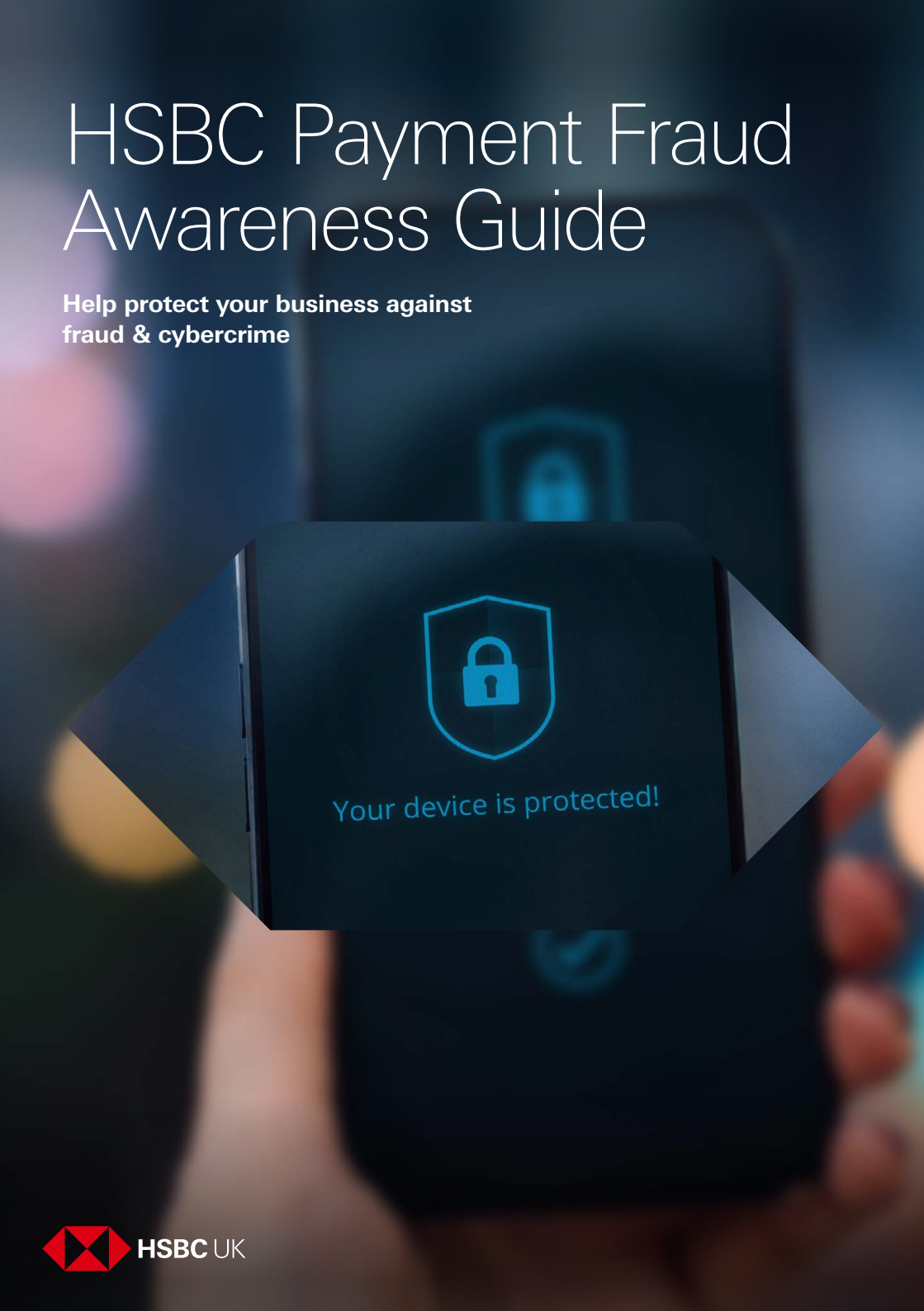
HSBC Payment Fraud Awareness Guide

Help protect your business against fraud & cybercrime



HSBC UK

Contents

Payment Fraud and Scams: protect your business

Useful information for you

Fraud is one of the most common threats to businesses today.

Payment fraud can result in significant financial losses. Businesses of every size are at risk. This guide is designed to equip you and your staff to spot and prevent payment fraud and scams, and to take the right steps if you fall victim.

