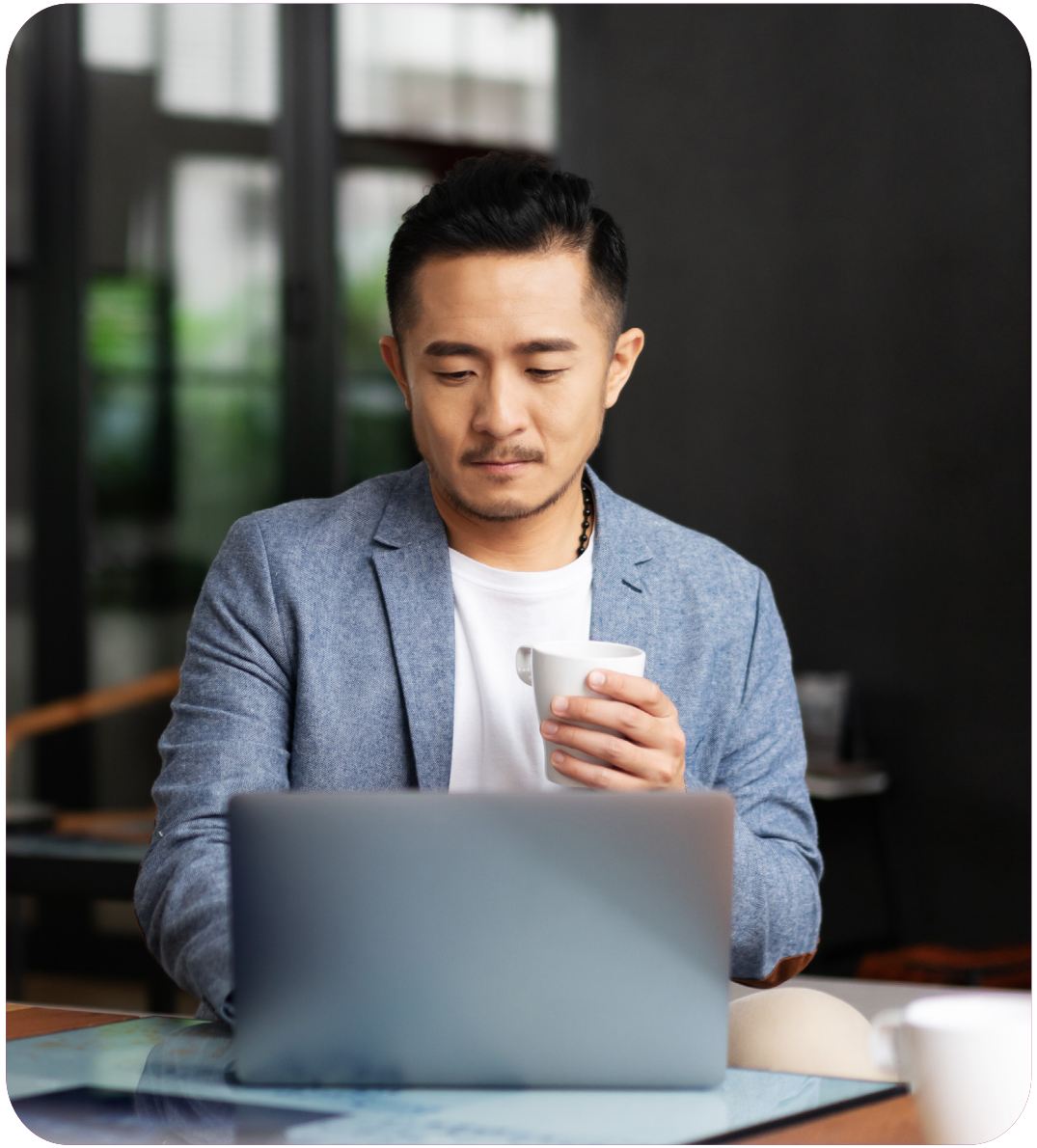
Ulster Bank
Help for what matters

Detect and protect

Fraud and scams can come in many guises.

Introduction

Fraudsters will specifically target businesses with certain scams so it’s important to recognise and report these as early as possible. They’re not always complex, sometimes a simple email or phone call is all it takes.



Contents

What's the difference between fraud and a scam?

