

# HSBC Payment Fraud Awareness Guide

Help protect your business against fraud & cybercrime



# Types of payment fraud & 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** is 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** 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

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:

- 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 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 & tone.
- Perhaps most importantly – often the payment they are requesting is actually due.
- **Often the only difference is that the business's 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.
- Or they may use a spoof email envelope and header, hoping the recipient will not notice and engage with it as with a legitimate message.

## CEO fraud

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 difficult to verify.
- Again, the email account may have been compromised through phishing or data breach, and information gathered through company websites or social media.

# Other Common Attack Types

## Vishing & Telephone Scams

Phone scams, or vishing, are 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 code.**

## Account takeover fraud

Fraudsters may contact you via telephone, often from "spoofed" telephone numbers displaying the HSBC telephone banking number or that of the company they are purporting to be. Fraudsters know company practices inside out and will take you through the process you would expect in order to gain trust. For example, a verification process.

They will then use various methods to trick you into providing them with security details such as usernames, passwords, 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.
- 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 do not need to be complicated or expensive. Everyone has a role to play.

- Foster a sense of vigilance in the parts of your business that could be vulnerable.
- Educate employees about how to identify and avoid scams, and make sure they are aware of the company's security policies and procedures.
- Query any request that is unusual or out of context.
- Critically, **any new payee or account details need to be verified.**
- The next few slides provide more detailed guidance to support individuals responsible for payments.



# Check the email address

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 vs J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

# Check the email thoroughly

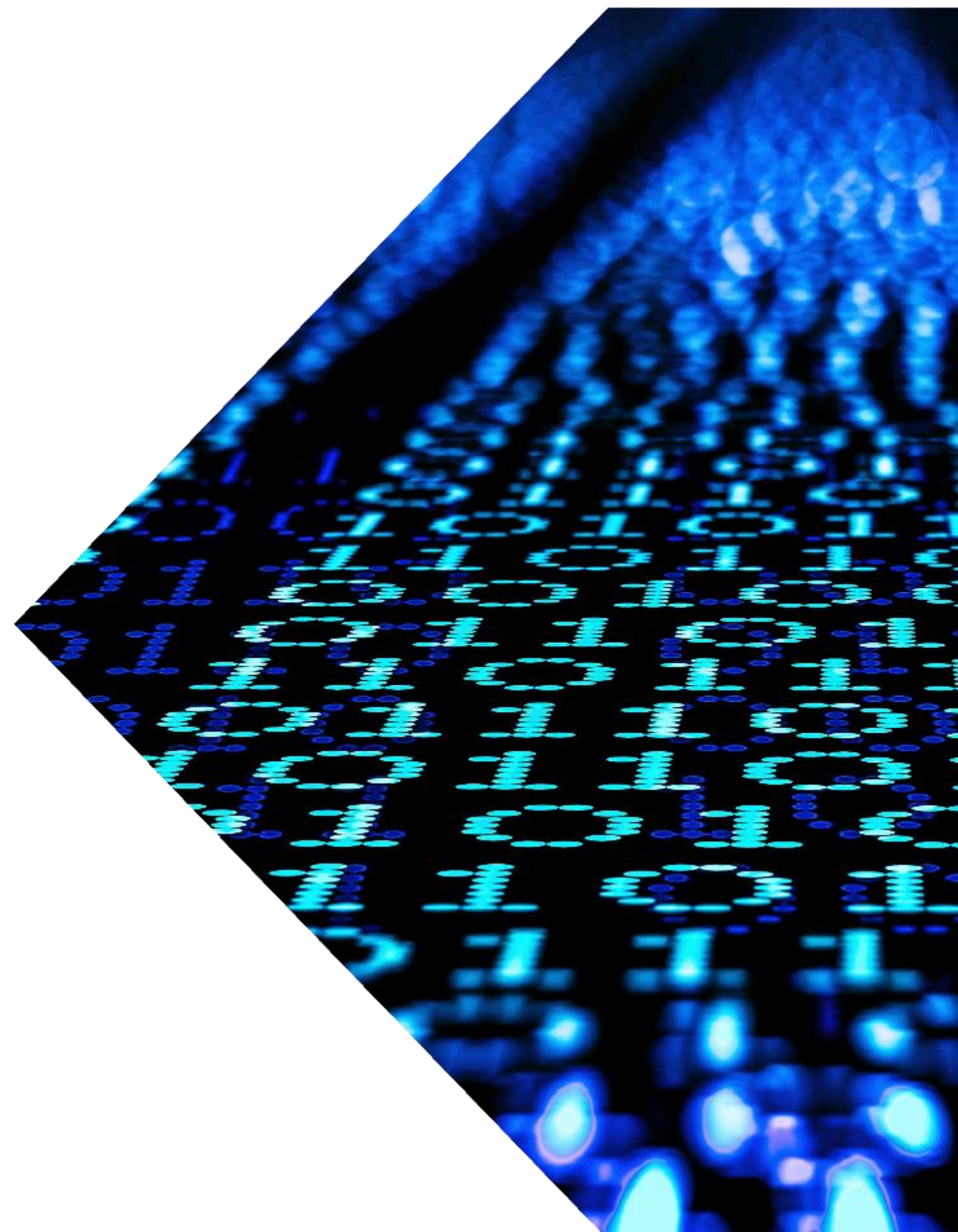
Urgency is a red flag.

