We're working hard to protect you against fraud but we can't do it alone.

Find out more about the different types of fraud and how to protect yourself.

HSBC

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 we believe we're better protected when we work together to combat fraud.

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

- Your PIN or full password, even by tapping them into your phone keypad.
- Your Secure Key Code.
- To move money to another 'safe' account in your name - even if we suspect fraud.
- To withdraw money to hand over for safekeeping.
- To hand over cash, your PIN, cards or cheque book, to a courier at your home, even if you are a victim of fraud.
- To pay for goods using your card and then hand them over to us for safekeeping.

Passwords

Try to update your passwords at least twice a year. Avoid using duplicate passwords or ones that are easy to guess.

Secure online banking devices and cheque books

Keep log in devices in a safe place. If your business operates on a dual control environment, ensure that the inputting and approving of payments are conducted by different members of staff.

Shred important documents

Shred any paperwork that reveal personal and business information, such as bank statements, card details and other sensitive data.

Check bank statements regularly

If there are any transactions that you don't recognise, always contact us.

Question uninvited approaches

If you are approached about payments, invoices etc., contact the company directly using an email or phone number that you can check is genuine.

Adopt internal processes

Have suitable checks in place to verify new payment requests, e.g. check account numbers, beneficiary names to ensure it aligns to existing suppliers and long standing instructions.

Personal information

Never share security details beyond authorised staff e.g. usernames and card details. Be careful with what you share on social media sites and check your privacy settings.

Stay safe online

Update your device's operating system as soon as they become available. Install anti-virus software from a well-known company, and always check that websites you're using are genuine.

Fraud vs Scam

The terms fraud and scam are often quoted and sound like the same thing, however, there are subtle differences between the two.

- What is fraud – Fraud is where a criminal makes a payment from your bank account without your knowledge or authority.
- What are scams – A scam is where you have been tricked or forced into making or authorising a payment from your bank account.

Email Scams

Email scams -or phishing- are when a fraudster sends you an email, encouraging you to share personal details or to click on fake links. Take a few minutes to check whether the email seems genuine or not.

Red flags you can look out for:

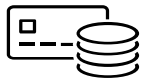
- You are asked to make an urgent payment
- **The sender email address doesn't match** the website address or the organisation it says it's from - hover your cursor over the sender's name to revel the true address
- It asks you to share personal information
- **Check the email address**, especially the domain e.g. @CompanyABC.com instead of @CompanyACB.com as fraudsters will look to align to the original domain.
- If you get a suspicious email that relates to HSBC. Don't click on any links. Don't open any attachments. Just forward the email to phishing@hsbc.com – we will investigate it.

Email interception scams - payment/ invoice diversion

Criminals monitor email traffic and when payments are due they send their own email that looks and feels like a genuine message from the company. Always check with the company on a known genuine number before making payments to new bank details.

Red flags you can look out for:

- **You receive an urgent email with new payment details** in the name of a person or business you have not dealt with before. A vague reason will be given for the change, such as "my accounts have been blocked", "I'm having issues in receiving payments" or "this is how things are done".
- **Poor spelling and grammar in the email is often a clear indicator of a scam**. Scammers will want to get your money and information as quickly as possible and will not be concerned with their spelling or grammar.
- **Does the request make sense?** If you have received an email out of the blue, from someone you have not dealt with before, containing new bank account details, then stop! Call the person or business on a published, trusted and verified number to confirm if the request is genuine. Do not use or click on any phone numbers contained in the email as they can easily be spoofed.
- **Account details have changed.** Fraudsters may tell you that the bank details for your payments have changed and give you the new details to send your payment to. This could be a supplier request payment for a regular invoice.



Account Takeover Fraud

This growing crime is a form of identity theft, where a fraudsters gains controls of a victim's bank or card accounts and then makes unauthorised payments.

Red flags you can look out for:

- **You're asked to download a specific piece of software**. Fraudster call, impersonating a service provider or bank claiming system problems, to fix the problem will ask you to log onto your computer and follow a number of actions. The software will allow the fraudster to see your screen and by asking you to log on onto your Online Banking they will gain the opportunity to steal your banking details.
- **Fraudster offers you a refund**, the caller offers you a refund and "accidentally" send you too much money and asks you to return the overpayment. This creates a new payment to the fraudster on your account and now the fraudster can transfer money from your account to the fraudster account.