$10.2bn

Global cost of reported business email compromise in 2022
Source: FBI Internet Crime Complaint Centre

This guide will help you learn about common fraud and scams that could impact your business and outlines some practical steps you can take to prevent your business from falling victim to fraudsters. Education on this topic across an organisation makes for a better protected business, and this guide provides a number of tips and checklists which can be shared across management and payment teams.

Types of Payment Fraud and scams which could impact your business

How a fraudster might contact you

- **Authorised Push Payment** - (APP) scams happen when a business is tricked into sending money to a fraudster posing as a genuine payee. It's important to understand how criminals may get in touch.
- **Phishing** - a common theme in many APP scams. This describes attackers' attempts to trick users into clicking on a link that will download malware for example, or direct them to a fake website.
- **Vishing** - if you receive an unexpected phone call about money, there's a good chance it's a scam. Scammers may claim to be a business or authority you know and trust, like your bank or the police. They may know personal details about you and can even make their phone number look authentic using a technique called 'number spoofing'.
- **Smishing** - this is where scammers send fake text messages, pretending to be your bank or another legitimate organisation. Their goal is to make you reply with your personal or financial details so they can steal money from your account. Fraudsters may also utilise common messaging platforms.

Business Email Compromise

Useful information for you

Fake emails are a common tool used in scams.

When payments are due, criminals send an email designed to look and read like a genuine message from a supplier. They tell you the bank details for your payment have changed, provide new details and request payment.

These can be hard to spot for the following reasons:

- The attackers often use the vendor's regular email address, or a spoofed email address, which looks just like the legitimate address.
- They will make invoices look authentic.
- There may be no perceptible difference in the vendor employee's email signature or communication style.
- In some circumstances, the attacker may have gained access to the legitimate inbox, so it will be coming from an authentic email address. The attacker will have access to the email chain and will be able to reply using similar language and tone.
- **Often, the payment being requested by the criminal is due with the legitimate supplier and the only difference is that the business' bank details have changed.**

How does email compromise happen?

Email account takeover

- The attacker uses hacking or stolen account credentials to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user's contacts, email style and personal data, to make their messages more convincing.

Email impersonation

- The criminal sets up an account with a very similar address to the real one.
- Alternatively, they may use a spoof email envelope and header, hoping the recipient won't notice and that they engage with it like they would with a legitimate email from the supplier.

CEO fraud

Useful information for you

Criminals impersonate a senior manager in the company.

- They send an email to the accounts department, requesting that a large payment be made urgently. This could even be for an acquisition or other important transaction.
- They often time this so that the manager they are impersonating is away, and the details are difficult to verify.
- Again, the email account may have been compromised through phishing or a data breach, with information gathered through company websites or social media.

Other Common Attack Types

Vishing and Telephone Scams

A phone scam, or vishing, is when a fraudster calls pretending to be your bank or another trusted organisation. They can even make their call appear to come from a number you know and trust. This is known as 'Phone Number Spoofing'.

They can sound very convincing and may already know some of your personal information, such as your account number or address. If you feel uncomfortable, or sense something is wrong, don't be afraid to end the call.

You can always call the organisation on a number that you know, such as the number on the back of your bank card.

Fraudsters can keep the line open and even spoof a dial tone, so try to use a different phone, or wait at least 30 seconds before making your call.

Typical examples include:

- 'Your bank' advise you that your account is at risk and you need to move your money to another account to keep it safe.
- 'Your bank' needs your help to investigate a fraud.
- Your internet or mobile provider calls you to fix a problem you haven't reported.

> A bank can already transfer funds at your request and would never ask for your passwords, PIN, any One Time Passcodes or secure key codes.

