Protecting your business from payment fraud and scams

Businesses are at risk of being targeted by fraudsters and cyber criminals, especially when making payments for products or services. Businesses are often targeted because criminals know payments are made regularly, often for substantial amounts.

HSBC UK

Common payment fraud and scams

Business Email Compromise

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

Business Email Compromise is when an email account is:

- spoofed by setting up an email address with subtle differences to trick the recipient for example J@**rn**business.com instead of J@**m**business.com, or
- compromised (hacked) by a fraudster through the use of malware (virus) or by obtaining the email password through another method (e.g. 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, these may be timed or align 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 to check the sort code and account number. Never use a number in the email as this could be the 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**.

Do	✔ 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. ✖ Open an attachment within an email or text which you're not expecting or appears suspicious. ✖ Act on the urgency of the 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.

Remote Access Takeover

One of the most common types of payment fraud that criminals use to target businesses is Remote Access Takeover. This is typically 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 internet banking secure key codes to stop a "fraudulent" payment. However, they use this to gain access to your internet banking and make fraudulent payments.

Other tactics used by criminals are listed below.

- Advising you to transfer funds to a 'safe account' and getting you to download software so they can gain remote access to your devices.
- 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.

Tips to protect your business from Remote Access Takeover

Do	✔ Keep your internet banking log on details and secure key safe. ✔ Take your time and question if the request is genuine. Conduct some further checks and research before taking any action. ✔ 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 including HSBC. ✖ Always believe a caller is genuine, as phone numbers can be spoofed (copied). If you're not sure you're speaking to a representative from a genuine company then end the call and phone the organisation on a genuine number from their website, 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 remote access software on to your device.

Checklist for making payments

When setting up a new payee or if a supplier asks for account details to be updated, ring a known contact on a known phone number and check the sort code and account number. Never use a number in the email trail as this could be a fraudster.	☐
Check the invoice and the email it's attached to carefully. Check the email address including the domain name. Don't rely on the displayed sender's name - you can often click on the name to reveal the full email address of the sender.	☐
If you're making the payment via a web browser, check the website address (URL) to make sure you're on the correct website.	☐
Pay attention to 'Confirmation of Payee' checks and the results conducted on UK payments where applicable.	☐
Check the email for spelling, grammar and punctuation mistakes, as scam emails commonly contain errors. Does the language and tone of the email seem normal for that contact?	☐
Don't click on any links or open any attachments if you have any reason to believe the email isn't genuine.	☐
If the request is coming from within your organisation, confirm the details in person, where possible.	☐
If you're unsure if a payment request is genuine, don't make the payment and escalate your concerns.	☐

Reporting fraud and scams

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

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 with 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).

Customer Information: Customer Service Centre, BX8 1HB.