- Treat any email relating to payments as suspicious if it uses urgent language or provides 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 are not expecting the communication and/or do not recognise the sender, **do not click links or open attachments.**

# Verify new payee or change of account details

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 is 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 to which they've gained access. That means you may recognise the sender because the email address is accurate, though the message itself is suspicious. Calling your contact verifies the request in the email. 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 round up 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**

Ensuring 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 is 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 is 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.

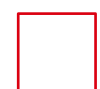
- Ask yourself is the request unusual or out of context? Does it make sense?**  
Any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a call back option should be treated as extremely suspicious. If you are not expecting the communication and/or do 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 vs J@mbusiness.com. Be aware that the displayed name can be hiding the actual sender's email address.
- Question the payment if you are unsure, even if it's coming from senior management.**  
Fraudsters know you are more likely to act on instructions from senior individuals. As such do not trust payment instructions via email, even if they are 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 is vital to limiting the impact of payment fraud and scams. Whilst it's important to perform call-backs there are a number of additional considerations to ensure 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 is from a supplier and you speak to your normal contact ask them to confirm with the accountable individual **via telephone**. Remember, the fraudster might have access to the inbox of that individual so validating the instructions via 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 then 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 ensure the best chance of recovering funds.

- **Stop all communication** with the fraudster.
- **Alert any relevant parties** (employees, customers, and financial institutions). It is extremely important to contact the bank with a view to initiating a payment recall as soon as possible. Funds move very quickly and it can be very difficult to get funds returned once they have gone.
- **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

Worried you've been the victim of fraud? We understand that cybercrime threats and attacks can be frustrating and we're here to help. If you need help or advice, or want to report a problem, [contact us](#) or your [HSBC Relationship Manager](#).

## Need to report fraudulent activity

- If you have authorised a payment and now believe you have been the victim of a scam, or you suspect you may have divulged your security details, call [your local HSBCnet Support Centre](#) or your HSBC Relationship Manager.

## Received a suspicious e-mail

- Stop. Don't reply. Don't click on any links. Don't open any attachments. Report to your HSBCnet System Administrator and forward the e-mail to [hsbcnet.phishing@hsbc.com](mailto:hsbcnet.phishing@hsbc.com) and we'll investigate it.

