Payment Fraud & Scams: Tips to protect your business

Find out more about the different types of fraud with tips to help protect yourself and your business

HSBC UK

Contents

We all think fraud is something that happens to other people...

...until it happens to us. The truth is, we're all equally susceptible, but if we learn to spot the fraudster's tricks, we can better protect ourselves and our businesses to combat fraud together.

We've been hard at work developing tools and techniques that make banking safer, but it's not enough. We need your help. If we all work together and follow a few simple steps, we can be better protected and keep your money safe – and that's good for everyone. We recommend the Take Five Challenge to help protect yourself against fraud and scams:

Stop
If someone contacts you unexpectedly and claims to be from a trusted organisation, be suspicious. Take a moment to stop and think before sharing personal or financial information.

Challenge
Could it be fake? It's ok to reject, refuse or ignore any requests or simply say no. Only fraudsters will put you under pressure to act urgently.

Protect
Don't click on unfamiliar links or call numbers from texts or emails. Instead, check they're genuine by going to the official website. Fraudsters may appear genuine, but their actions and requests are not.

It's important to remember that we will never ask you...

Your PIN or full password, even by tapping them into your phone keypad.

Any codes that you generate or we send to you by any method for the access or operation of your account including your secure key, card reader or sent to you by SMS or email.

To move money to any other account.

Install software onto your device or ask you to download a chat portal to access your account or stop a fraudulent payment.

How can you protect yourself and your business?

- **Always question uninvited approaches**
  Instead, contact the company directly using an email or phone number that you can check is genuine. If possible, try and contact using a different method of communication.
- **Don't share personal or business information**
  Never reveal your password or one-time passcodes over the phone or via email. Be careful with the level of detail shared on social media sites and check your privacy settings.
- **Never mislead the bank about the purpose of a payment**
  Criminals will often try to persuade you to tell the bank that the payment is for a different purpose to what they have told you. They may suggest it will speed up processing or the bank may stop the payment otherwise. This is a clear sign of fraud.
- **Stay safe online**
  Always update your computer, tablet and smartphone's operating systems as soon as they become available and install anti-virus software from a trusted organisation. Consider using a Virtual Private Network (VPN) this will provide an encrypted connection to protect your privacy and information.

- **Offer training to your employees**
  Offering training to your employees helps them spot fraudulent activity and will strengthen your businesses front line defence, this is one of the most cost-effective fraud prevention tasks you can undertake.
- **Register for Voice ID**
  Consider registering for HSBC Voice ID, this is a form of biometric identification that verifies you through your unique voiceprint increasing your account security.
- **Update your passwords**
  Consider having a strict and complex password creation system in place for your business to make sure that passwords are strong and unique. Using Two Factor Authentication where it's offered will help keep your accounts safer by adding a second layer of protection.
- **Have a response and recovery plan in place**
  Have plans in place for when something happens and know what actions must take place if your business does fall victim to a fraud or cyber-attack. Make sure to test your plan regularly to make sure it works and it's effective.
- **Check bank and card statements regularly**
  Verify transactions against invoices, if there are any transactions you don't recognise, always contact us.
- **Cancel bank cards of previous employees**
  Cancel cards and online banking access for previous employees as soon as they have left the business to prevent unauthorised use.
- **Shop safe online**
  If you're buying something online and you don't know the seller, never pay by bank transfer. Always use credit card, debit card or PayPal – or a payment option that offers some protection against fraud.
- **Shred important documents**
  Shred any paperwork that reveals personal or business information, such as bank statements, card details and other sensitive data.
- **Check your credit report**
  Check both your personal and business credit reports at least once a year for any unusual activity.

Business Email Compromise – Payment/invoice diversion

Business Email Compromise is a type of Authorised Push Payment scam. This happens when a person or business is tricked into sending money to a fraudster posing as a genuine organisation.

Business Email Compromise may occur when an email account is:

- Spoofed by setting up an email address with subtle differences to the genuine email address to trick the recipient. For example, using letters that are similar such as using 'rn' instead of 'm'- J@rnbusiness.com instead of J@mbusiness.com.
- Compromised (hacked) by a fraudster through the use of malware (virus) or by obtaining the email password through another method, such as a vishing call.