Fraud: fraud is where you've identified suspicious activity on your account, this may be regarding a transaction that you didn't knowingly make or an update to your contact details that wasn't done by you.

Scam: a scam is where you have knowingly parted with your money and/or personal details with the expectation that you were dealing with a genuine person/company. This may have been done through intimidation, promises of cash, prizes, services, fictitious returns on investments and even romance.

Topics

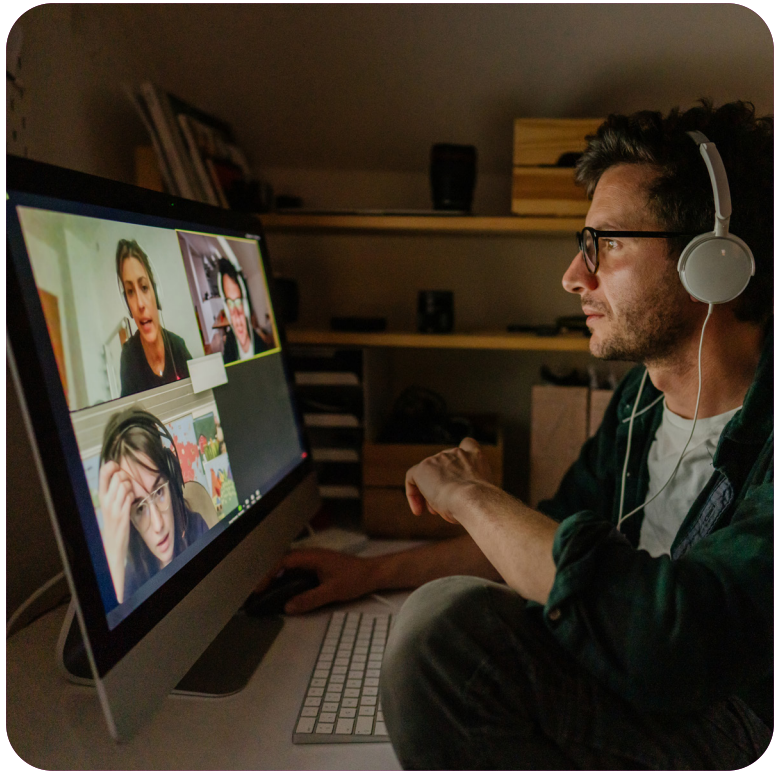
Social engineering

Back to contents

Fraudsters are known to exploit our natural tendency to trust others and use this to manipulate people into providing personal or confidential information. This approach of targeting people is known as social engineering.

One of your best fraud defences is your staff. They're able to spot a variety of fraud attempts and report them. However, they can also be one of the weakest links in your security.

Watch **this short film** highlighting how easily criminals can access your details.



