Fraud: Don't Miss a Trick

Host Names: Michele Mcwha HSBC
Michelle Newman Southport Police

HSBC UK

TAKE FIVE TO STOP FRAUD

What's the difference between fraud and a scam?

HSBC UK

Difference between fraud and a scam

Fraud

Fraud is suspicious activity on your account that you didn't know about and didn't authorise.

Examples of fraud include:

- unauthorised use of your credit or debit card
- Bank account takeover
- Identity theft - a fraudster uses your details to open accounts in your name

Scams

A scam involves you making or authorising the payment yourself.

Examples of scams include:

- Instructions to transfer money to another account (e.g a 'safe account)
- Fake investment opportunities
- Requests for money from a scammer who has befriended you or struck up a romance online
- ‘Too good to be true' deals that must be paid for by bank transfer

What are common methods fraudsters use to contact you?

HSBC UK

Phone Calls

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’.

But if someone calls you out of the blue and asks you to move money or share your account details, just hang up.

Emails

Phishing

Email scams 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.

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 more special offers.

Text Messages

Smishing

Scammers send fake text messages pretending to be your bank or another legitimate company.

Scammers may use language you’d expect to hear for an organisation you trust. Phrases and slogans

.

Phone Calls

Vishing

Typically, fraudsters will ask you to:

- transfer money to a 'safe account' or a known beneficiary as your account has been compromised
- withdraw cash and hand it over to the police for investigation
- press a number on your keypad to speak with a customer service representative (a fraudster in disguise)
- share personal or financial details

What you should do:

- hang up
- make sure the line is fully disconnected
- wait 15 seconds
- use a different phone and contact the organisation you know is genuine

Emails

Phishing

Typically, these emails will:

- encourage you to click on a website link
- urge you to take action quickly and threaten to close your account if you don't respond
- pretend that you're owed money
- ask you to share confidential information, such as your online banking details, passwords, account numbers or PINs
- include instructions on how to reply or verify your account – like completing a form attached to the email
- could contain spelling and grammar errors

What you should do:

- don't tap any links
- don't download any attachments
- don't reply
- report it to us at phishing@hsbc.com
- delete the email

Text Messages

Smishing

Typically, these messages will:

- encourage you to take urgent action by tapping a link or making a call
- ask you to verify new payees, transactions or devices
- look and sound like genuine messages but with new wording added
- often come from unknown mobile numbers

What you should do:

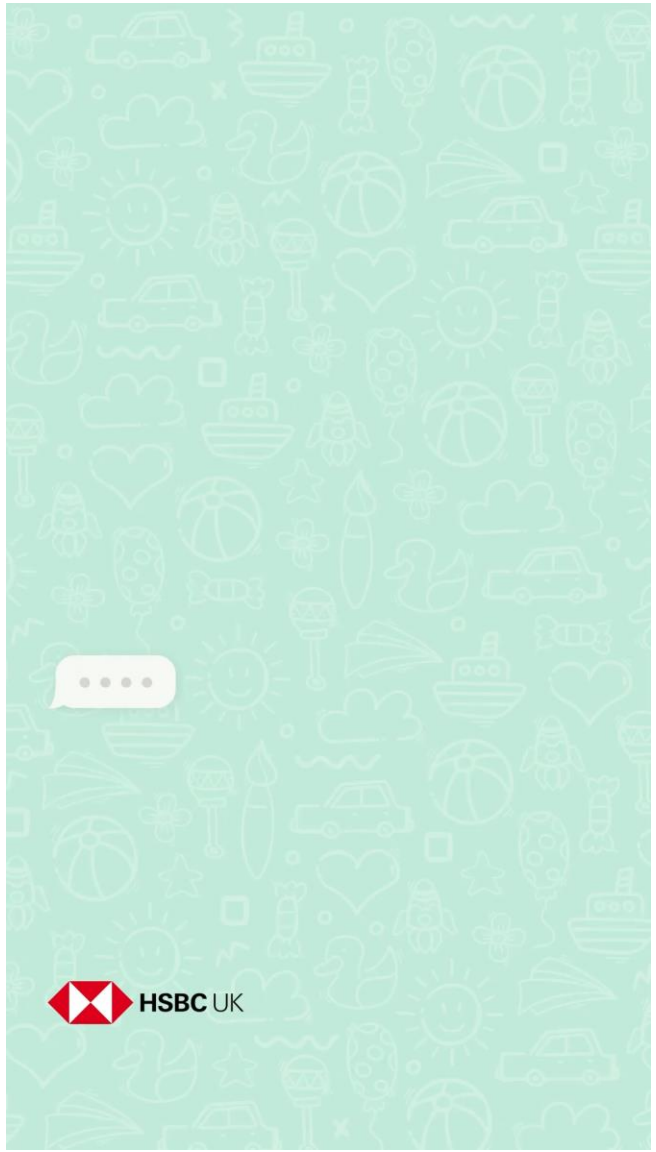
- don't tap any links
- don't download any attachments
- don't reply
- report it to us at phishing@hsbc.com
- delete the message
- contact the organisation using a phone number you've verified, or visit their website