Suppliers or other senior staff in your organisation can have their emails hacked – these can even carry on from previous email trails. Fraudsters use hacking or spoofing to make payment requests, which are often aligned with genuine activities of your business.

Tips to protect your business from Business Email Compromise

Do

- Always verify new payment details from suppliers by phoning a known contact, on a known telephone number or one from the company's official website, to check the sort code and account number. Never use a number in the email as this could be a fraudster.
- Implement a two-step payment verification process which includes a non-email check (e.g. phone/SMS) with the initiator.
- Check email addresses for granular details by looking for subtle differences, such as added letters, numbers, special characters or a different domain like .com instead of .co.uk.
- Always check the sender's name/email address, clicking on the name will reveal the full email address of the sender.
- When receiving payment instructions from within your organisation, verify payment details with the instructing party in person, where possible or by phoning them.

- Examine website links, email addresses and spelling in all correspondence as these can be giveaway signs of a fraudulent email.
- Consider blocking email auto-forwarding to make it harder for information to be stolen.

Don't

- Overshare personal information on social media – such as pet names, birthdays and family connections as this information could be harvested by fraudsters to and used to convince you they're contacting you from a genuine organisation.
- Open an attachment within an email or text which you're not expecting as this could infect your machine with malware.
- Act on urgency of a request. Take your time to validate the legitimacy of the communication.
- Be put off seeking a second opinion. If you're unsure if a request is genuine, don't action it and refer it to a colleague or manager.
- Leave it to chance. Make sure all staff receive training on fraud and scams and understand what Business Email Compromise is, how it can affect your organisation and how they can escalate concerns.

Business Email Compromise – CEO Fraud

CEO Fraud is where criminals impersonate the CEO or other senior members of staff in the organisation and send emails to the accounts department to make a large payment urgently. They often time this so that the manager they are impersonating is away and the details are difficult to verify, they impersonate senior management to play on their authority.

Remember, if you feel pressured, Take Five; Stop, Challenge, and Protect. Escalate concerns internally to your manager and report the incident to Action Fraud. Always take the time to validate the request.

Tips to help protect yourself and your business from CEO Fraud

Do

- Embed a risk culture where staff feel comfortable to escalate concerns.
- Read the communication carefully, check if the spelling and grammar is correct and check if the email matches company records.

- Verify the payment with the senior member of staff in person where possible, or by calling a phone number from a trusted source such as your company records, and not from the email.

Don't

- Feel pressured into making the payment, question its legitimacy and seek a second opinion from your manager or colleague.

If you run a business, email interception and CEO Fraud are the most common scams to be aware of.

For more information, visit business.hsbc.uk/fraud-centre.

Phone scams

Phone scams often start with an initial vishing call, where a fraudster calls you out of the blue, pretending to be your bank or another trusted organisation, vishing for information about you and your business. They can even use phone number spoofing, making their call appear to come from a number you know and trust.

Remote Access Takeover fraud

One of the most common types of payment fraud that criminals use is Remote Access Takeover. This is when someone calls you pretending to be from HSBC or another trusted organisation, such as the Police or a utility provider, and persuades you to provide online banking secure key codes to stop a "fraudulent" payment. However, they use these details to gain access to your online banking and make fraudulent payments.

Other phone scams used by criminals

- Safe accounts: advising you to transfer funds to a 'safe account', however, the account is in the criminal's control.
- Software downloads: advising you to visit a website, download software or access a 'chat link or portal' so they can remotely access your systems to help you with a problem or verify your IP address. However, this gives them greater access to your systems and information.

If they're successful in persuading you to download software:

- They may ask you to log in to your online banking so they can check your account. Then, whilst you're logged on, they'll remotely access your internet banking to make fraudulent payments without you knowing.
- The download may install malicious software 'malware', which they can use to steal your details for use at a later date.

