Q2 2026

Fraudulent contact and scam awareness

As we move into the second quarter of the year, you may become more active online — managing your accounts, making payments and interacting with various digital prompts. These are things scammers may try to exploit.

Criminals use convincing methods to target both your information and your money. Emerging threats like deepfake scams continue to grow and are designed to catch you off guard. More established threats like Authorised Push Payment fraud remain a large risk.

This leaflet sets out the key fraud risks including some new tactics, alongside the more common payment and impersonation frauds. It explains how these scams operate, why they are effective, and the practical steps you can take to recognise warning signs and protect yourself from financial loss.

Key tips

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

- Where possible, enable Multi Factor Authentication. 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.
- Avoid storing passwords on your devices in locations that are easy to access should your device be compromised – use a password manager.
- Use strong passwords with at least 12 characters, combining uppercase and lowercase letters, numbers, and special symbols (e.g. !, ?, #).
- 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.

Deepfake scams

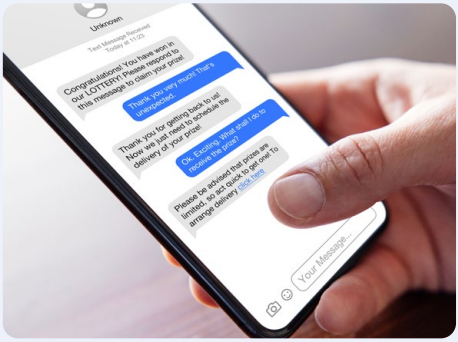
Deepfake scams use artificial intelligence to create convincing fake audio, video, or images that appear to show a real person.

Criminals can clone a trusted voice or manipulate video footage to make it appear as though a family member, colleague, or public figure is urgently requesting money or sensitive information. These approaches draw on details gathered from social media or data breaches to increase credibility. You may receive a voicemail that sounds exactly like someone you know, or join a video call where the person appears genuine, with the aim of pressuring you into making a payment, sharing account details, or bypassing normal security checks.

If you receive an unexpected or urgent request, pause and verify it using a known, trusted contact method. Never rely solely on voice or video confirmation when money or sensitive information is involved. One of the best ways to protect yourself is to come up with a safe phrase to check whether the call from your 'loved one' is real or not. It can become a sort of emergency code that only you and your immediate family or very close friends know, a simple and effective barrier against fraud.

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 or data breaches to make convincing phishing messages. These can include fake emails, texts, calls, or even deepfake media. 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.

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 the Credit Industry Fraud Avoidance System (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.

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. Before you send any payment on your phone, stop and check it's really the right person. A fraudster can pretend to be anyone.

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 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 (15) March 2026