Instant Messaging Scams

Criminals also pose as loved ones and send messages out of the blue, pretending to be children who have lost their phone.

They will ask for money urgently, or ask you to share a code that has ‘accidentally’ been sent to you.

This could be via platforms such as WhatsApp or Facebook Messenger.



Top Tip!

Always remain vigilant when using online platforms to talk to family or friends. Call and speak to them directly.

Key Takeaways

Most fraud & scams start by criminals obtaining your personal or financial details through social engineering.

That could be by text, email or a phone call – don't give fraudsters a way in!

STOP

Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT

Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Stay safe, stay alert

HSBC UK

Remember, we'll never ask you to:

1. Tell us your card’s 4-digit PIN

2. Share your online banking passwords. Or anyone time passcodes (including from your secure key)

3. Transfer money anywhere, including to a 'safe' account

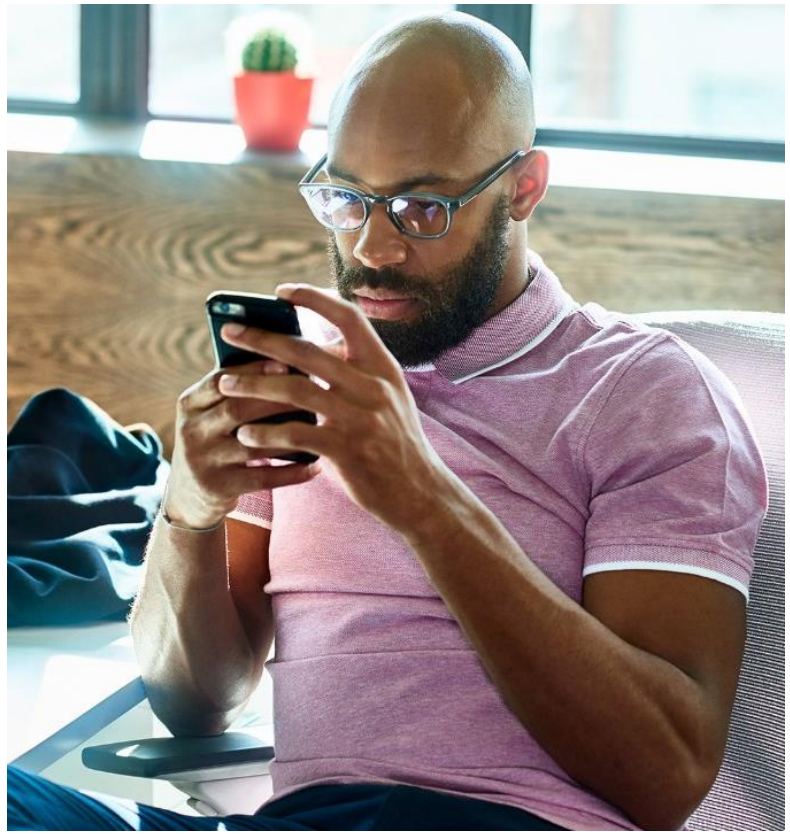
4. Send us your card, cheque book or cash

What are the common scams?