- Call redirection: Asking you to key in *21* followed by a phone number – if you get cut off, however, this redirects all calls including fraud checks to the criminal's number.
- Card fraud: Fraudsters may advise you that your card details have been compromised and you either need to:
  - Confirm your card details so it can be blocked; in reality, they're using your card details to make payments.
  - Provide one-time passcodes to stop transactions; however, they may already have your card details and these codes are being used to make payments.
  - Return your card so a new one can be issued and advise you your card has been blocked; however, they're going to obtain your bank card and use it.
- Bypassing phone security: Fraudsters will sometimes advise they need to pass you to another department to pass telephone security. What they're actually doing is transferring you to the genuine financial institution to pass their telephone security checks. They then take over the call and attempt to deal with the company directly, instructing them to make payments.

Tips to help protect yourself and your business from Phone Scams and Remote Access Takeover

Do

- Keep your online banking log on details and secure key safe.
- Take your time and question if the request is genuine. If in doubt, terminate the call and call the organisation back on a genuine phone number such as one from their official website.
- Make sure you have a company procedure for staff to escalate concerns.
- Seek a second opinion if you're unsure if a request is genuine.

Don't

- Give out internet banking log on details, secure key codes or one-time passcodes to anyone – HSBC don't need these to stop payments.
- Always believe a caller is genuine, as phone numbers can be spoofed (copied). If you're unsure you are speaking to a representative from a genuine company then end the call and phone the organisation on a genuine number such as one from their official website, and if possible, use a different phone.
- Send funds to a 'safe account'. HSBC will never ask you to send funds to another account to safeguard them.
- Download any software on your machine – HSBC will never ask you to do this.

Investment scams

Investment scams claim to offer high returns for very little risk. Fraudsters often use false testimonials, fake celebrity endorsements, spoof websites, cloned companies, and other marketing materials to make the scams appear genuine. They often call out of the blue to offer you the opportunity to invest. They may have set up a fake business with a similar name to a genuine investment company, often creating fake websites, investment brochures and social media adverts to make their scam appear more legitimate.

Types of investment scams

- Fictious investments that don't exist.
- A genuine investment opportunity but the criminal doesn't place the funds in the investments.
- A criminal pretending to be a representative of a genuine investment company.

Ways to spot an investment scam

- It seems too good to be true – high returns for a low risk.
- False testimonials and fake celebrity endorsements, promoting lavish lifestyles on social media.
- You feel pressured into making a quick decision, for example if the caller states the offer is 'only available right now' or 'don't miss out'. Legitimate organisations will never pressure you into investing on the spot.
- You're approached out of the blue via phone, email, text message with an investment opportunity.

- The ‘company’ contacting you won’t allow you to call back.
- You may have been told to keep the opportunity to yourself.
- The only contact details you’re given is a mobile phone number or a PO box address.
- The company want to take control of your accounts or investments, especially when cryptocurrency is being used.

Tips to help protect yourself and your business from Investment scams

Do

- Carry out research on the investment and the company, don’t rely on word-of-mouth referrals, others personal experiences or celebrity testimonials. Take your time to understand the offer.
- Check email addresses and website domains very carefully for subtle differences such as added letters, numbers, special characters, or a different domain like .com instead of .co.uk.
- Use different communication channels, don’t rely on contact via social media, always verify over the phone on a genuine number such as one from the company’s official website.
- Get a second opinion; speak to trusted friends or family members or seek professional independent advice before conducting any investment.
- Ensure any cryptocurrency investment is held in your name and you have full access to the account/wallet.
- Visit the FCA website to check if the company or individual is genuine and regulated on the official registered list of companies. Check that the company or individual is authorised to undertake the activities they offer. There’s also a list of reported investment scams and cloned companies to check if you’re dealing with a known scam.
- If the investment company isn’t FCA regulated, you may not be covered under Financial Ombudsman (FOS). If the company is operating outside of the UK, contact the countries FCA equivalent.
- Research independent online reviews about the company/investment to check for consumers’ recent experiences, don’t trust those on the company’s website as they could be fake.

Don't

- Trust something which seems too good to be true – high returns for a low risk rarely ever occurs.
- Feel pressured into making a quick decision. For example, if the caller states the offer is 'only available right now' or 'don't miss out'. Legitimate organisations will not pressure you into investing on the spot.
- Trust out of the blue contact via phone, email, text message or by someone calling at your house with an investment opportunity.
- Take it for granted that someone you know have conducted thorough checks when recommending an investment opportunity, always do your own research.

