

BUSINESS & COMMERCIAL

**Helping to protect
your business
from fraud**



**BANK OF
SCOTLAND**

Fraud Guidance

Fraud is a growing threat and it's important to stay vigilant and informed about the different types of scams.

This guide includes information on common frauds and where you can go to learn more. Make sure you share this information with your colleagues, so that everyone is aware.

! Contact us immediately on **0345 122 7801**, if you think any of your Bank of Scotland Business Bank accounts have been accessed by a third party or targeted for fraud.

You'll need to tell us the reason for your call so we can direct you to our fraud team.

Please get in touch even if you haven't suffered any loss from the attempted fraud.

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 offers 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.



Contents

Top tips	Page 4
How to spot and avoid scams	
Email payment fraud	Page 5
Ransomware	Page 7
Scam calls	Page 9
Scam messages	Page 11
Buying Online	Page 12
Employee fraud	Page 13



Select the home button at the top of the page to return to this contents page, wherever you are in the document.



Top tips



Keep your passwords safe.
NEVER give your Online Banking passwords or card reader codes to anyone who calls, emails or texts. Never enter them online at the request of a caller.



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, message or incoming call.



Only download files or select links from a trusted source. Check first to make sure it's safe.



Train your employees regularly as it can help to keep your business safe. Visit our Fraud Hub to use a free online training course.



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

Email payment fraud



The goal of the fraudster

Trick a business or individual to make a payment into an account they hold.



How this scam works

- ▶ Fraudsters break into email accounts and watch messages between businesses, suppliers and employees.
- ▶ When the time's right, they email pretending to be a supplier or colleague. The email might include an earlier chain of genuine messages, or an attachment such as an invoice.
- ▶ They can pretend to be an important person at your work, like a CEO. Fraudsters hope you pay without checking it's real.
- ▶ They make the email address look like one that's known and trusted. Or they take control of someone's mailbox.
- ▶ The message says payment details for a business or employee who's paid regularly have changed. Or it demands that an urgent payment is 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 sender of the email to check it's genuine. Confirm the account number to be paid with them.
- ▶ If a payment involves more than one person or business, like an agent, make sure everyone you deal with independently checks the payment details.
- ▶ If an email with an invoice wants you to follow a link, stop and think. Is it real? A link in a scam email can put a virus on your device, or take you to a fake website.
- ▶ Ask your IT team or provider to set up additional email security, such as warning banners. And use support and guidance from the **National Cyber Security Centre**.
- ▶ Always use a telephone number you trust, like one in your contacts. Never use one from an email. Set up a person or team you can trust at your clients to help you double-check invoices.

Case study

The target: The finance department at XYZ Building

The set-up:

XYZ often buys 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 gets the email, they pay the invoice without checking any of the payment details. The money goes to the fraudster's account.

When ABC sends the real invoice, XYZ uncovers the scam, but it's too late for XYZ who loses all their money.

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

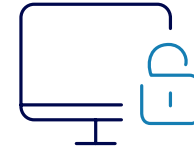


Ransomware



The goal of the fraudster

To get a business or individual to pay a ransom.



How this scam works

- ▶ The fraudster sends an email including a computer virus such as malicious software (Malware).
- ▶ Ransomware (a type of Malware) hides in the attachments or links in the email.
- ▶ Fraudsters use it to steal files or block access to a business computer or network.
- ▶ They send a ransom demand to remove the block and/or return stolen files.
- ▶ It's usually demanded that the ransom is paid in a digital currency like Bitcoin. This is because it's harder to trace.

How to avoid this scam

- ▶ Install good quality anti-virus and firewall software on all business devices and run regular scans.
- ▶ Update anti-virus, firewall, other software and operating systems as soon as updates are available.
- ▶ Backup key files and data regularly and keep these backups offline - not connected to a 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. For more information visit business.bankofscotland.co.uk/business-resource-centre/cybersecurity-offer

Case study

The target: ABC Retail

The set-up:

An employee at ABC clicked on a link in an email without checking if it was a genuine message.