HSBC UK

Authorised Push Payment Scams (APP Scams)

If a criminal tricks you into transferring money to them by bank transfer, it's known as an **Authorised Push Payment (APP Scam).**



It differs from other types of fraud, where criminals get access to accounts and steal money without the account holder's knowledge.

With APP scams, criminals often try to persuade you to take action in a hurry.

They make you panic before you have time to think it through properly.

To help protect customers from fraud, we've signed up to a voluntary code (CRM Code) to combat APP scams voluntary code to combat APP scams.

Let's take a look at some typical APP scams and warning signs to beware of.

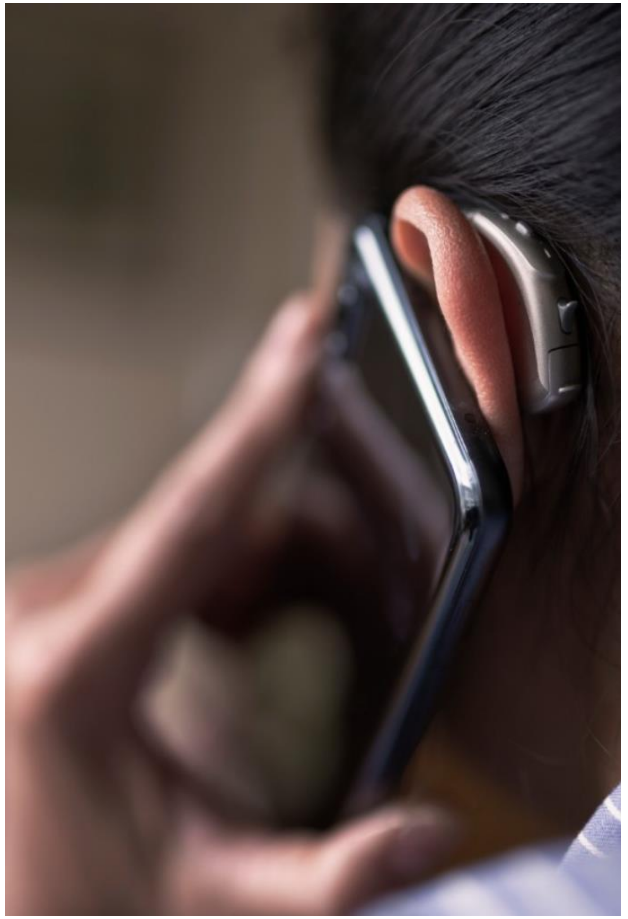
Safe account scams

You may be tricked into sending money to a ‘safe account’.

For example, criminals may claim your account has been compromised and tell you to move your money to a new account that's been opened for you.

Typically, these scams;

- claim to have your personal or financial details
- state there is staff fraud or on-going investigations
- encourage you to act quickly to ‘safe guard’ your account
- call from what seems a HSBC contact number



HSBC will NEVER ask you to move your money into another account to safeguard your money.

Impersonation Scams

Impersonation of police and bank staff

In this scam, the criminal gets in touch and pretends to be from either the police or the victim's bank, they will then convince their victim to make a payment to an account they control.

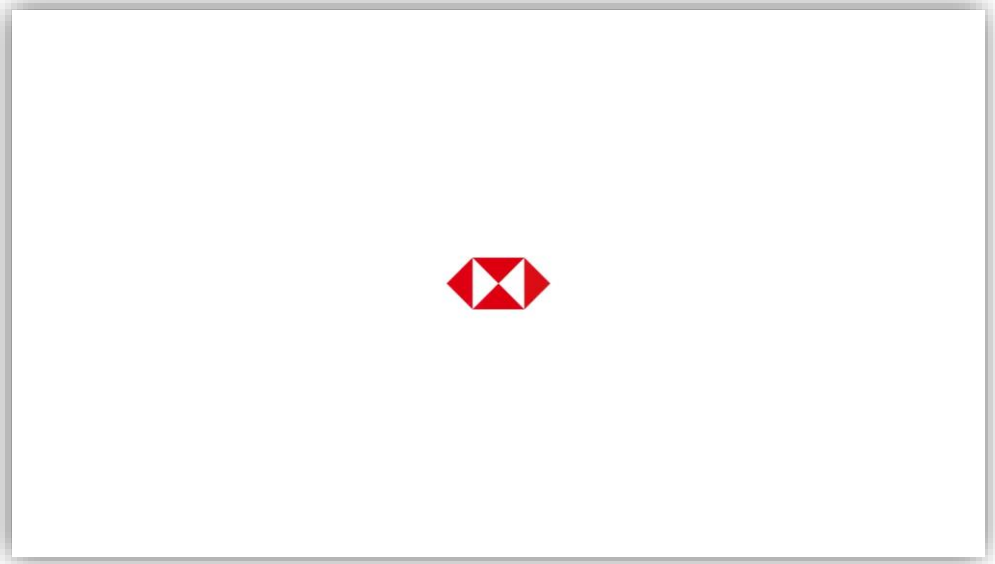
Impersonation scam of other organisations