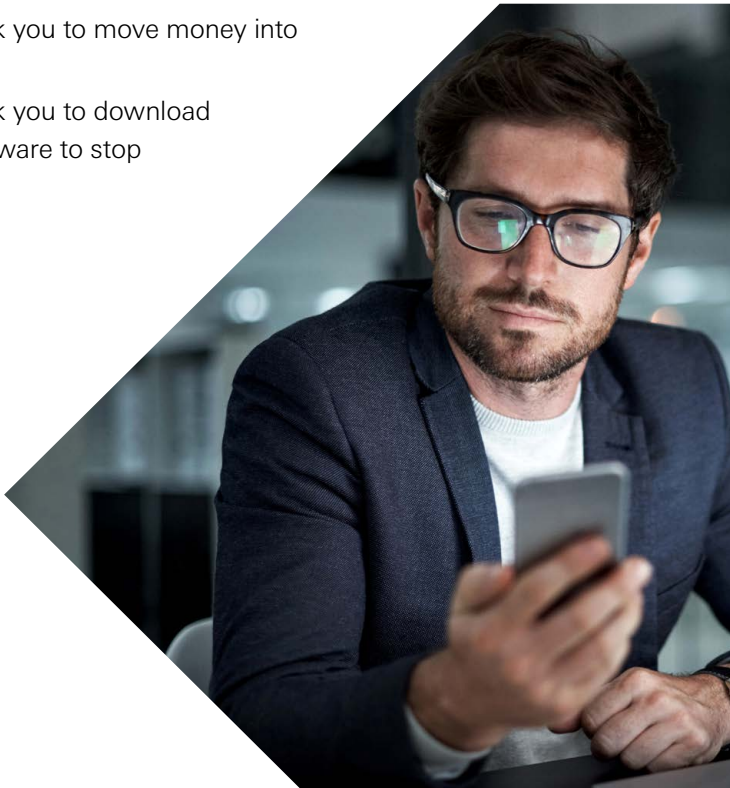
Account takeover fraud

Fraudsters may contact you by telephone, often from "spoofed" telephone numbers displaying a legitimate number from the company they're purporting to be. Fraudsters know company practices inside out and will take you through the process you'd usually expect, in order to gain trust. For example, a verification process.

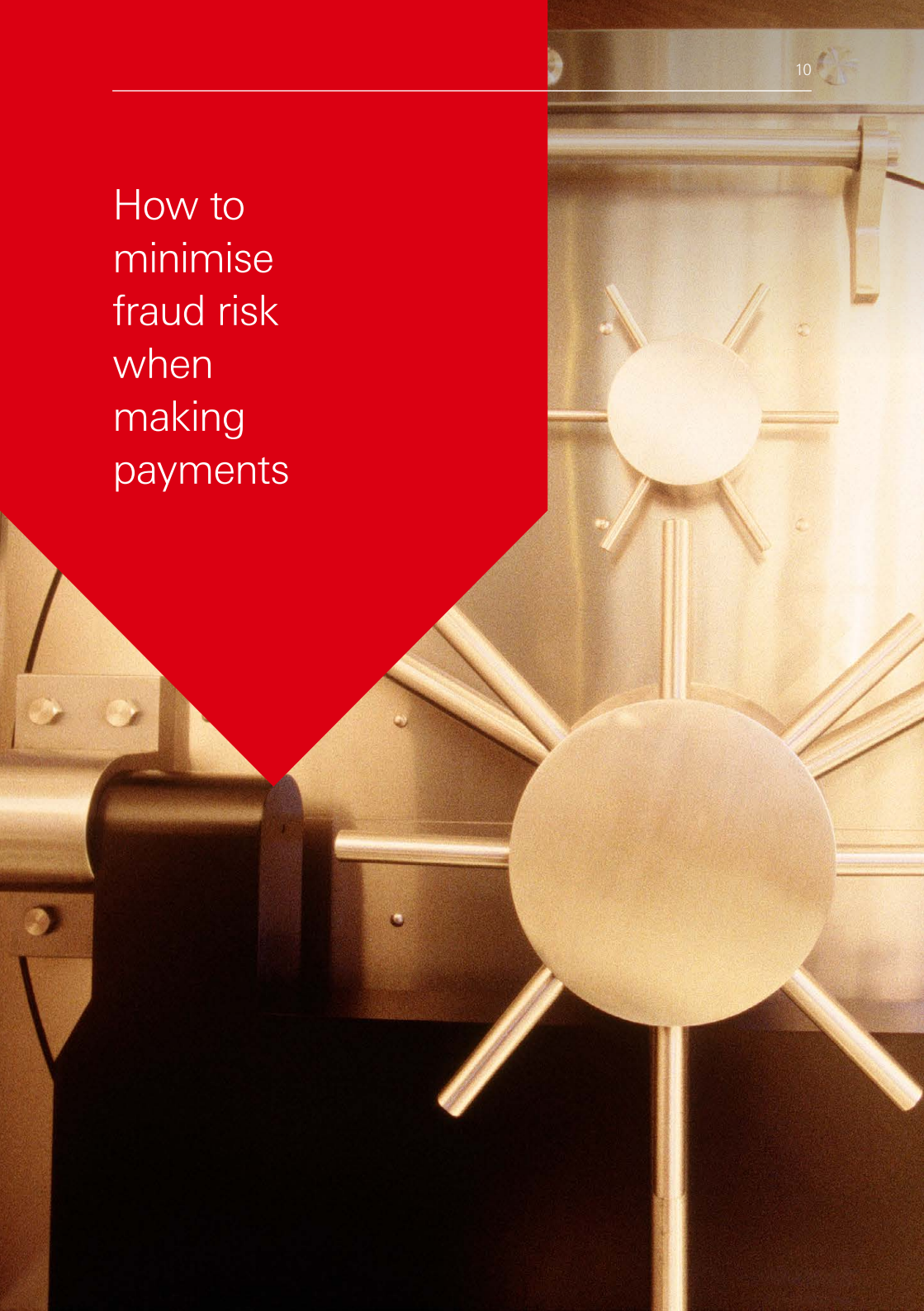
They'll then use various methods to trick you into providing them with security details, such as usernames, passwords and secure key codes. Fraudsters can then use this information to successfully take over your account and pay funds away.

