COMMERCIAL BANKING

Helping to protect your business from fraud

BANK OF SCOTLAND

By the side of business

Fraud is a growing threat to business

To help keep your business safe, this guide has information on common business frauds and where you can go to learn more. It also includes a link to a free online training course. Have a read and share it with others at work so everyone can be aware of fraud.

You can find fraud information and access a free online training course on our Fraud Hub:
bankofscotland.co.uk/fraud
Or scan the QR code.

In this guide

How to spot and avoid scams

How we can help

Type of scam:
Email payment fraud

Fraudsters can send an email that pretends to be a supplier or another person from your business. Their goal is to try to trick you in to paying an account they hold.

How this scam works:

- Fraudsters can break into email accounts and watch messages between businesses, suppliers and employees.
- When the time is right, they can send an email that seems to be from a supplier or a colleague.
- They can either make the email address look similar to one you know and trust, or take control of someone's mailbox. The email can include a previous chain of genuine messages.
- The message can say that payment details for a business or an employee you pay regularly has changed, or that an urgent payment needs to be made.

How to avoid this scam:

- Always double-check any change of payment details, urgent payment requests or invoices that come by email.
- Talk to the person or business who sent the email to check it's genuine and confirm the account number to be paid.
- Use a telephone number you know and trust, not one from an email.

Case study

The target:
The finance department at XYZ Building*.

The set up:
XYZ often buy materials from ABC Merchants*. They keep in touch by email and phone to confirm order details and to send invoices.

Fraudsters used a computer virus hidden in a random email to break into ABC's email account. They find a message about a recent order from XYZ and reply with a new invoice that looks just like the real thing. But, they change the payment details to a different account.

The scam:
When XYZ finance department get the email, they pay the invoice without checking any of the payment details. The money goes to the fraudster's account. The scam is only uncovered when ABC send the real invoice, but it's too late for XYZ who lose all of their money.

* The business names used in this case study have been changed, to protect the identity of the genuine client.

Type of scam: Ransomware

Fraudsters can use emails to send a computer virus such as malicious software (malware). Ransomware is a type of malware that can block access to your business computer network or key files. Fraudsters then demand a ransom to remove the block.

How this scam works:

- Ransomware usually hides in attachments or links within a scam email.
- It's used by fraudsters to steal files or block access to your business computer or network.
- An attack is followed by a ransom demand to remove the block and/or return the stolen files.
- Fraudsters usually want a ransom to be paid in a digital currency, like Bitcoin which is harder to trace.

How to avoid this scam:

- Install good quality anti-virus and firewall software on all your business devices and run regular scans.
- Update your anti-virus, firewall, other software and operating systems as soon as updates are available.
- Backup key files and data on a regular basis and keep these backups offline – not connected to your computer network.
- Create a ransomware attack plan so you know what to do and who to contact in case it happens.
- Consider taking out business cyber insurance.

Case study

The target:
ABC Retail*

The set up:
A member of staff at ABC clicked on a link in an email without checking if it was a genuine message.

Some time later, one of their computers displayed a message which stated that all of the data on their system had been encrypted and a ransom payment of £25,000 payable in Bitcoin was demanded to access the decryption key to unlock the data.

The message stated that the decryption key would be destroyed within a short period if the ransom wasn't paid.

The scam:
ABC decided not to pay the fraudsters because there was no guarantee the block would be removed or that the data accessed would not be used or sold by the criminals.

ABC was forced to scale back trading for 3 weeks and faced significant costs and disruption while restoring their computer systems and critical data. They also suffered damage to their reputation as they needed to alert their customer base about the breach.

* The business name used in this case study has been changed, to protect the identity of the genuine client.

Type of scam: Scam calls

Fraudsters can call to pretend to be someone you trust. Their aim is to get sensitive business details, or to trick you to move money to another account.

How this scam works:

- You get a call that claims to be from a genuine organisation, such as a bank, the Police or a well-known company.
- Fraudsters can copy genuine phone numbers so it looks real on your caller ID.
- Fraudsters do their research to help them sound genuine. This means they may know facts about you or your business.
- They can ask for passwords or online banking codes to log in to your business account and steal money.
- If they pretend to be a bank, they can say there's a problem with your business account to try to get you to move money to another account.
- They may try to convince an employee to download something to their computer. This download will contain a virus which allows them to control the computer remotely and steal online banking passwords and codes.