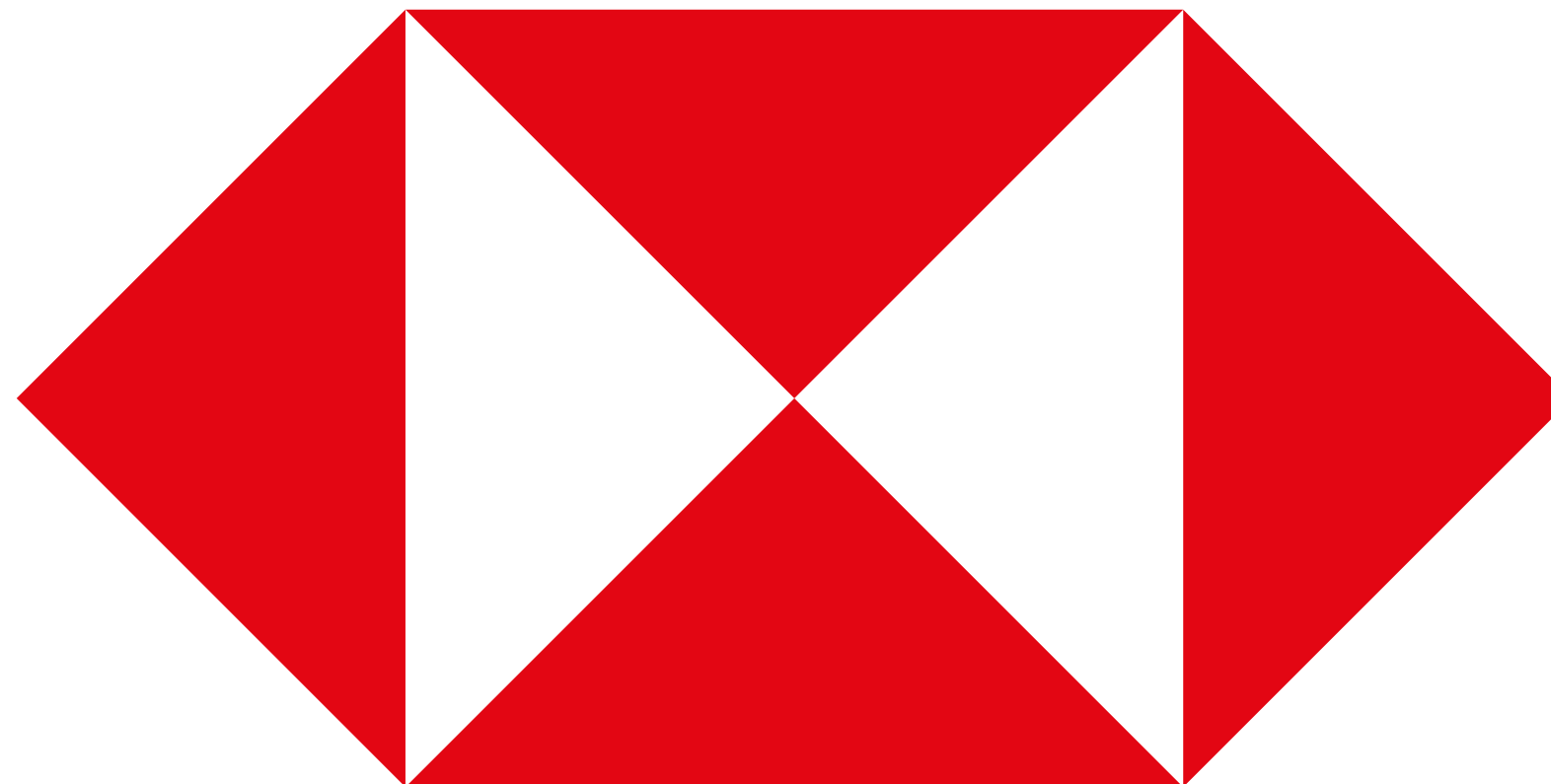
## Someone suspicious called me claiming to be from HSBC

- End the call and call back using a verified phone number to confirm the call is genuine. Don't provide any information to the caller. HSBC will never ask you to provide the code generated by your Security Device.

Uncover [useful information](#) on specific types of cyber attack and advice on how to mitigate the risk of them happening to you.

In case you have been a victim of Fraud, we recommend you raise a Police case with local authorities.





Issued by: HSBC Bank Middle East Limited U.A.E Branch, P.O.Box 66, Dubai, U.A.E, regulated by the Central Bank of the U.A.E for the purposes of this promotion and lead regulated by the Dubai Financial Services Authority.

Distributed by:

- HSBC Bank Middle East Limited Kuwait Branch P.O. Box 1683 Safat 13017, regulated by the Central Bank of Kuwait, Capital Markets Authority for licensed Securities Activities for the purposes of this promotion and lead regulated by the Dubai Financial Services Authority.
- HSBC Bank Egypt S.A.E., P.O. Box 124, Maadi, Cairo, Egypt.
- HSBC Bank Middle East Limited Qatar Branch, P O Box 57, Doha, Qatar, regulated by Qatar Central Bank for the purposes of this promotion and lead regulated by the Dubai Financial Services Authority.
- HSBC Bank Middle East Limited Bahrain Branch, P.O. Box 57, Manama, Kingdom of Bahrain, licensed and regulated by the Central Bank of Bahrain as a Conventional Retail Bank and lead regulated by the Dubai Financial Services Authority.
- Issued by HSBC Bank Middle East Limited Algeria Branch, Business District Algiers, Complexe Immobilier Oriental Business Park, Bab Ezzouar, 16024, Algiers, regulated by the Central Bank of Algeria for the purposes of this promotion and lead regulated by the Dubai Financial Services Authority.