Q3 2025

Fraudulent contact and scam awareness

As we head into the third quarter of the year, scams are evolving just as quickly as technology. We're here to help you recognise the warning signs and stay protected.

As online interactions continue to grow, so too do the opportunities for scammers to exploit individuals. The sophistication of scams has reached new levels, with fraudsters increasingly using advanced techniques like social engineering and identity theft to manipulate victims. The rapid rise of online scams is having a significant financial impact, with billions of pounds lost every year.

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
- MFA is a 'must-have' in the modern threat landscape and is fundamental in protecting against unauthorised access to your account, even if your username and password have been compromised.

Action Fraud urges the use of strong passwords and **multi-factor authentication (MFA)** to protect email and social media accounts. You should enable MFA on TOL via **Account Settings > Security**. **It will become compulsory by the end of the year.**

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.

Authorised Push Payment (APP) fraud

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

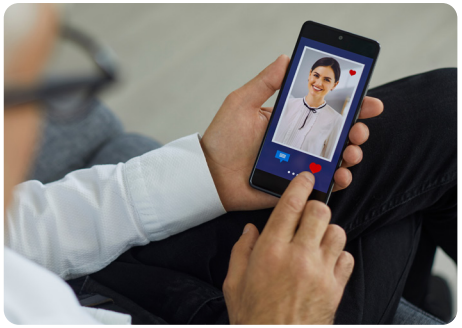
Scammers often impersonate trusted organisations; such as banks, government bodies, or even close friends or family, using phone calls, emails, or messages on social media. They pressure the victim into making a payment, often urgently, by claiming it's for a legitimate reason, such as settling a debt,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

Romance fraud

As a victim of a romance scam, you could be left struggling with the financial impact and emotional trauma of coming to terms with a relationship that wasn't real.



Be careful in what you share online, as scammers often target victims on social media platforms like Facebook or dating apps such as Tinder or eHarmony. They quickly try to move the conversation onto another private messaging platform, like WhatsApp. Using sophisticated techniques, including deepfake images and videos, they can convincingly pose as your perfect match to gain trust and steal money for reasons such as ongoing healthcare costs, travel (including a visa to come to the UK), or English lessons.

You could be a target if you are going through a difficult time—perhaps experiencing a bereavement, a relationship breakdown, or feeling lonely. Those with limited support, learning difficulties, or poor English skills can also be at risk.

Impersonation scams

Be wary of someone pretending to be in authority (such as from the police, your bank or the Financial Conduct Authority) trying to convince you to make a payment to an account they control.

It could start with a phone call or text message claiming there has been fraud on your account, and you need to transfer money to a 'safe account'. However, the criminal controls the recipient account. To commit this fraud, the criminal will do research on you and gather information from other scams and data breaches to make their approach sound genuine.

Criminals may pose as the police and ask you to take part in an undercover operation to investigate 'fraudulent' activity at your bank.

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 TOL, 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.

We strongly recommend you enable MFA on all your important accounts, including TOL. MFA adds an extra layer of security by requiring a second step, such as a code from an app, in addition to your password, making it more difficult for a fraudster to access your accounts and money. When setting up MFA, we highly recommend using an authenticator app (like Google Authenticator or Microsoft Authenticator) as the second step, as it offers a higher level of security.

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 (12) July 2025

"Transact" is operated by Integrated Financial Arrangements Ltd, 29 Clement's Lane, London EC4N 7AE | Tel: (020) 7608 4900 | Email: info@transact-online.co.uk | Web: *www.transact-online.co.uk* | Registered office: as above; Registered in England and Wales under number: 3727592. Authorised and regulated by the Financial Conduct Authority (entered on the Financial Services Register under number: 190856).