Here, a criminal claims to represent an organisation such as a utility company or government department.

Common scams include bogus claims that the victim must settle a fine, pay overdue tax or return a refund.

Sometimes the criminal asks for remote access to the victim's computer as part of the scam, claiming they need to help 'fix' a problem.

STOP and contact the company directly, using a phone number or website that is genuine.



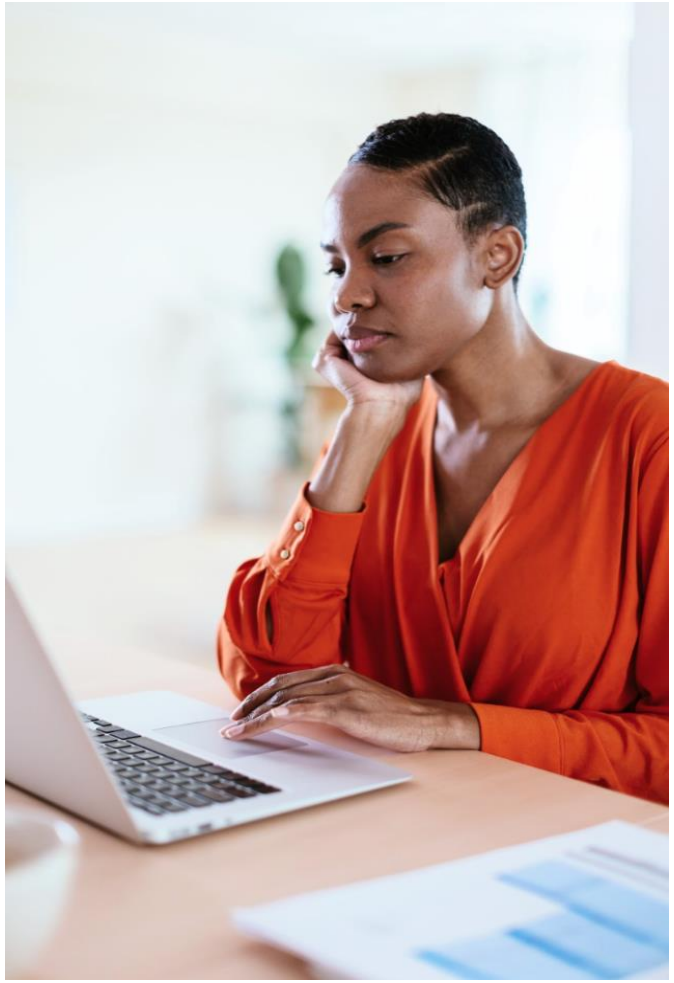
Purchase Scams

Purchase scams happen when you're paying for an item or service.

The item doesn't arrive, or you don't receive the service and your money is lost.

Typically, these scams;

- ask you to send money via bank transfer rather than using a card or cheque
- offer a too-good-to-be-true deal or discount
- have 'limited availability', or are a 'special offer' to encourage you to act quickly
- persuade you to send money before receiving a service
- are advertised on social media or other online marketplaces, or in some cases through legitimate looking websites that have actually been set up by fraudsters



If a deal seems too good to be true, it probably is.

Romance Scams

In a romance scam, you're persuaded to make a payment to a person you have met, often online through social media or dating websites, and with whom they believe they are in a relationship.

