The co-operative bank

Ethical then, now and **always**

Business Fraud Prevention Guide

Protecting your business against fraud

Fraud Fighter

Contents

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

Helping you spot the warning signs of fraud

Every year, businesses lose millions of pounds to fraudsters. These criminals have a variety of sophisticated scams to try and steal 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 education and awareness, is therefore a vital tool for combating 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 redirection 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 information about businesses and their suppliers. 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 redirection scams, and they can cause huge financial loss.

Sometimes fraudsters even imitate an actual invoice and change the bank account details directly on the pdf of the invoice.

Invoice fraud 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 bank account 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 £80,000.

A few weeks later, the business received an email from the genuine supplier, requesting payment that was outstanding. They advised the business that their account details hadn't changed and that they had not 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 the £80,000 payment was not recovered. The scale and speed of the movement of money suggested the criminals were involved in highly-organised crime.

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 - pick up the phone to check that the request is genuine using trusted details from their website. Liaising via email may mean you are speaking to a fraudster.
- Don't be pressured into processing payments without carrying out checks.
- Carefully scrutinise all invoices you receive - look out for misspellings 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 verified genuine one.
- Be suspicious if the name of the person you're paying doesn't match the account name. Especially if someone has told you to ignore that they don't match.

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 Chief 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.

CEO fraud 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.

Remember:

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

Ways to protect your business

- 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 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.
- Be suspicious if the name of the person you're paying doesn't match the account name. Especially if someone has told you to ignore that they don't match.

Impersonation scams – pretending to be the police or your bank

Trusting people is something we all do instinctively, and when someone calls saying that they are from the Fraud Department of your bank or even the police, you should trust them right? Wrong!

Criminals will call you pretending to be from your bank or the police. They catch you off guard, claiming that fraudulent activity has been spotted on your account or that they are concerned about the safety of your money. They use a number of techniques, pressuring you into doing what they ask and before you know it, they've stolen your money.

How does this happen?

1. You receive a call out of the blue from your local 'police' and they'll tell you that they suspect fraud has occurred on your bank account. They will ask you to help with their investigation and to move your money to another account to 'keep it safe'. They'll ask you to withhold from telling your bank the real reason you are moving your money as the bank could be involved. Moving this money is a trap and would result in your money being stolen by a fraudster.

2. Another twist on this type of scam is when they call pretending to be from the Fraud Department of your bank, asking you again to move your money to keep it safe.

Protect yourself – think fraud!

- Be vigilant, the bank or the police will never ask you to move your money out of your account to keep it safe or ask you to visit a branch and take out cash to hand over to them.
- The bank or police will never ask you to assist with an investigation.
- If you have been instructed to tell the bank, that you are moving your money for a different reason or you have been told not to trust us, then stop! It's a scam!
- Contact your telephone service provider to discuss call-blocking solutions.
- Don't rely on the caller ID display on the phone to check if the caller is genuine. Fraudsters can manipulate this.

Remember

× **Never** share your bank account or security information in full.

× **Never** share the PIN for your card with anyone.

× **Never** tell anyone your Online Banking One Time Passcodes that we send to you in a text or an email. **Not even us.**

× If we suspect fraud on your account we may send you a message to check it was really you making the payment. We will never call you and ask you for any details from this message or tell you how to reply to it.

If you think you have been targeted or fallen victim to a scam, call **159** where your call will be safely routed through to us.

Other impersonation scams

Criminals will call you, pretending to be from trusted broadband providers like BT, TalkTalk, Sky or Microsoft. They'll claim that they are calling in relation to issues with your broadband, but the steps they take you through to 'fix' the problem could lead to you losing your money.

How does this happen?

1. One example of this scam is that you receive a call telling you that there is an issue with your broadband. They tell you they can fix it either by clicking on a link in an email, or by downloading an app to your device that allows them access to your device remotely. The link or app gives criminals complete control of your computer.