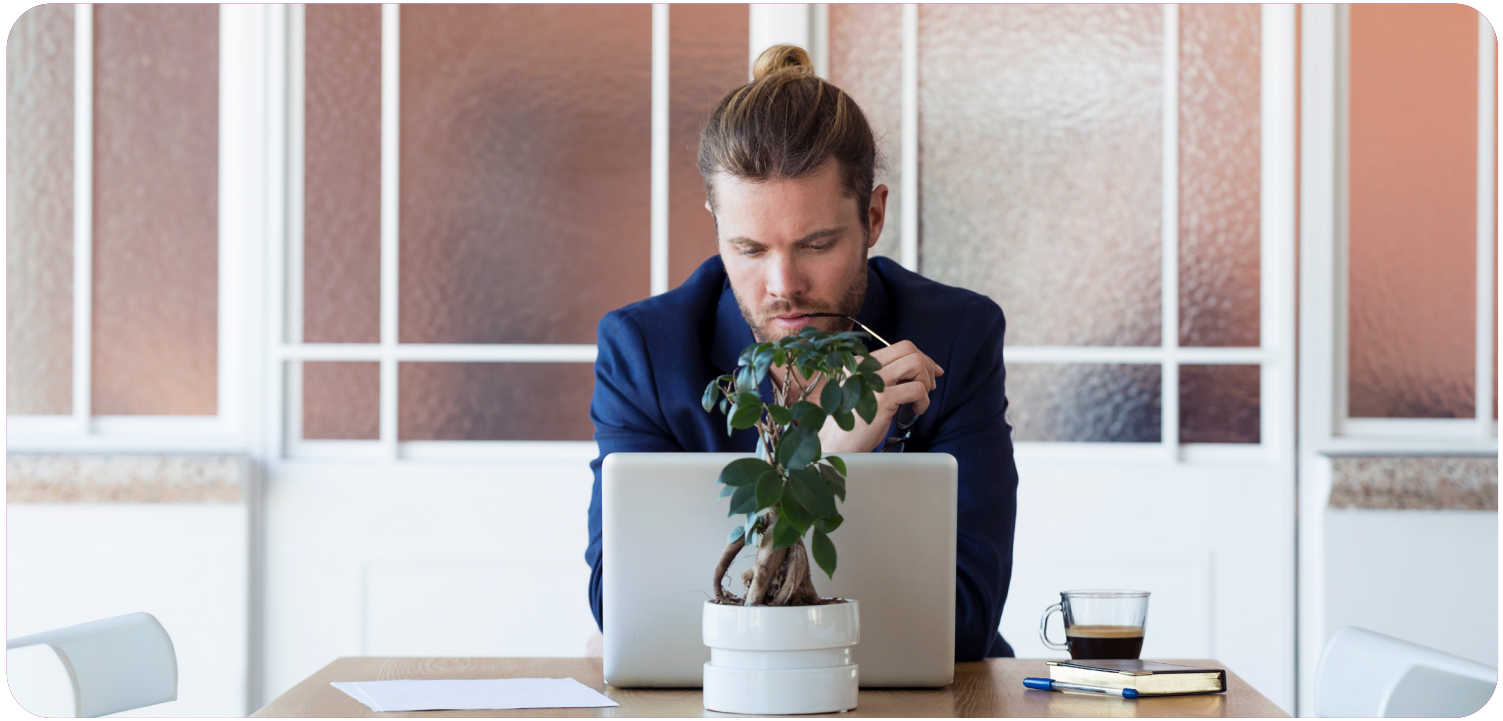
How you can help

- Make sure regular fraud awareness training is in place for everyone.
- 'Think Twice' – don't be put under pressure to make an urgent decision.
- Understand what information is available online about you and where you work as fraudsters can use this information to target scams.
- Consider testing staff using an ethical phishing campaign to see how good your staff are at spotting them.

Invoice redirection

Back to contents

Using a combination of information available online and social engineering techniques, fraudsters will contact you to update account details and ask for payments to be made to the new fraudulent account.



How you can help

- Challenge all requests to amend account details
- If you have any doubt, contact the supplier using contact details that you already hold on file to verify the request – don't rely on contact details given to you when the account changes are requested.
- Never rely solely on an email for verification as fraudsters can hack accounts and intercept emails.
- Be aware that letters and emails may appear to be genuine with the correct letterheads, logos, email addresses and signatures.
- Confirm to the supplier that the payment has been made.
- Watch **this short film** on how you can take some simple steps to protect your business.

Bogus boss

Back to contents

Anyone can be impersonated. The amount of information available online helps fraudsters send seemingly genuine emails, usually relating to payments, impersonating senior management, staff, customers and suppliers.

This is also known as CEO fraud or business email compromise fraud.

How you can help

- Challenge payment requests, even if they're from someone senior.
- If you have any doubt as to whether the email or content is genuine, contact the sender using details you already hold to confirm.
- Check if the email address has characters added or removed and look out for it changing when you hover your cursor over their name or when you look at its properties.

Telephone fraud – vishing

Back to contents

Telephone fraud, also known as vishing, is where fraudsters impersonate bank staff over the phone, claiming there's an issue with your account that requires urgent attention.

Some common examples are:

- suspicious transactions have been identified
- malicious software has been detected
- there's an internal investigation and you must avoid contacting bank staff.

Calls often seem urgent to get you to act as quickly as possible, giving you minimal time to think about whether the call is fraudulent.

How you can help

- Never be afraid to terminate a call if you have any doubts.
- Don't assume a call is genuine just because the caller knows information about you or the business.
- Be aware of 'warm-up' calls where no information is requested, as these are often carried out to set the scene for a follow-up call.
- Remember, we'll never ask you for your PIN, passwords, smartcard or card reader codes over the phone.
- We'll never ask you to key or authorise test payments, reverse transactions or to download screen-sharing software.
- Never use the caller ID number displayed to verify the caller as this can be 'spoofed' to look like the caller is calling from a recognisable number.