Fraudsters will use fake profiles to target their victims in an attempt to start a relationship which they will try to develop over a long period of time…

Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.

They may tell you;

- they live outside the UK and claim they need money to pay for the cost of travelling to see you.
- they have a relative who needs an urgent operation, but can't afford to pay for it
- they have a large inheritance, but can't access the money
- they will ask for you to help fund an investment opportunity

Never send money to someone you've only met online.

Investment Scams

In an investment scam, a criminal convinces you to move your money to a fictitious fund or to pay for a fake investment.

Criminals may contact you with investment opportunities offering guaranteed, or very high, returns.

They'll usually cold call you, and in order to convince you, use false testimonials or fake celebrity endorsements.

They may set up spoof websites and fake companies that have similar (or the same) names as genuine investment organisations.

They can produce convincing marketing materials and might refer to current news to make the opportunity seem realistic.

If it seems to good to be true, it probably is.

Cryptocurrency

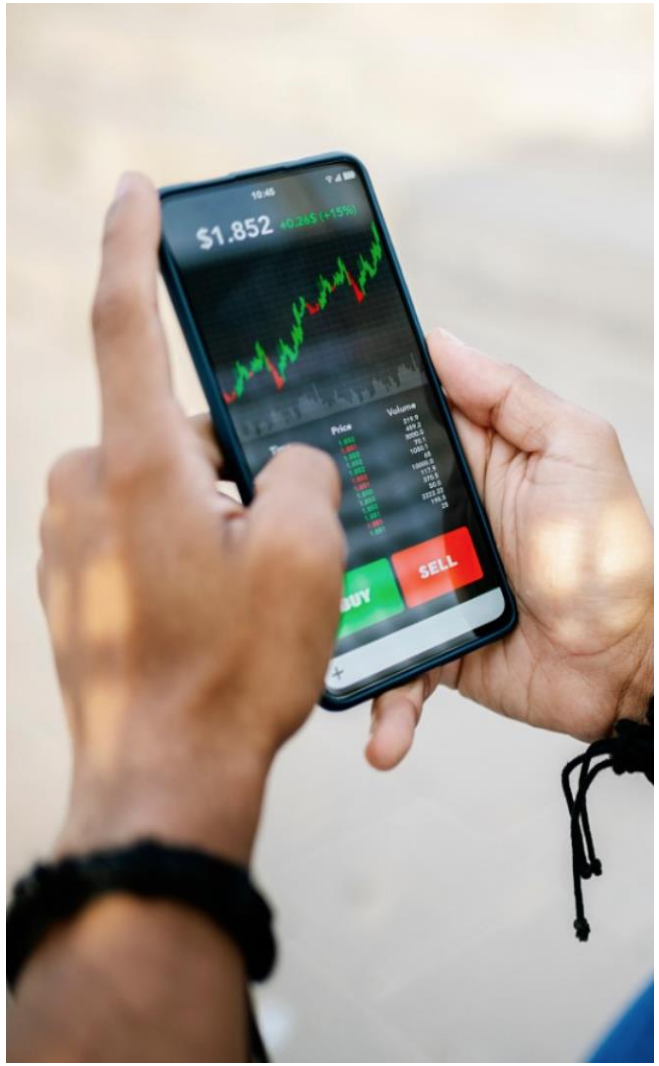
Cryptocurrency is a digital asset that can be traded or exchanged online. It has increased in popularity over the last few years, with some people seeing high returns on investments.

However, criminals are using this as an opportunity to steal your money.

They may do this by;

- Getting you to move money to a crypto asset account or asking for access to your wallet in order to 'manage your investment'
- Offering fake investments that don't really exist or aren't worth the money.
- Impersonating famous people on social media to make their offer look real and more appealing
- Providing a return in the short term, convincing you to invest more, leading to more fraud in the long term.
- Creating professional looking websites with fake reviews

Fraudsters will try to rush you, but take your time. If it feels wrong or too good to be true, it often is.