Remember:

- HSBC will never ask you for card PIN numbers, passwords or secure key codes.
- You should never disclose secure codes to anyone.
- HSBC will never ask you to move money into a secure account.
- HSBC will never ask you to download remote access software to stop a payment.



How to minimise fraud risk when making payments

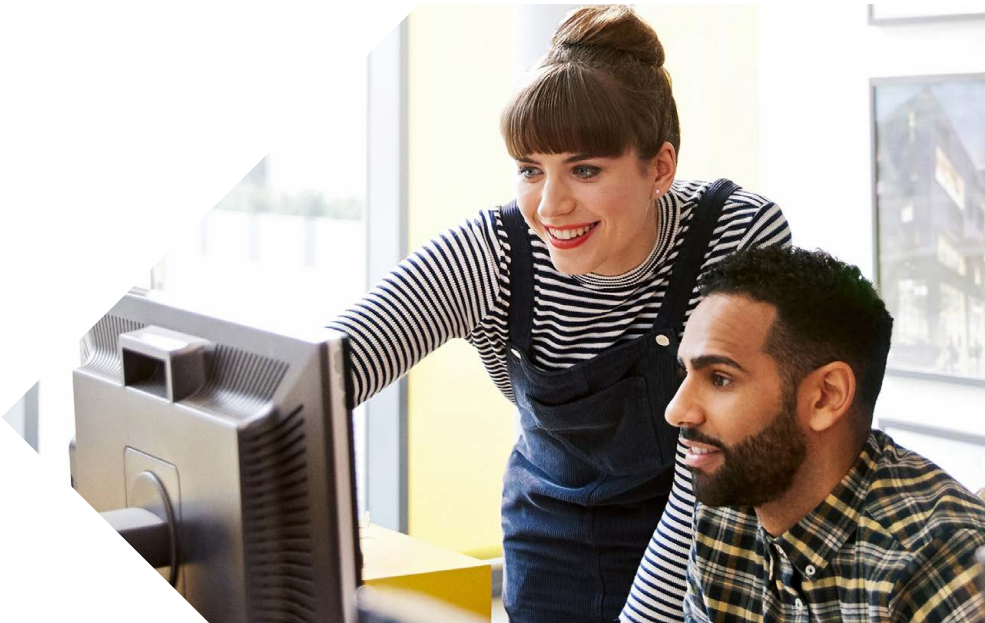


Minimise payment fraud risk

There are steps every business can take to minimise payment fraud and scam risk that don't need to be complicated or expensive. Everyone has a role to play.

These steps include:

- Fostering a sense of vigilance in the parts of your business that could be vulnerable.
- Educating employees about how to identify and avoid scams, and make sure they're aware of the company's security policies and procedures.
- Querying any requests which seem unusual or out of context.
- Most importantly, **any new payee or account details need to be verified before making any payments**.
- The next few slides provide more detailed guidance to support individuals responsible for payments.



Check the email address

Useful information for you

Fraudsters will pose as reputable individuals.