Mobile fraud – smishing

Back to contents

Some fraudsters use text messages to get you to divulge personal or sensitive information such as PINs or passcodes. The message will often appear to be from a legitimate source and may ask you to click on a link or open an attachment.

Links and attachments may lead to an attempt to infect your device with a virus or redirect you to a fake website, which could compromise your account details.

They can also make messages appearing in the same text chain look genuine, which make these messages tough to spot.

How you can help

- Don't text back or reply STOP to the messages.
- Don't call the number. Always contact the bank using a number you know and trust.
- Consider using virtual private networks (VPNs).
- Don't install apps from untrusted sources.
- Consider using an anti-virus app for mobile smartphones and tablets.
- Exercise care when using public Wi-Fi networks.

Email fraud – phishing

Back to contents

Emails are one of the most common communication channels fraudsters use. They're designed to entice or scare you into clicking on a link or opening an attachment that contains malicious software or redirects you to fake websites. The sender usually impersonates a well-known business or government department and scare tactics are often used to make you worry so you'll act without thinking it through.

How you can help

- Be wary of any email attachments or prompts to open links as these might also infect your computer with malware.
- Check the grammar and spelling. This can be a big giveaway of a scam email.
- Be aware that fraudsters can impersonate and 'spoof' email addresses to make them appear genuine – hover your mouse over the address to see the true sender.
- Is your account being threatened? No bank will close your account if you don't do what they say.
- Are you being offered something unexpected? Unfortunately, being the winner of a competition you never entered doesn't happen.

Insider fraud

Back to contents

When someone in your company commits fraud against it, they often start by taking small amounts of money. If these go undetected, the amounts may increase as the person gains confidence.

Insider fraud, also known as employee or internal fraud, happens because employees have the advantage of knowing how the business works, which allows them to hide their tracks. It can often take several months or years before the fraud is discovered.

How you can help

- Carry out pre- and post-employment screening checks on all staff, including right to work, qualifications, references and criminal records.
- Restrict and monitor access to sensitive information.
- Consider a tiered authority for payments and segregation of duties.
- Manage a robust annual leave policy.
- Document continued reconciling of statements and transactions.

Cheque fraud

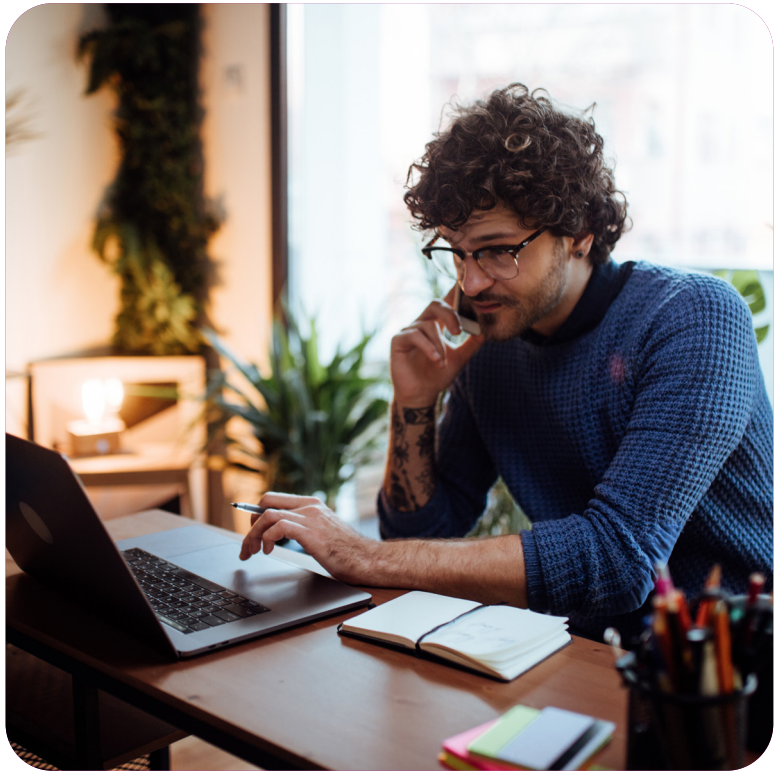
Back to contents

From the simple interception and alteration of a cheque payee or amount to cheque printing and forging of customer signatures, the technology used by fraudsters to make a forged or altered cheque look genuine is astounding.