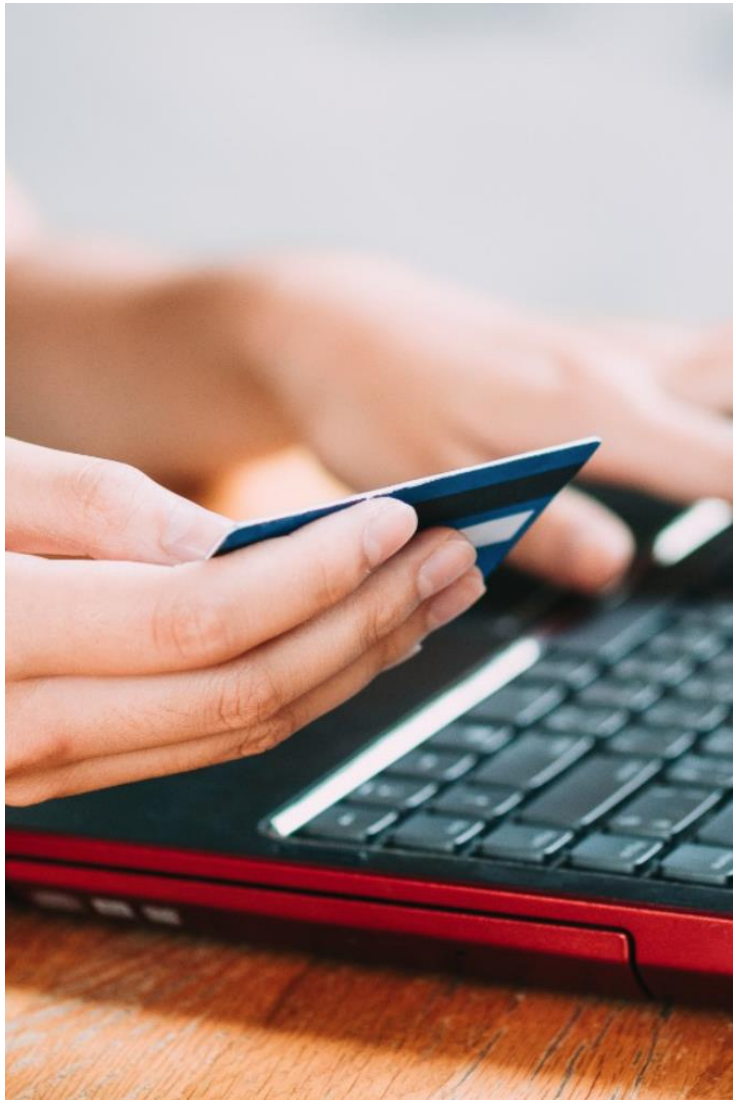
Payment Diversion Scams

Criminals can hack and monitor your emails, and when payments are due, they'll send their own email that looks like a genuine message from a real company.

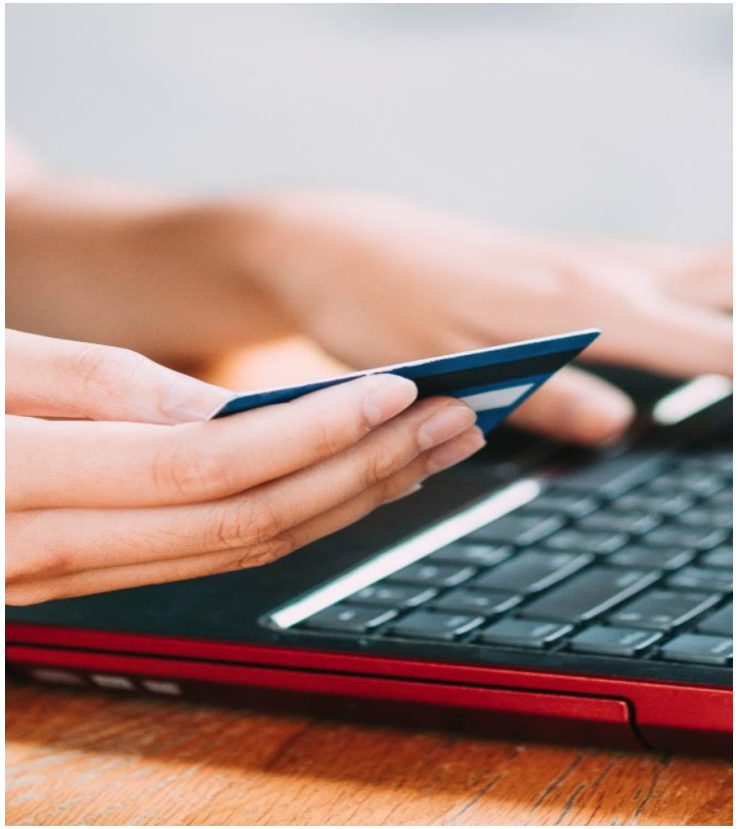
They may tell you;