Later, one of their computers showed a message that said the data on their system had been encrypted.

It demanded a ransom payment of £25,000, payable in Bitcoin to access the decryption key to unlock the data.

It said that they would destroy the decryption key within a short period if ABC didn't pay the ransom.

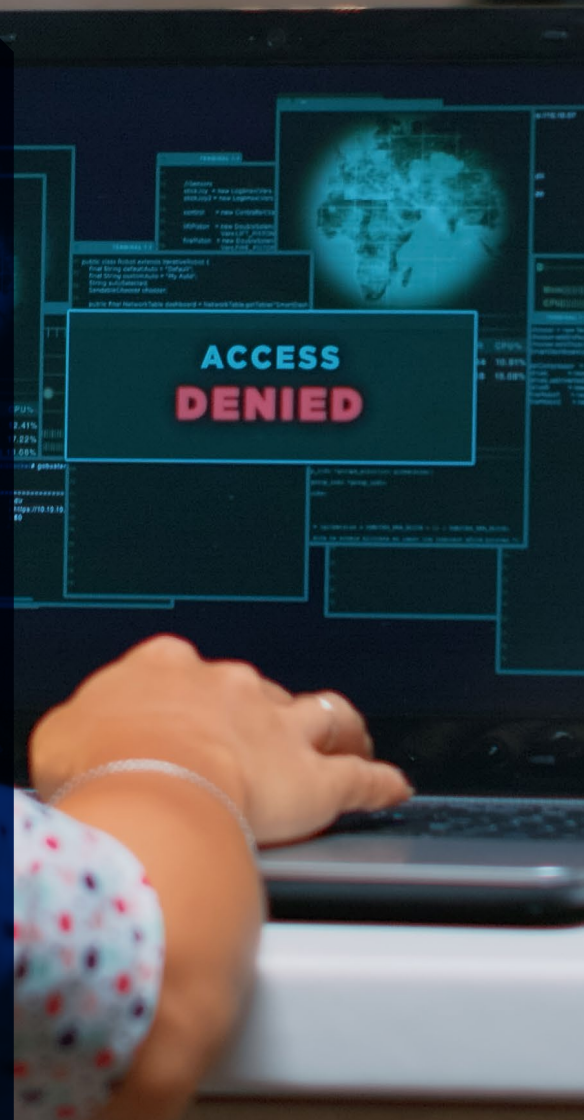
The scam:

ABC decided not to pay the fraudsters because there was no guarantee the criminals would remove the block. Or that they wouldn't use or sell the data accessed.

Forced to scale back trading for three weeks, ABC 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.



Scam calls



The goal of the fraudster

To get sensitive business details, or to trick an individual to move money to another account.



How this scam works

- ▶ A caller will claim they're from a genuine organisation, like a bank, the Police or a well-known company.
- ▶ They'll copy genuine phone numbers, so it looks real on a caller ID.
- ▶ Fraudsters do their research to help them sound genuine. So, they may know facts about an individual or a business.
- ▶ They'll ask for passwords or Online Banking codes to log in to business accounts and steal money.
- ▶ If pretending to be a bank, they'll say there's a problem with a business account. This is to get the individual to move money to another account.
- ▶ They'll try to convince an employee to download something to their computer. The download will have a virus, allowing them to control the computer remotely and steal Online Banking passwords and codes.
- ▶ Fraudsters use Artificial Intelligence (AI) to create deep fake audio and video of someone in a business. It seems the individual is speaking to a colleague on a video call, but the images and audio are fake. The fraudsters trick the individual into making a payment.

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 shows on your caller ID.
- ▶ Tell your employees 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.
- ▶ Never rely purely on a phone call or video chat within your business as a method of authorising payments.
- ▶ Always check payment details using a second independent contact method, such as calling them back on a number you know is right.