Email and Text Message Scams

Email scams (phishing) and Text message scams (smishing) are when a fraudster contacts you pretending to be from your bank or another organisation that you trust.

Often the email or text is encouraging you to share personal details or to click on fake links, they may even tell you that there's been fraud on your bank account.

Clicking on a fake link may result in you being targeted in different ways, like a phone call from 'your bank's fraud department' or inviting you to take up special offers. If you input your personal or business information into the link, you may be a target for future phone scams or other scams, or it may lead to the hacker installing malware or ransomware onto your device to steal your information or bribe you.

Typical examples of phishing and smishing

- An email or text from 'HMRC' advising you're owed a tax refund.
- An email from your solicitor providing new bank details for a deposit for a property purchase.
- Receiving an email or text from a courier advising you they have a parcel for you, but you need to pay a fee in order to obtain it.
- An email or text from HSBC or any other financial institution asking you to update your banking details or asking you to move your money to a 'safe account'.
- An email or text company tells you your payment has failed and to click on a link to update your bank details or make a payment.

Tips to help protect yourself and your business from phishing/smishing

Do

- Check the email address for any subtle irregularities, such as the email address not matching the website address of the organisation it says it's from – hover your cursor over the sender's name to reveal the true address.
- Check the content of the email – look out for spelling or grammatical errors.
- Forward suspicious emails to the Suspicions Email Reporting Service at report@ phishing.gov.uk
- When selling a phone/device or when giving it away, make sure to conduct a factory reset on the device. This will clear all of your data and content from it. Instructions on how to complete this for your device can be found in the user guide.
- Forward suspicious text messages to 7726 to report them to your phone operator.
- You can check the contact is genuine by contacting the organisation on a genuine number such as one from their official website.
- Delete the email/text message.

Don't

- Rush and make an urgent payment.
- Click on any links immediately, they may contain malicious malware – hover your cursor over the link to reveal it's true destination, as criminals are looking to steal your personal information.
- Give out any personal information which the email demands from you.
- Trust any out of the blue contact from a number or email address which you don't recognise.

Additional Resources

HSBC Website
The new HSBC UK Business Banking Fraud Centre offers education, support, and guidance, to help protect you and your business from fraud and cybercrime. The webpage has the registration details of upcoming Fraud and Cyber awareness webinars, which are open to everyone, as well as access to previous recordings. Please visit business.hsbc.uk/fraud-centre.

If you think you've been a victim of a fraud or scam, please report it to us following the instructions on our website at business.hsbc.uk/fraud-reporting.

If you suspect fraud on your account, pop into your local branch or call us on 0345 760 6060.

National Cyber Security Centre (NCSC) is a UK government organisation which provides advice and support for the public and private sector in how to avoid computer security threats. They provide free resources which your business and employees can use to help educate yourself and your staff about how to spot fraudulent activity.

Report a phishing email at report@phishing.gov.uk.

National Cyber Security Centre

Action Fraud is the UK's national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. Report frauds, scams, and cyberattacks using the online reporting service at actionfraud.police.uk available 24/7, the service enables you to both report a fraud and find help and support. Alternatively, you can talk to their fraud and cybercrime specialists by calling 0300 123 2040.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Take Five is a national campaign offering straightforward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate a trusted organisation. Please visit the Business Advice section of the Take Five website at takefive-stopfraud.org.uk/advice/business-advice.

TAKE FIVE
TO STOP FRAUD™

STOP CHALLENGE PROTECT

Accessibility

If you need any of this information in a different format, please let us know. **This includes large print, braille, or audio.** You can speak to us using the live chat on our website, by visiting one of our branches, or by giving us a call.

There are also lots of other options available to help you communicate with us. Some of these are provided by third parties who are responsible for the service. These include a Text Relay Service and a British Sign Language (BSL) Video Relay Service. To find out more please get in touch. You can also visit: business.hsbc.uk/accessibility or: business.hsbc.uk/contact-us.

business.hsbc.uk

HSBC UK Bank plc. Registered in England and Wales (company number: 9928412). Registered Office: 1 Centenary Square, Birmingham, B1 1HQ. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register number: 765112).