- The bank details for your payment have changed and give you new details to send your payments to
- This could be if you're in buying a property, car or holiday, for example)

Call the company on a number you're sure is genuine to confirm.



Advanced Fee Scams



In this type of scam, a criminal convinces you to pay a fee that they claim will result in the release of a much larger payment or high value goods.

They may tell you;

- **you've won** a lottery
- that gold or jewellery is being held at **customs**
- you have **inheritance** due
- you can pay **a fee to recover funds** held in investments

The fraudster tells you a fee must be paid first.

These scams often begin with an email or a letter sent by the criminal to the victim.

When the payment is made, the promised goods or money never materialise.

What else should I be aware of?

HSBC UK

Money mules

Scammers prey on those who are low on funds to act as ‘money mules’.

This means you allow money to be transferred through your bank account in exchange for payment.

Students or those strapped for cash are often targeted, with job adverts and spam emails offering ‘easy money’.

You’ll be asked to provide your bank details, receive a payment into your account and then either withdraw it in cash, or transfer it to another account.

It might seem like a harmless way to increase your income, but the money being transferred is stolen and used to fund organised crime.

This can get you into serious trouble.

How to stay safe

HSBC UK

HSBC Fraud & Cyber Awareness App

Download Now

Download on the App Store

Available on the Google Play

Top tips for staying secure online from National Cyber Security Centre

Use three random words when creating passwords

Using browsers & apps to safely store your passwords

Turn on 2-step verification (2sv)

Protect emails by using strong and separate passwords

Backing up your data

How we help to protect you

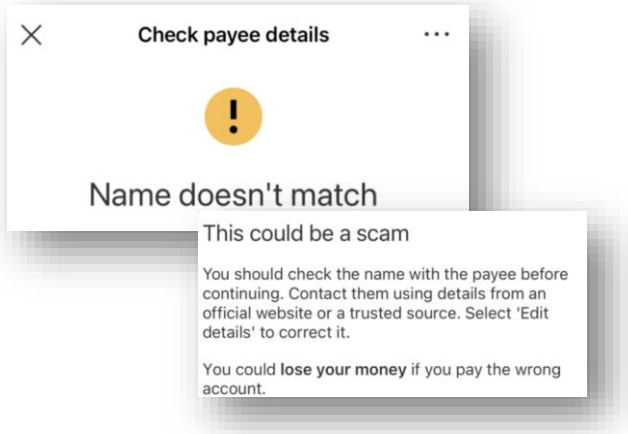
HSBC UK

Confirmation of Payee

HSBC offers a name checking service called Confirmation of Payee.

When you make a one-off payment, set up a new regular payment or amend an existing payment, the service lets you check you're paying the right person or business.

That way, you can see if the name matches the details you've been told!