2. They'll spend hours on the phone with you pretending to resolve the issues, asking you to log in to your emails and online banking to check everything is working OK. They may even offer you 'compensation'. They'll then say that they've accidentally credited you with too much money and ask you to send it back urgently. You log on to your online account, but as the criminal have access to your device, they trick you with fake screens to make you think there is a problem or making you think they've compensated you with too much money. In reality, they have moved your savings to your account and without realising you send it all to the criminal.

3. Another twist on this scam is that the caller pretends to be from a trusted retailer like **Amazon**, telling you that you're due a refund and you need to check that you've received it. Or they may pose as someone from **HMRC** threatening prosecution for unpaid taxes.

Ways to protect your business

- Be very wary if you are called by someone you don't know. Do not be pressured. If you're unsure if you are speaking to the genuine company, put the phone down immediately and don't answer any further calls from them. Contact the company directly using a number from a trusted source, such as their website, and call them back, ideally from another phone to check if the caller was genuine.

- It may be a coincidence that you are having problems with your broadband. If you are, call them directly yourself for advice or support. That way, you know that you have started the conversation and are happy you're dealing with the genuine company should they need to access your device for technical support.

Remember, if you receive a call:

× **Never** share your bank account or security information in full

× **Never** share the PIN for your card with anyone

× **Never** tell anyone your Online Banking One Time Passcodes that we send to you in a text or an email. **Not even us!**

× **Never** agree to download an app or software on your mobile, tablet or computer that allows someone to access it remotely. The Bank, the Police or any other trusted organisation would never ask you to do this.

Fake emails and texts

Many victims of fraud and scams wonder how the criminals managed to get hold of their personal or financial information. They do this by sending out mass volumes of fake emails and text messages in the hope that someone will respond and give them the information they need. The messages will be riddled with links or telephone numbers all designed to gather your information.

How does this happen?

You receive a fake email or text message from a well-known parcel delivery company claiming that they have been unable to deliver your parcel. You're asked to click on a link to arrange for the parcel to be delivered and will be asked to confirm your personal or financial information. Once the criminal has this, they typically use this information to scam you days, or weeks, further down the line. They may call you impersonating trusted organisations, or they may use the information to gain access to your bank account or to even use your card details fraudulently.

There are a wide variety of fake emails and text messages distributed by criminals with common asks of you, such as:

- Friend/Family in need WhatsApp messages claiming their mobile number has changed and going on to ask for financial help
- Pay immediately!
- Complete this form
- Sign up here
- Verify your security or log in here
- Contact us on...

Protect yourself - think scam!

- Be very wary of unexpected emails and text messages and avoid sharing your personal or financial information via email.
- Never click on a link in an unexpected email that asks you to 'log in' or 'pay now'.
- Stop and think, don't respond immediately. To check if it is genuine, we advise you to contact the company directly using a telephone number from their genuine website.
- Look out for some simple signs of a fake message:
  - They don't use your first name or use your full email address as your name
  - The message is threatening or has a strong sense of urgency
  - It may look like a genuine email address that has been changed very slightly to look similar e.g. Co-0perativebank.co.uk
  - The email contains spelling errors or uses poor grammar.

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.

Important tips

- 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!
- Don't use a search engine to access your Online Banking account. Instead, always type www.co-operativebank.co.uk/business into the address bar.
- Never allow anyone to access your device remotely unless you have initiated the call and you know that the person you are dealing with is genuine.
- 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 over share 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.

Call 159 immediately if you think you are being targeted or have fallen victim to a scam.

Reporting fraud

If you believe your online banking security has been compromised or if you do not recognise transactions on your account call us on **+44 (0)3457 213 213***

If you need to report your card as lost or stolen, call us on **+44 (0)345 600 6000**

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

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

The **co-operative** bank

Ethical then, now and **always**

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 of 02/2025

We like our communications to have an impact on you – but not on the environment. This product is made of material from well-managed, FSC®-certified forests and other controlled sources.

MKT93091 02/2025