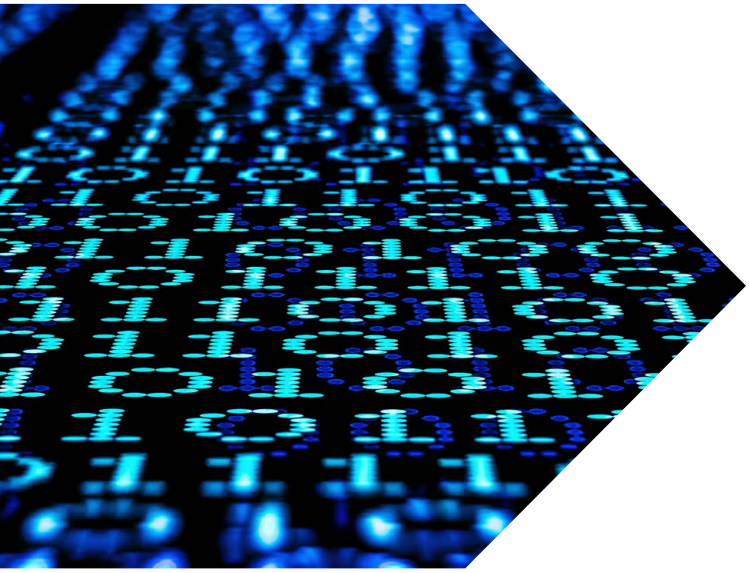
- If the name attached to the email is familiar (someone you know or regularly correspond with), check to be sure the email address matches.
- If it's a co-worker, the email address should be listed in the company email directory (if you have one).
- Be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one, but will alter a letter or two hoping that recipients don't notice. For example, J@rnbusiness.com instead of J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

Check the email thoroughly

Useful information for you

Urgency is a red flag.

- Treat any ‘urgent’ email relating to payments as suspicious – this could include providing excuses for the lack of a call back option.
- Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. Treat external emails with extreme caution, especially those containing links or attachments. Be aware that Generative AI is making it easier for attackers to create convincing malicious emails.
- If you’re not expecting the communication and/or don’t recognise the sender, **do not click links or open attachments**.



Verify new payee or change of account details

Useful information for you

Check with the instructing party using known contact details.

- Where possible, try to speak to someone you know. For example, if the change request is coming from someone within the business, try to confirm it directly with that individual by telephone.
- If it's from a supplier, speak to your normal contact by telephone. Remember to also check the sort code and account number.
- Don't reply to the email or use contact details within the email.
- Often, cybercriminals are sending phishing emails to individuals in the contact lists of the account that they've gained access to. That means you may recognise the sender because the email address is accurate, though the message itself is suspicious. By calling your known contact, they can verify the request in the email is genuine. If not genuine, it may also alert them that their email account has been compromised.

Minimise the risk of payment fraud

Fraud can happen to any type of business and in many different ways. Luckily, there are steps you can take to help protect your business against fraud and cybercrime. Here's a summary of some top tips and useful checklists you can utilise to help mitigate fraud risk within your business.

Top tips

Create and embed clear security procedures for payment teams

Making sure all payments are properly validated is the most important action in fraud prevention. Create a procedure to prevent payment teams authorising new or amended payments without proper validation. Following this procedure should mean that payment teams never move money based solely on unverified email or telephone instructions, even when they appear trustworthy. Best practice is to encourage staff to contact payees directly to confirm new or amended payment requests.

Raise employee awareness

Provide employees with adequate training. Fraud awareness is everybody's responsibility within an organisation. Create a risk-based culture and have a procedure for staff to escalate concerns to management. Staff should feel able to challenge and query instructions.

Encourage all staff to think before they click

It's fine to click on links when you're on trusted websites. However, avoid clicking on links that appear in unverified emails and instant messages. If you hover over a link, you will be able to see the hidden URL and verify its legitimacy. Double check email addresses and look out for poor spelling and grammar before clicking on any links or downloading any attachments.

Strengthen your passwords

Consider password managers or using a passphrase – a string of words that are typically longer than a traditional password. Passphrases are easy to remember, but very difficult to crack. Encourage employees to choose three random words and to select a mixture of alpha-numeric characters and symbols.

Know what do in an event of a fraud/cyber-attack

If you or your company fall victim, it's important to act quickly. Reporting known or suspected security incidents helps protect the workplace. Contact your financial institution.

Checklist: Senior Management

The most cost-effective way to limit the impact of payment fraud is to prevent it from occurring in the first place. This checklist is designed to help provide some key tips for keeping your business safe.

