COMMERCIAL BANKING

Helping to protect your business from fraud

BANK OF SCOTLAND

By the side of business

Fraud Guidance

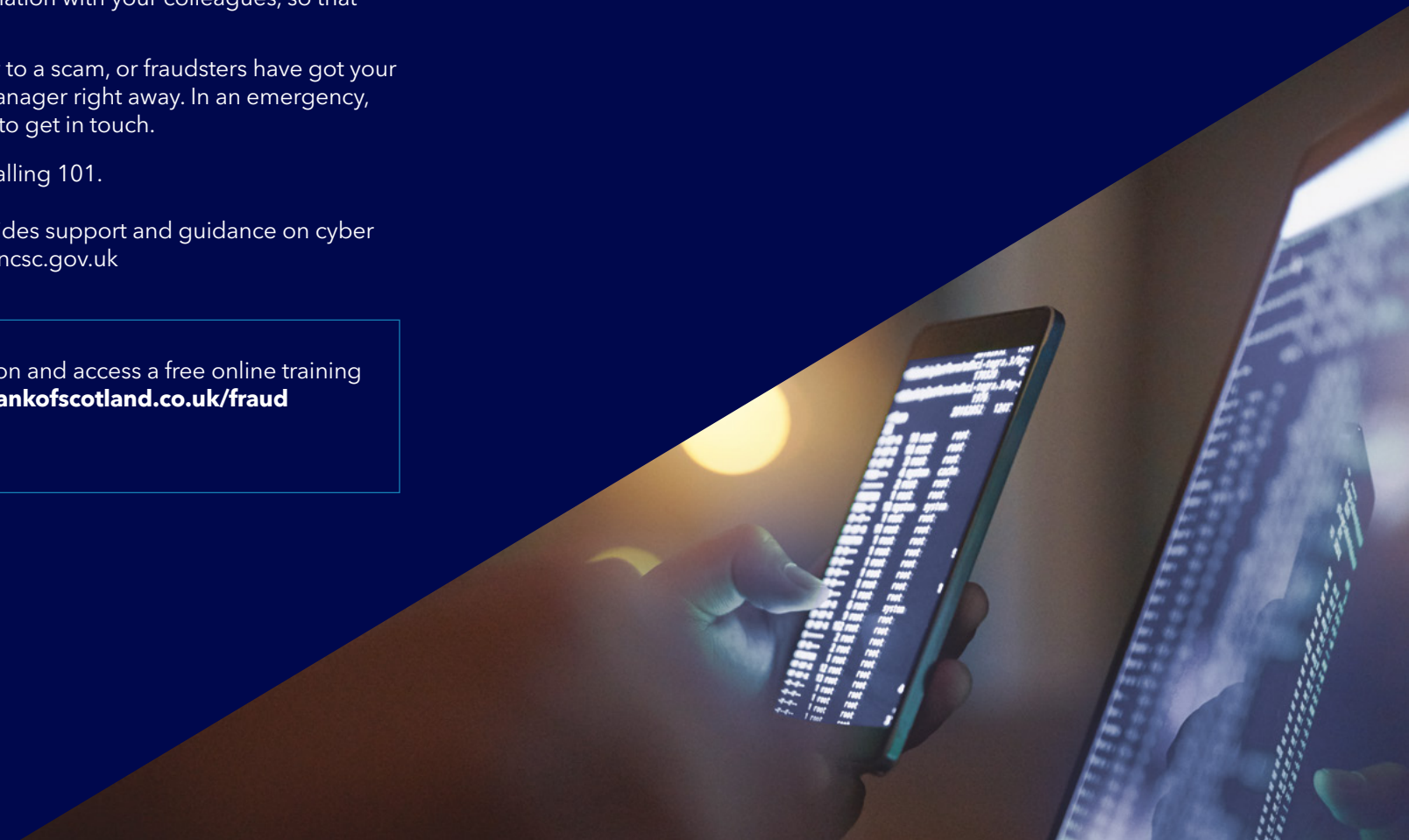
Fraud is a growing threat to businesses and it's crucial to stay vigilant and informed about the different types of scams.