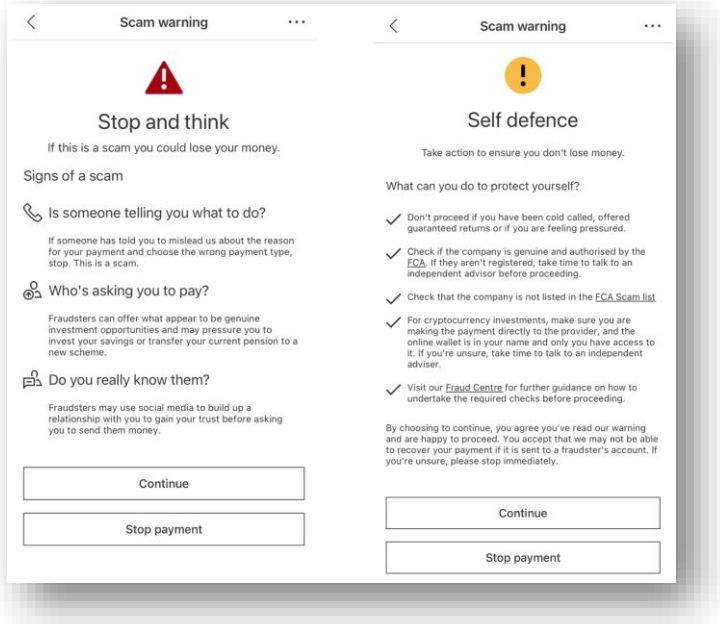
Scam Warnings

To protect you from fraud, we carefully monitor transactions.

You may receive warning when processing a payment with actions to take before you proceed.

If you receive one of these pop-ups, please take the time to read the information before proceeding, it may save you from a scam!

Never let anybody coach you into what option to choose for your payment, either online or when speaking to us directly.



Digital Security Promise

We'll keep a lookout 24/7 for unusual activity on your account.

We'll look to refund any money stolen by fraudsters from your account, as long as you keep your security details safe.

We'll help you to stay up-to-date with our latest security advice.

Note: If you've been tricked into authorising a payment, this may be covered by the new voluntary guide which HSBC is one of the first banks to sign up to. It's not covered by our Digital Security Promise

Let’s test your knowledge

HSBC UK

Message 1

We attempted to deliver your package at 19:05 on Wednesday, 20th October 2021 but no one was available.

Your parcel was returned to our depot.

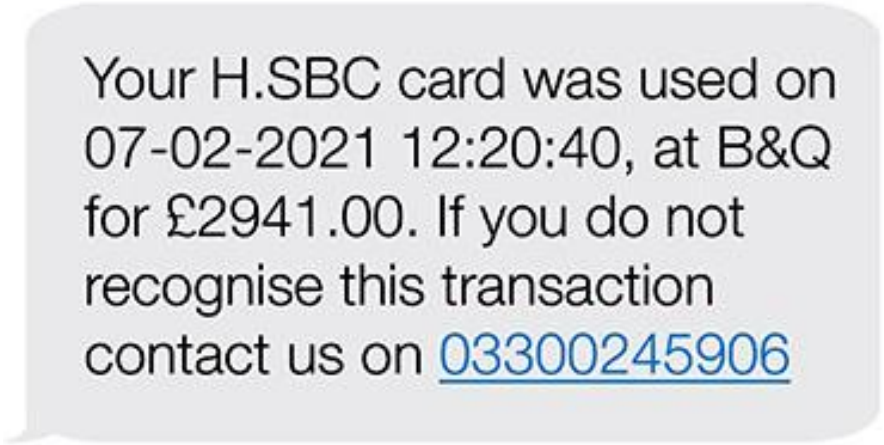
Pay to reschedule your delivery by pressing here https://bit.ly/2jh1nuk

FAKE!

The red flags

- Are you expecting a parcel?
- Why would you need to pay for re-delivery?
- Suspicious link

Message 2



FAKE!

The red flags

- H.SBC?
- Large transaction to make you panic?
- How do you know that's a genuine number?

GENUINE

Signs it is genuine

- Confirming minor details of your card
- Specific dates & times
- Clear instructions of how to confirm
- No strange number to call

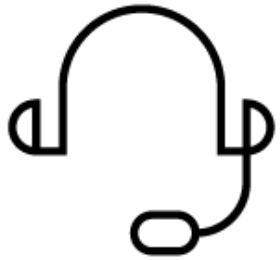
How to report a fraud or scam

HSBC UK

Live Chat

Mobile Banking
1. Log on to online banking.
2. Select the ‘Chat’ tab to the right of the page.

Online Banking
1. Log on to mobile banking in the app.
2. Select the 'Support' tab.
3. Select 'Chat with us'.



Phone

From the UK
03457 404 404

From the outside the UK
+44 1226 261 010

Using the number on the back of your debit / credit card

Lines are open from 08:00–20:00 every day.

Remember, when it comes to fraud

- Stop
- Challenge
- Protect

HSBC UK

Thank you