online (TOL). MFA is a security method that requires a code in addition to your password as a secondary login step before you can access an account.

You should enable MFA on TOL via **Account Settings > Security**. **It will become compulsory by the end of the year.** Read more about MFA inside.

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.

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.

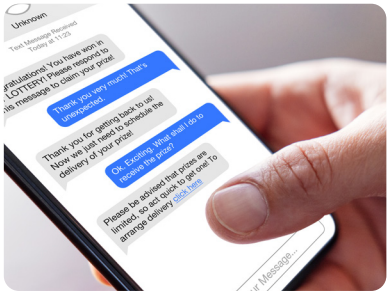
Fraudsters artificially inflate the value of a little-known share or cryptocurrency by spreading false or misleading claims. Once enough people buy in and the price is "pumped" up, the criminals quickly sell their holdings. The value then collapses almost instantly, leaving victims with significantly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

Social engineering

Social engineering is when fraudsters manipulate people into giving away information or taking actions that put them at risk.

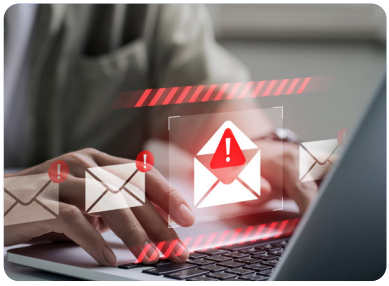
Fraudsters use personal details — often gathered from social media, company sites, or data breaches — to craft convincing phishing messages. These can include fake emails, texts, calls, or even deepfake voices and images. Their goal? To trick you into clicking links, sharing sensitive info, or transferring money.



Being cautious about what you share online and questioning unusual requests can help reduce the risk.

Malware

Malware (malicious software) is a type of software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.



Cybercriminals make extensive use of malware as it is an invaluable part of their toolkit that enables them to achieve monetary gain though a variety of channels, whether it be extortion, financial fraud or through the sale of retrieved information.

In the context of Transact Online, if a cybercriminal is successful in deploying malware to your system or device, then they will have the ability to obtain your username and password, gain access to your portfolio and your personal data, and may also attempt to steal your money.

Multi-factor authentication (MFA)

MFA makes it more difficult for a fraudster to access your accounts and money; it protects against unauthorised access to your account, even if your username and password have been compromised. When setting up MFA, we highly recommend using an **authenticator app** (like Google Authenticator or Microsoft Authenticator) as the second step. An authenticator app generates time-sensitive security codes to use alongside your usual account login details, which offers a higher level of security.

A guide on multi-factor authentication can be found on our website and TOL.

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 (13) September 2025