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

- ! If you think your business has lost money to a scam, or fraudsters have got 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**

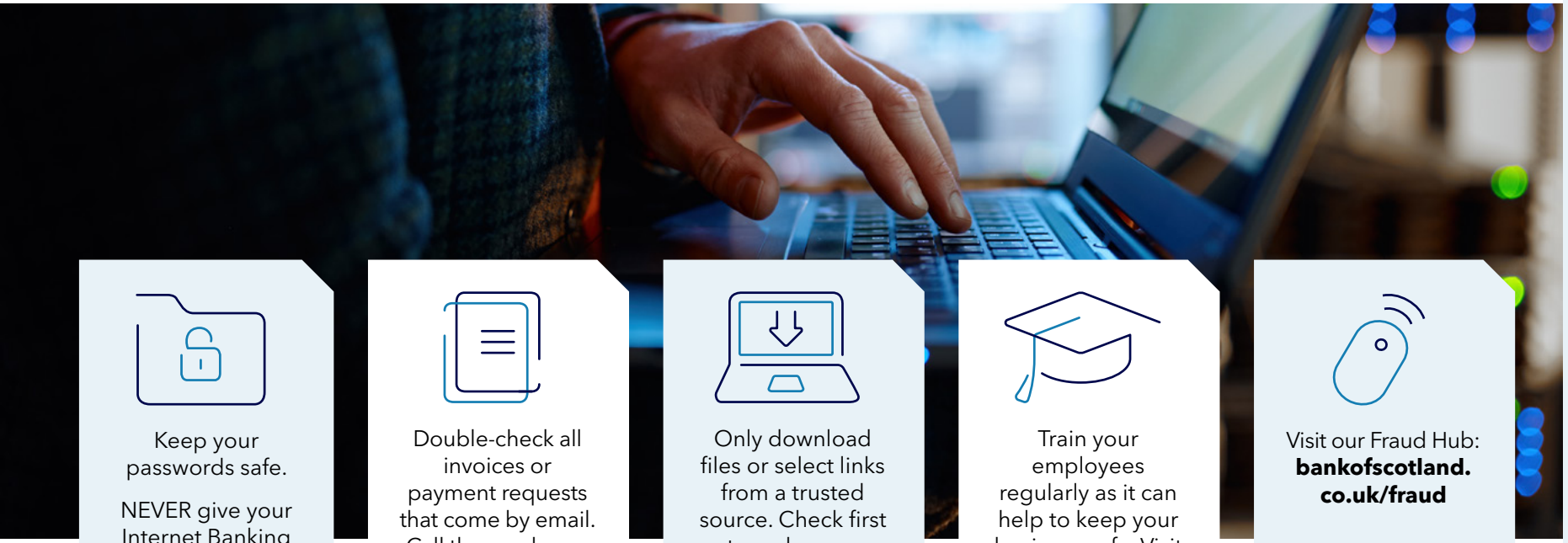
Or scan the QR code.



Contents

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 Internet 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 send an email impersonating a supplier or colleague. The email might include an earlier chain of genuine messages.
- 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.
- Use a telephone number that's known and trusted, not one from an email.

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.

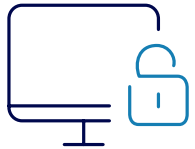
The business names used in this case study have been changed, to protect the identity of the genuine client.

Top tips
Email payment fraud
Ransomware
Scam calls
Scam messages
Buying online
Employee fraud

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.

Top tips
Email payment fraud
Ransomware
Scam calls
Scam messages
Buying online
Employee fraud

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.

A bit later, one of their computers displayed a message that says that 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.

Top tips
Email payment fraud
Ransomware
Scam calls
Scam messages
Buying online
Employee fraud

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 Internet 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 Internet Banking passwords and codes.
- Fraudsters use Artificial Intelligence (AI) to create deep fake audio and video of someone in a business. It appears 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 appears 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 Internet 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 disperses the money, 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.

Scam messages

The goal of the fraudster

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

How this scam works

- A text appears to have come from a bank or another trusted organisation.
- 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 genuine looking website will ask an individual to log on or give personal or confidential banking details.
- 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.

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.

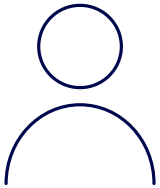
How to avoid this scam

- 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.

Our Service Promise
Please let us know if you have a problem – we're here to help. See our complaints process on our 'Help & Support' page at: **business.bankofscotland.co.uk/complaint**

Find out more

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.

1/4520996-6 (10/24)

BANK OF SCOTLAND
By the side of business