- [ ] Does your business have procedures that require validation of new or amended payment instructions? Do staff know where they can source known contact details?
- [ ] Have you got protocols around how, who and by what means staff can request payments to be made and how these can be verified if there are concerns?
- [ ] Are passwords of a suitable strength (e.g., minimum character lengths, use of alphanumeric and symbols). Have you considered using a password manager or mandate the use of passphrases?
- [ ] Has two-factor authentication been considered and applied where possible?
- [ ] Do your staff know what to do in the event of a fraudulent payment being sent?
- [ ] Do you have an incident response plan for cyber incidents, i.e., a compromised email address?
- [ ] Do you regularly discuss the potential risks of fraud with individuals submitting payments?

Checklist: Processing payments – 1 of 2

It's important to adopt a general mindset of awareness and action in the parts of your business that could be vulnerable. The checklist below has been created to support individuals responsible for making payments and to harbour a culture of fraud awareness.

- [ ] **Ask yourself - is the request unusual or out of context and does it make sense?**
  Any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a call back option should be treated as extremely suspicious. If you're not expecting the communication and/or do not recognise the sender, **do not click any links or open any attachments**.

- [ ] **Check that the email address is legitimate**
  If the name attached to the email is familiar (someone you regularly correspond with), check to **be sure the email address matches**. Fraudsters will pretend to be reputable individuals. If it's a co-worker, the email address should be listed in the company email directory (if you have one).

  Also, be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one but will alter a letter or two so that the recipients don't notice e.g., J@rnbusiness.com instead of J@mbusiness.com. Be aware that the displayed name can be hiding the actual sender's email address.

☐ **Question the payment if you're unsure, even if it's coming from senior management**

Fraudsters know you're more likely to act on instructions from senior individuals. As such, don't trust payment instructions received by email, even if they're from a senior executive or business partner. Fraudsters may also use common messaging platforms to facilitate fraud.

⚠ Remember, the fraudster might have access to the inbox you are corresponding with.

Checklist: Processing payments – 2 of 2

Verification of new and amended payment details are vital to limiting the impact of payment fraud and scams. Whilst it's important to perform callbacks, there are a number of additional considerations to make sure you minimise the risk.

☐ **Verify all new payees and all requests to change account details**

Check with the instructing party using known contact details. Where possible, try to speak to the individual accountable for the change in details. If it's from a supplier and you speak to your normal contact, ask them to confirm with the accountable individual by telephone. Remember, the fraudster might have access to the inbox of that individual, so validating the instructions on email could mean the response is coming from the fraudster!

- Don't reply to the email or use contact details within the email. If the fraudsters have gained access to someone else's account, they will likely change the contact details and you could end up speaking to the fraudster.
- Call the requesting party, do not rely on them calling you. Fraudsters know that a call-back could be part of the process so might try to navigate this step by contacting you first.

⚠ Remember that once a payment has been released, it's not always possible to recover the funds.

What to do if you fall victim

If you fall victim to payment fraud

Act immediately to minimise the damage from fraud and to make sure the best chance of recovering funds.

- **Stop all communication** with the fraudster.
- **Alert any relevant parties** (employees, customers and financial institutions). It's extremely important to contact the bank with a view to initiating a payment recall as soon as possible. Funds move very quickly and it's not always possible to recover funds.
- **Report the fraud** to the appropriate authorities.
- **Review your financial records** to identify any unauthorised transactions or suspicious activity.
- **Keep all documentation** related to the fraud, including emails, invoices and any other correspondence.
- **Review and update your security policies** and procedures.

Reporting fraud to HSBC

If you believe there's a fraudulent bank transfer or bill payment that you didn't authorise, you can contact us between 8:00am to 8:00pm, Monday to Sunday on:

- 03452 669 337 if you're calling from the UK.
- +44 1470 697 107 if you're calling from outside the UK.
- 0800 169 9903 if the payment was made through HSBCnet (lines open 24 hours a day, 7 days a week).

If you've authorised a bank transfer or bill payment and now believe you've been the victim of a scam, you can call us 24 hours a day, 7 days a week on:

- 03455 873 523 if you're calling from the UK.
- +44 1226 260 878 if you're calling from outside the UK.
- 0800 169 9903 if the payment was made through HSBCnet (lines are open 24 hours a day, 7 days a week).