Even though cheque usage is on the decline cheque fraud has become more organised. Advances in computer and printing technology, coupled with the relatively low cost of equipment, mean that fraudsters can now target almost any cheque.

How you can help

- Write or print starting from the very left and use reasonably large text, leaving no spaces and drawing a line through unused areas.
- Add further details on the payee line if you can, for example 'HM Revenue and Customs re JJ Jones Ref 12345'.
- Only have essential information on your cheques, avoid detailing designations such as 'director' and 'secretary' and never print signing instructions on the cheque.
- If you send a cheque by post, avoid using envelopes that reveal their contents and send high-value cheques via secure mail.
- Want to customise your cheques? All cheque designs need to have strict anti-fraud devices and other industry standards.
- For further advice on using cheques visit **cheque payment security**.

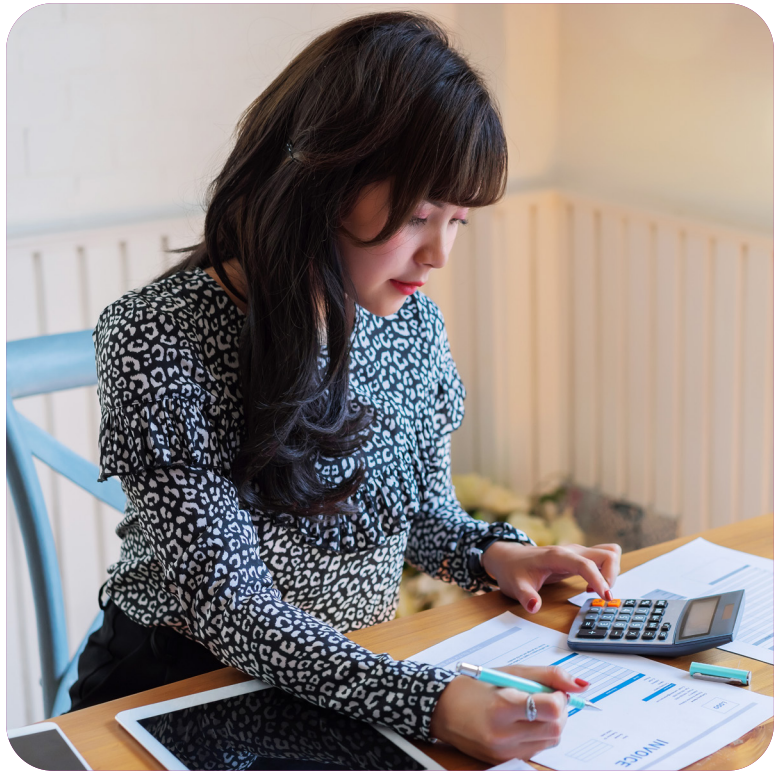


Overpayment fraud

Back to contents

Following the payment of goods or services, be on guard for new customers asking to change their order or saying an error has been made and an urgent refund is required. These customers are often based abroad and payment will usually be by cheque or draft, which is paid into the company bank account.

Companies are keen to build strong relationships with new customers therefore will process the refund quickly using an electronic payment facility. In due course, the cheque used to pay for the goods or services is returned unpaid because it's fraudulent and the company who made the refund is left out of pocket.



How you can help

- Make sure any funds paid into your account are irrevocable before making a refund.
- Be wary when a customer asks for a refund to be paid to a different account/method than the original payment.
- Never be afraid to refer to your colleagues or contact the bank if you feel that something isn't right about an instruction or payment.
- You shouldn't feel pressured to release the goods or return any of the funds until the payment has cleared.

Card fraud

Back to contents

Using your card
Fraudsters use cards, card details or stolen personal information obtained through a variety of sources from stolen cards to captured card and personal information to company data breaches and bogus text and emails.

Another common ploy is fraudulent competitions and the 'sale' of discounted goods to entice customers into sharing their card details.

Lost and stolen cards
Fraudsters often use lost or stolen cards to make a purchase or withdraw money. You should always report any lost or stolen cards to your bank or card company straight away.

Shield your PIN when you use an ATM. If you spot anything suspicious, such as someone watching you, don't use the machine and report it to your bank.