How to avoid this scam:

- If you're not sure about a call from a bank, the Police or other organisation, hang up. If you need to check it's genuine, contact a number you trust, not one from the call.
- Never rely on the number that appears on your caller ID.
- Make sure all your staff know that a bank will never call to ask for online passwords, PINs or card reader codes.
- Remember: we'll never call to tell you to move your money to another account.

Case study

The target:
A company called Builders Limited*.

The set up:
A person calling Builders Limited say they are from the Bank and the caller ID shows a number that matches one from the Bank. The caller provides Builders Limited with a website address where they should go to download the Bank's webchat software, enabling a secure conversation about suspicious payments. However, the software they download actually allows the caller to take control of their computer.

The scam:
The caller tells Builders Limited to log in to their online banking, however when they do this the screen goes blank.

They then ask Builders Limited to generate a card reader code to put a stop on the fraudulent payments which they say have been identified. As the caller has control of the computer and now knows the card reader code, they can make a fraudulent payment of £184k. The funds are quickly dispersed and Builders Limited only managed to get a small amount back.

*The business name used in this case study has been changed, to protect the identity of the genuine client.

Type of scam: Scam messages

Fraudsters can use texts or messages on social media to trick an individual within a business.

How this scam works:

- A text can appear to have come from a bank or another trusted organisation. Fraudsters can copy genuine phone numbers so it looks real on the sender's ID.
- The message could contain a link which if clicked puts a virus on your phone. Or it could lead to a genuine looking website that asks you to log in or give personal or confidential banking details.
- Fraudsters can use social media, such as WhatsApp, to send messages that claim to come from somebody you know who needs help. The message will ask for a payment to be made to a new account.

How to avoid this scam:

- If you get an unexpected text or message, make sure it's genuine before you reply. Don't click on any links or make a payment until you've checked.
- Check by calling the person who claims to have sent the message on a number you know and trust, not one from a text or social media message.
- Keep your passwords and personal details private.

Visit our Fraud Hub: **bankofscotland.co.uk/fraud**

Type of scam: Employee fraud

This is when someone you employ commits fraud against your business.

How this scam works:

- If you trust an employee or contractor, you may not expect them to commit fraud.
- Employee fraud can include false expenses claims, stealing money or data, and using the business account to pay for personal things.
- This kind of fraud can cause serious damage to your business as it may go unnoticed for many years.
- The costs of dealing with employee fraud can be high and the chance of getting lost money back is often slim.

How to avoid this scam:

- Make sure your business has a robust hiring process that includes criminal record and character checks. Keep it up-to-date.
- Have senior colleagues oversee employees who deal with business finances. Use dual approval for all payments.
- Regularly check who can use business accounts, systems and files. Only allow those who need it to have access and remove access immediately when someone leaves, changes roles and no longer needs access.
- Allow problems at work to be reported anonymously through a whistleblowing service.

Visit our Fraud Hub: **bankofscotland.co.uk/fraud**

Top tips

Keep your passwords safe. **NEVER** give your online banking passwords or card reader codes to anyone who calls, emails or texts.

Double-check all invoices or payment requests that come by email. Call the sender on a phone number you know and trust, not one from an invoice or message.

Think before you click. Only download files or click on links from a trusted source. Check first to make sure it's safe.

Train your staff regularly as it can help to keep your business safe. Visit our fraud hub to use a free online training course.

Further help and guidance

If you think your business has lost money to a scam, or fraudsters have obtained your banking details, call your Relationship Manager right away. In an emergency, dial **159** to talk with us. This is a safe way to get in touch.

Report any fraud to Police Scotland, by calling **101**.

The National Cyber Security Centre provides support and guidance on cyber security to organisations in the UK. **www.ncsc.gov.uk**

You can find fraud information and access a free online training course on our Fraud Hub: **bankofscotland.co.uk/fraud**

Or scan the QR code.

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at **business.bankofscotland.co.uk/help/contact-us/complaints-procedure**

Get in touch

bankofscotland.co.uk/fraud

Contact your relationship management team

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use Relay UK. More information on the Relay UK Service can be found at: relayuk.bt.com

Important information

Please note that any data sent via email is not secure and could be read by others.

1/4520996-6 (09/23)

BANK OF SCOTLAND