CEO Fraud

Criminals impersonate a senior manager in the company and send an email to the accounts department to make a payment urgently. Always take the time to validate the request.

Red flags you can look out for:

- **CEO/ Manager/ Owner is away**. Fraudsters often time this so that the manager they are impersonating is away and the details are difficult to verify.

Text Scams

Text scams -or smishing- are when a fraudster sends you a text that appears to be from your bank or another organisation that you trust. The text may offer vouchers or a tax refund.

Red flags you can look out for:

- **You have been a victim of fraud.** Fraudsters may tell you that there's been fraud on your account and ask you to share or update personal details. They might also tell you that your Online Banking access has been restricted and ask you to click on the link to reinstate access.

Phone Scams

Phone scams-or vishing-are when a fraudster calls pretending to be your bank or another trusted organisation. They can even make their phone number look like a number you know and trust.

Red flags you can look out for:

- **Know your details**. Fraudsters can sound very convincing and may have some of your details such as your account numbers. If you feel uncomfortable, or sense something is wrong, end the call and call the organisation on a number 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 10 seconds before making the call.
- **Request passwords and codes.** Fraudsters may tell you that payments have been made from you account and request passwords and secure key codes to stop/ cancel the payments. A bank can transfer funds at your request and would never ask for your passwords, PIN, or secure key codes.

Investment Scams

Investment scams claim to offer high returns for very little risk. Fraudsters often use false testimonials, fake celebrities' endorsements, spoof websites and other marketing materials to make the scam appear genuine. If seems too good to be true, it generally is.

Red flags you can look out for:

- You receive an offer to purchase precious metals or gems, and to have them delivered to your home.
- **You're approached by phone, email, text message** or by someone calling at your house with an investment opportunity.
- **Scammers will offer investments with high rates of return for little or no risk**. Seems too good to be true.
- **You find an online investment.** Always check that the website you are using is genuine. Visit your local Police and FCA website where there is an approved companies and known scammers list together with useful tips on staying safe.
- **You feel pressured into making a quick decision**, for example if the caller states the offer is "only available right now".

Ransomware Attack

Malicious software infects your computer, preventing you from accessing files, data or even infecting other components on the network. Messages are usually displayed which demand a 'ransom' to be paid in order to regain control over your system. This software is usually downloaded via email, websites or unlicensed software.

To keep your business safe, it's important to have up-to-date anti-virus software, hardware, security upgrades and to have a strong response, recovery and back-up process in place.

Red flags you can look out for:

- **Avoid accessing questionable websites or free software.** If websites are not from a reputable source, they could expose you to unnecessary risk. Consider blocking any software that is not already authorised – this is known as 'application whitelisting'.
- **Avoid using USB sticks.** Especially if they are not from a verified source.
- **Don't use the same password for different business logins.** This increases the likelihood of a more widespread attack.

What to do if you have been a victim of a fraud or a scam?

If you believe that you have fallen victim to a fraud or a scam, then the below tips will guide you on what to do:

- Call your bank straight away using a published and trusted number. Do not click on or dial any numbers that have been sent to you by message or email as they can be easily spoofed.
- Call the police to report the fraud or scam. You will be asked to provide as much information as possible to assist them, so make sure you keep a note of all calls, correspondence and payments made.
- Do not click on any links, email addresses or phone numbers contained in messages or emails.
- Block the person from contacting you further. If you have been speaking with someone by phone, text messages or email, then block them so you cannot be contacted any more. You may be contacted by the same person using different details afterwards, so ensure you block them too.
- If you are being pressured into making a payment or disclosing information, then stop. You will never be pressured into taking action or threatened by your bank, by a government department or by a police force. If you feel you are being pressured, then terminate the call, speak to a trusted person, such as a friend or family member for guidance, and then verify the call using a published and trusted phone number found on a website or on the back of a bank card.

For more information and contact details visit:

- HSBC Fraud and Cyber Awareness App: download this free app, by simply searching 'HSBC Fraud and Cyber Awareness' on the iOS or android app store.
- FCA: Financial Conduct Authority warning list: fca.org.uk/scamsmart/warning-list
- Action Fraud – National Fraud & Cyber Crime Reporting Centre: https://www.actionfraud.police.uk/business-protection
- National Crime Agency: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
- CIFAS – The UK's Fraud Prevention Community: https://www.cifas.org.uk/pr
- UK Finance: https://www.ukfinance.org.uk/