You've not received your new card
If you're expecting a new card and it hasn't arrived, call your bank or card company.

If your address changes you should tell your bank or card issuer immediately and ask Royal Mail to redirect your post. If other people have access to your post, consider collecting it from a local branch.

Contactless transactions
Contactless cards are embedded with multiple layers of security and transactions have the same protection as chip and PIN, making them safer than cash. And for added protection you'll also be asked to enter your PIN to verify your identity from time to time.

The contactless technology only works when a card is within a few centimetres of the terminal, making it highly unlikely for details to be intercepted while in use.

How you can help

- If you're using a retailer for the first time, always take time to do some research about them.
- Trust your instincts – be suspicious of prices that are too good to be true.
- Ensure your card issuer has your up-to-date contact details.
- Check your statements regularly and contact your card company immediately if you spot something you don't recognise.
- Check your credit record for any applications you don't recognise. You can do this by contacting a credit reference agency.
- For advice on accepting card payments for your business visit **card security**.

Protecting your business

Back to contents

Payments are central to the successful running of almost all businesses. Whether making or receiving payments, it's important make sure they're secure.

- Bankline
- Heimdal Security
- Fraud awareness seminars
- Reporting fraud or a scam

Bankline – enhanced digital banking for your business

Bankline is a sophisticated and secure online banking system designed to support your business. It contains a range of security features to put you in control and protect your business from fraud and cyber-attacks.

- There are dual control features, which let you decide when two or more users will be needed to approve payments and profile changes.
- You can set customised payment limits that work for your business and decide when extra levels of approval are required.
- An audit log captures all activities on an individual level. This can be tracked by users with the appropriate privileges.

You can also use Bankline Mobile, a secure mobile app that complements our Bankline service. Offering touch ID/Face ID for iPhone and fingerprint for Android as well as advanced anti-fraud systems, our robust security checks make sure your business is protected.

For more information about Bankline and Bankline Mobile please visit **Bankline**.

Bankline and The Bankline Mobile app are available to those who have an Ulster Bank business current account. Fees may apply. The Bankline Mobile app is available on iPhones (running iOS 11 or higher) and Android devices (running version 6 or higher) and to customers with a Bankline account.

Heimdal™ Threat Prevention, Patch & Asset Management

Cyber-attacks against businesses are becoming more sophisticated every day. Fraudsters can now lock you out of your PC and demand money to reinstate you. This is called ransomware. There are other malicious programmes, designed to steal your bank funds and copy your most valuable data.

We have partnered with Heimdal to offer the latest security software, Heimdal™ Threat Prevention, Patch & Asset Management, to Bankline users. Heimdal cleverly protects against threats that may otherwise go undetected and is easy to install.

Heimdal™ Threat Prevention, Patch & Asset Management offer

For Bankline customers, we're offering one free license to use on up to 10 computers. If you choose to install on more than 10 devices, fees will apply.

Heimdal™ Threat Prevention, Patch & Asset Management installs quickly, integrates with any existing security setup and delivers comprehensive, customisable automated reports.

Follow the below links for further information on the protection Heimdal provides and to register:

Ulster Bank registration page
Ulster Bank terms and conditions

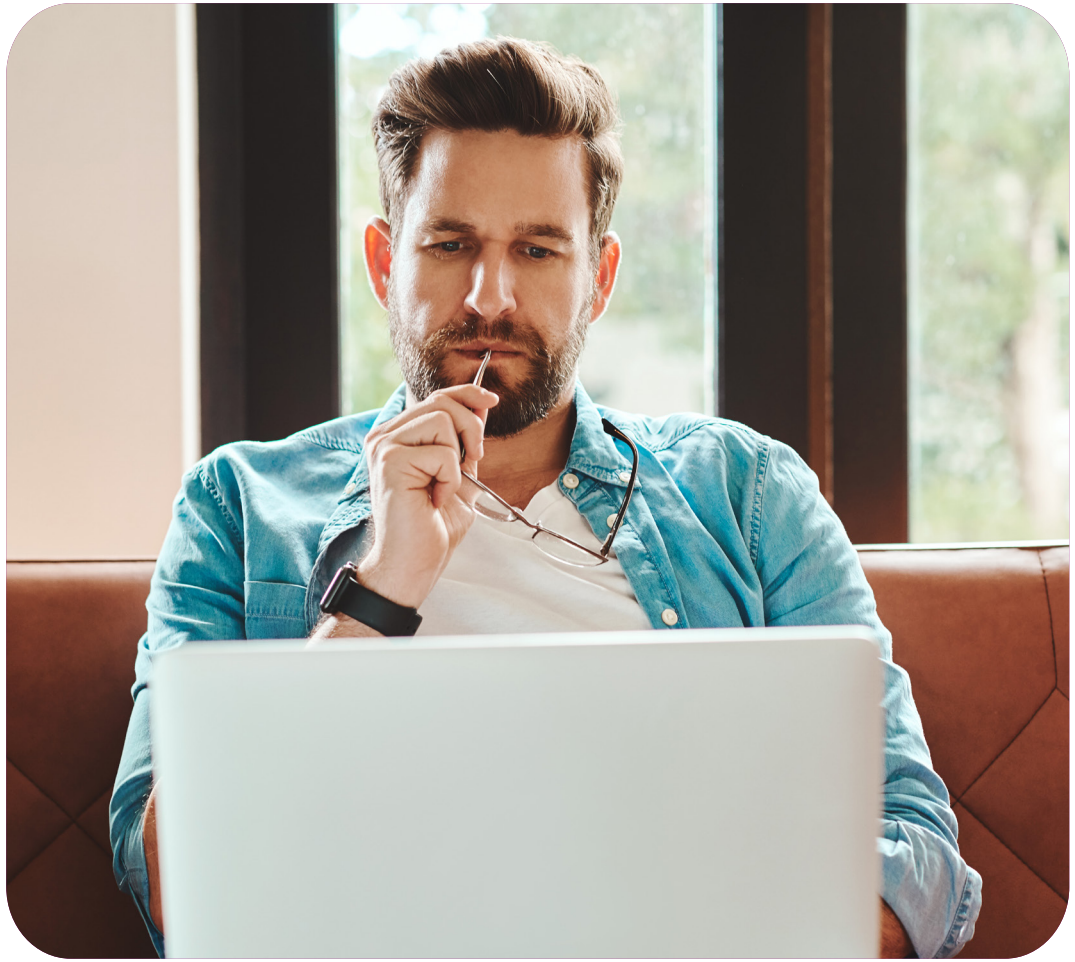
Fraud awareness sessions

Back to contents

Did you know we offer fraud awareness sessions, which highlight the latest fraud risks to help businesses and their staff to stay safe? We can help staff feel empowered to promote a culture of fraud awareness and security.

They're often held online and our regional analysts also offer one-to-one business seminars, usually held on the business premises when circumstances allow.

You can register to attend one of our fraud awareness sessions by visiting **digital.ulsterbank.co.uk/business/security**.



Reporting fraud or a scam

Back to contents

If you believe you've been the victim of fraud or a scam you should call us straight away. We want to help as quickly as possible, so please try and have as much information about the transaction or event as possible, when you call us.

Commercial Banking fraud reporting

Is this the right number for me? Commercial companies will typically have:

- More than 10 employees
- A relationship manager
- Turnover of more than £2m per year
- A Bankline profile

Call: **0800 161 5157**

Relay UK: **18001 0800 161 5157**

If you're outside the UK, call: **+44 0126 850 2401**

Business Banking fraud reporting

Is this the right number for me? Business Banking customers will typically have:

- Fewer than 10 employees
- Turnover of less than £2m per year
- Anytime Banking

Call: **0345 300 3986**

Relay UK: **18001 0345 300 3986**

If you're outside the UK, call: **+44 1252 230 8047**

Our lines are open Monday to Friday 8am – 8pm, Saturday 8am – 6pm and Sunday 9am – 5pm.

Reporting fraud on a Business Credit Card

Call: **0800 161 5164**

Relay UK: **18001 0800 161 5164**

If you're outside the UK, call: **+44 345 300 4351**

Have you received a suspicious phone call? Call us now on **03457 424 365** (**+44 289 053 8033** if you are overseas). Our lines are open 24 hours a day.

Please forward any suspicious texts to **88355**. Standard network rates apply.

Please forward suspicious emails to **phishing@ulsterbank.com**.

Further guidance is available on our **security centre**.

Ulster Bank
Help for what matters

Thank you.