If you suspect you may have divulged your security details, please call 03455 873 523 if you're calling from the UK or +44 1226 260 878 if you're calling from outside the UK.

We recommend you also report fraud to Action Fraud by calling 0300 123 2040 or online at actionfraud.police.uk.

If you suffer a cyber attack

- **Disconnect the affected devices** from the internet to prevent the spread of malware or further unauthorised access.
- **Change the passwords** for all affected accounts, including email, network, and any other accounts that may have been compromised.
- Use a reputable security firm to **conduct a full audit** of your systems to identify any other vulnerabilities or breaches.
- **Alert any relevant parties**, such as employees, customers, and regulatory authorities, and provide them with any necessary information.
- **Determine the source** of the attack and take steps to prevent similar attacks in the future.

Jargon buster

Fraud and cyber terms you need to know

- **Anti-Virus** – a computer program used to prevent, detect and sometimes remove malicious software.
- **Bring Your Own Device (BYOD)** – a policy implemented by businesses that allows an employee to use their own personal electronic devices for work purposes.
- **Common Vulnerabilities and Exposures (CVE)** – a publicly available list of known security vulnerabilities, indexed with unique ID numbers, descriptions and references.
- **Cryptocurrency** – peer-to-peer decentralised, digital currencies that are traded like a commodity.
- **Cyber-attack** – malicious targeting of computer systems, networks, infrastructures or devices.
- **Cyber incident** – defined by the National Cyber Security Centre (NCSC) as a 'breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)'.
- **Dark web** – the portion of the internet that isn't indexed by a search engine and is only accessed with special permissions or software.
- **Digital footprint** – a trail of data left behind after internet use. This can include passive information such as stored cookies, or information that's been actively placed on the internet, such as social media posts.
- **Encryption** – the process of mathematically scrambling data. This data can be encrypted at rest, like data saved to a hard drive, or in transit, like data sent via HTTPS between your web browser and your bank's server. Encrypting data doesn't make it invisible to malicious cyber actors; it simply converts it into useless, unintelligible gibberish.
- **Firewall** – a network security system that monitors and controls incoming and outgoing network traffic based on a set of rules.

- **Hacker** – a person engaged in a wide range of computer network exploitation (CNE). 'Black hat' hackers generally conduct malicious CNE, whereas 'white hat' hackers conduct CNE for the benefit of cyber defences.
- **Malware** – an umbrella term for a wide variety of malicious code designed to accomplish nefarious goals such as providing remote access, loading or dropping additional malware, stealing bank information, encrypting and denying access to data, or hijacking a device's computing power.
- **Patching** – process of updating an existing software or hardware to fix known bugs and vulnerabilities.
- **Penetration testing (pen testing)** – a process used by organisations to probe their own security with tactics used by cyber threat actors, usually conducted by 'red teams' or teams of professional white hat hackers.
- **Phishing** – usually conducted via email, this is a message designed to trick the recipient in to disclosing sensitive information, click a malicious link and/or open a malicious attachment. Phishing is often used to establish initial access on a device or network.
- **Ransomware** – a type of malicious software that blocks or otherwise restricts access to data under the promise that the restriction will be removed once a ransom has been paid.
- **Smishing** – a phishing message via SMS/text message.
- **Social engineering** – the manipulation of people to perform an action, usually to disclose personal information.
- **Spear phishing** – a phishing message that has been directed to a specific person or select group of people.
- **Trojan** – malware disguised as a seemingly innocent file or program in an effort to convince a potential victim that it can be opened safely. Trojans are very common and are frequently delivered via phishing emails or loaded by other malware called 'loaders'.

- **Two-factor authentication (2FA)** – a process of authentication where a user is required to have two factors, such as a known password and a one-time passcode (OTP). Generally, these factors are categorised as something you know (a password), something you are (a fingerprint), or something you have (a key card).
- **Virtual Private Networks (VPN)** – allow for secure private connections over public infrastructure, originally developed for use by organisations to authenticate the employee to internal network resources like email servers or shared folders. Today, consumer VPNs are increasingly used by individuals to create encrypted connections to a VPN server of their choice and use that server to connect to other internet resources.
- **Vishing** – a phishing attempt via phone call with a heavy use of social engineering.
- **Zero-day vulnerability** – a vulnerability identified prior to a patch or update being issued. Malware that exploit's such a vulnerability is commonly referred to as a zero-day exploit.

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 service 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).