Fraud Awareness

Protecting your business against fraud

for people with **purpose**
The **co-operative** bank

Important:
Read/share with your teams to protect your business from fraud

Contents

Helping you spot the warning signs of fraud

Every year, the British public loses billions of pounds to fraudsters, these criminals have a variety of trained scams to try and steal people's money.

This guide highlights key scams that affect businesses across the UK. Fraudsters target sole traders, charities and large corporations; they don't discriminate and the effects of this type of crime to businesses, people and their families can be devastating. Prevention, through awareness, is therefore a vital tool for combatting fraudsters and protecting your money.

If you'd like to stay on top of scams, visit our website **co-operativebank.co.uk/business/security** where you can learn more about current scams and how to prevent yourself or your business from becoming a victim.

Take a moment to stop and think

STOP Simply taking a moment to stop and think before parting with your money or information could keep you safe.
CHALLENGE Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
PROTECT Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Invoice fraud

Invoice re-direction fraud happens when a criminal contacts your company, posing as a genuine supplier, tradesman or solicitor and asks you to change the bank account details you use to pay them. This can be done by a hacked or spoofed email, a fake letter or by telephone.

It's not difficult for fraudsters to find out business invoice details. They'll spend weeks or even months gathering information using company websites, social media and blogs for details of high-value contract details, company employee structures and supplier partnerships.

Often, the fraudulent payment is only discovered when the genuine supplier chases for non-payment. Businesses are particularly vulnerable to invoice re-direction scams, and they can cause huge financial loss.

A real case study

A business received an email they thought one of their regular suppliers had sent. The email advised them of a change to the supplier's bank details and instructed the business to take immediate action to update their records and to pay the outstanding invoice. The business acted on the email and made an immediate payment of £80k.

A few weeks later, the business received an email from the genuine supplier, requesting payment. They advised the business that their account details hadn't changed and that they'd never sent an email asking to change them.

Concerned, the business contacted their bank and following an investigation, it was revealed that the request to alter the payment details was fraudulent. The email quoted slightly different contact details to that of the genuine supplier; a full stop appeared within the email address.

Unfortunately, the majority of funds weren't recovered. The scale and speed of the movement of money suggested the criminals were involved in highly-organised crime.

We support the national fraud awareness campaign Take Five - to learn more visit takefive-stopfraud.org.uk

CEO fraud

CEO fraud happens when a fraudster impersonates a company's senior executive, instructing the employee to make an urgent payment outside of normal procedures. They typically target a company's finance department via a hacked or spoofed email.

The emails are very convincing and the member of staff will do as their boss has instructed, sending the funds to account details quoted, only to find out that the account is controlled by fraudsters.

A real case study

A bookkeeper of a small business received an email and invoice attachment from their Managing Director (MD), requesting that they urgently send three payments to the supplier detailed on the invoice. The bookkeeper double-checked this, as they typically only pay invoices at the end of the month. The MD confirmed it was urgent, so the bookkeeper went ahead and made the payments. It turned out that the email account of the MD had been hacked and the bookkeeper was, in fact, speaking to a criminal.

Impersonation scams

This is a variation of social engineering and happens when criminals contact you out of the blue, often pretending to be the Police, a bank or other trusted organisations such as HMRC, Microsoft or a well-known broadband provider. They try to manipulate you into transferring money into another account by creating a sense of urgency, or by coercing you to download software on to your device, which gives them access to your bank account.

Fraudsters pretending to be from your bank, the police or a well-known service provider, may tell you that:

- Fraud has been identified on your account, or an urgent security check is required, so they need your passwords or PIN.
- You are due a refund and need to provide your card details or account information.
- Your bank is under investigation and, posing as the police, give you a 'safe' account number to transfer your money in to; or ask you to withdraw it and meet an officer to hand it over.
- Your internet broadband has been compromised.
- You need to download software, or click on a link in an email, that allows them to remotely access your device.

Neither the Bank nor the Police will ever ask you to move your money to another account to keep it safe.

If you think you've been a victim of fraud or would like to talk to one of our friendly fraud support team contact us on...

+44 (0) 3457 213 213* **(lines open 8am to 8pm Monday to Friday and 9am to 12pm Saturday)**

Ways to protect your business

CEO fraud

- Educate your employees about this type of scam and the tricks fraudsters may use.
- Always validate any urgent payment requests, especially if it's outside of the usual process with your CEO or senior management, ideally in person or by calling them on a trusted number before making the payment. Avoid replying directly to the email until you've validated the request.
- Most importantly, there should be constant and cautious communication between the CEO and the Finance Department. Many victims of CEO Fraud have a relaxed attitude when it comes to communicating financial matters; you must take care when emailing confidential information.

Invoice fraud

- Educate employees about this type of scam.
- Establish at least two designated points of contact with all your regular suppliers.
- Always check any change of bank account or payment arrangements directly with the supplier - use established contact details only or use a trusted telephone number from their website.
- Don't be pressured into processing payments without carrying out checks.
- Carefully scrutinise all invoices you receive - look out for mis-spellings or slight changes to email addresses.
- Check that the invoice and the amount is as expected.
- Check to make sure that the goods listed on the invoice are as expected.
- For substantial payments, insist on meeting or talking to a designated point of contact first.
- Think about how much information you share on your website or when publishing details of your suppliers.
- Reconcile accounts regularly - so potential fraud is detected more quickly.
- Check the email address matches to a known genuine one.

Internet safety

Online fraud

The internet brings many benefits but it also gives fraudsters the chance to steal your personal or financial information, through computer malware, fake emails, websites or social media accounts. It's important to know the basics of how to stay safe.

Protect your device

- If you access online banking through a tablet or mobile phone, we recommend you set up strong passwords or passcodes on your device and keep it locked when it isn't in use.
- Never tell anyone the codes from your security token or those generated from the app. Not even us!
- Never allow anyone to access your device remotely in order to keep your bank account safe.
- If you are asked to download software and then asked to log in to online banking, it's a scam!
- Protect your device by downloading security and anti-virus software, keeping them updated when prompted.
- Don't overshare your information on social media – be careful what you post.
- Check your privacy settings to help ensure you are only sharing with people you want to.

Reporting Fraud

How to get in touch with us about fraud

Take your pick from the options below:

For business banking customers
+44 (0) 3457 213 213*

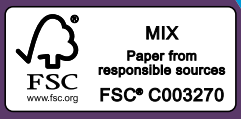
Online
Search: **Co-operative Bank Reporting Fraud**

At any branch
Search: **Co-operative Bank Branches**

Please call +44 (0) 3457 213 213* if you would like to receive this information in an alternative format such as large print, audio or Braille.

*Calls to 03 numbers cost the same as calls to numbers starting with 01 and 02. Calls may be monitored or recorded for security and training purposes.

Information correct as at 07/2021



We like our communications to have an impact on you – but not on the environment. This document is printed using vegetable oil-based inks on paper which is Forest Stewardship Council certified and made in an elemental chlorine-free process. I'm not finished – please recycle me!

MKT93091 07/2021