Case study

The target: Builders Limited

The set-up:

A person calling Builders Limited says they are from the Bank and the caller ID shows a number that matches one from the Bank.

They give Builders Limited a website address where they should go to download the Bank's web chat software.

But the software in fact allows the caller to take control of their computer.

The scam:

The caller tells Builders Limited to log in to their Online Banking, but 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 that they say they have identified.

As the caller has control of the computer and now knows the card reader code, they can make a fraudulent payment of £184,000.

The fraudster quickly dispersed the money.

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.



Scam messages



The goal of the fraudster

To use texts or messages on social media to trick an individual within a business to give banking details, or to make a payment.



How this scam works

- ▶ A text or message seems to have come from a bank or another trusted organisation. Fraudsters can use social media, such as WhatsApp, to send messages.
- ▶ The messages claim to come from somebody that's known to the individual who needs help. It asks for a payment to be made to a new account.
- ▶ Fraudsters copy genuine phone numbers, so the sender's ID can look real.
- ▶ The message includes a link that if selected puts a virus on the phone or the link takes the individual to a genuine looking website.
- ▶ The individual will be asked to log in or give personal or confidential banking details to the genuine looking website.

How to avoid this scam

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

Buying online



The goal of the fraudster

To get a business or individual to make a payment for an online purchase for an item that doesn't exist.



How this scam works

- ▶ Fraudsters target a business that makes online purchases by creating fake websites or social media profiles.
- ▶ They'll advertise anything they think a business might want to buy.
- ▶ They send phishing emails that appear to be from well-known organisations, offering low prices or items that are in demand.
- ▶ It can be difficult to tell the difference between a good deal and a scam. Although one important sign of a scam, is they'll usually want payment by bank transfer.

How to avoid this scam

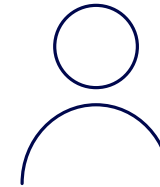
- ▶ Check out the seller before purchasing - check reviews, do they look genuine and are they from a wide range of buyers.
- ▶ Does the seller have an established website, with a history of reviews?
- ▶ Type in the right website address for a genuine seller, rather than using a link in a message or on social media.
- ▶ Pay safely - fraudsters usually want you to pay by bank transfer or a way that doesn't offer you protection. If you use a debit or credit card to pay for things online - this will help protect your money if things go wrong.
- ▶ If you can't pay by card or an item is large or expensive, go to see it personally. Only pay when you're happy and it's handed over.

Employee fraud



The goal of the fraudster

To make false expenses claims, steal money or data, and use the business account to pay for personal things.



How this scam works

- ▶ If a business trusts an employee or contractor, they may not expect them to carry out a fraud.
- ▶ This kind of fraud can cause serious damage to a business as it may go unnoticed for many years.
- ▶ Costs of employee fraud can be high. The chance of getting the 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 access to those who need it. Remove access straight away when someone leaves, changes roles and no longer needs access.
- ▶ Allow employees to report problems at work anonymously through a whistleblowing service.

Business help and support

We aim to provide you with a high level of service. If you have a query our Help & Support pages can help:
business.bankofscotland.co.uk/help

Find out more



bankofscotland.co.uk/fraud

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

Calls and online sessions may be monitored and/or recorded for quality evaluation, training and to ensure compliance with laws and regulations. Not all Telephone Banking services are available 24 hours a day, 7 days a week.

Important information

Bank of Scotland plc. Registered Office: The Mound, Edinburgh EH1 1YZ. Registered in Scotland no. SC327000.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 169628.

Eligible deposits with us are protected by the **Financial Services Compensation Scheme (FSCS)**. We are covered by the **Financial Ombudsman Service (FOS)**. Please note that due to FSCS and FOS eligibility criteria not all business customers will be covered.

While all reasonable care has been taken to ensure that the information provided is correct, no liability is accepted by Bank of Scotland for any loss or damage caused to any person relying on any statement or omission. This is for information only and should not be relied upon as offering advice for any set of circumstances. Specific advice should always be sought in each instance.

