Fraud:
Don't miss a trick

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

HSBC UK

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 if we learn to spot the fraudster's tricks, we can better protect ourselves and combat fraud together.

We've been hard at work developing tools and techniques that make banking safer, but it's not enough. We need your help. If we all work together and follow a few simple steps, we can be better protected and keep your money safe – and that's good for everyone.

Stop
If someone contacts you unexpectedly and claims to be from a trusted organisation, be suspicious. Take a moment to stop and think before sharing personal or financial information.

Challenge
Could it be fake? It's ok to reject, refuse or ignore any requests or simply say no. Only fraudsters will put you under pressure to act urgently.

Protect
Don't click on unfamiliar links or call numbers from texts or emails. Instead, check they're genuine by going to the official website. Fraudsters may appear genuine, but their actions and requests are not.

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

Your PIN or full password, even by tapping them into your phone keypad.

Any codes that you generate or we send to you by any method for the access or operation of your account including your secure key, card reader or sent to you by SMS or email.

To move money to any other account.

To withdraw money to hand over for safekeeping, checking or investigation of crime.

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 or gift cards, using your card and then hand them over to us for safekeeping.

How can I protect myself?

- **Always question uninvited approaches**
  Instead, contact the company directly using an email or phone number that you can check is genuine.
- **Don't share personal information**
  Never reveal your password or share your card details over email. Be careful with the level of detail shared on social media sites and check your privacy settings.
- **Never mislead the bank about the purpose of a payment**.
  Criminals will often try to persuade you to tell the bank that the payment is for something different to what they have told you. They may suggest it will go through smoother or the bank may stop the payment otherwise. This is a clear sign of fraud.

- **Stay safe online**
  Always update your computer, tablet and smartphone operating systems as soon as they become available and install anti-virus software.
- **Shop safe online**
  If you're buying something online and you don't know the seller, never pay by bank transfer. Always use a credit card, debit card or PayPal – or a payment option that offers some protection against fraud.
- **Be wary of doorstep tradesmen**
  If someone knocks on your door, unsolicited, and offers to do some work on your house that you didn't know you needed, be wary. Often it can start with a small job like clearing the gutters but quickly escalates as they find additional things that need doing. It is often overpriced and unnecessary. Always get further quotes from known and trustworthy tradesmen.
- **Register for Voice ID**
  HSBC Voice ID is making telephone banking safer than ever. It makes it easier to access your account through telephone banking and there's no need to use your security number. (Not applicable to Private Banking Clients).
- **Update your passwords**
  Try to change your passwords at least twice a year. Don't use a password that can be easily guessed and make sure that your Online Banking password isn't the same one you use for other websites.
- **Check bank statements regularly**
  If there are any transactions that you don't recognise, always contact us.
- **Shred important documents**
  Shred any paperwork that reveals personal information, such as bank statements, card details and other sensitive data.
- **Check your credit report**
  If someone has used your name to take out a loan or credit card, it may not show on your statements. Check your credit report at least once a year for any unusual activity.

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.

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.

Typical examples of phishing:

- 'HMRC' email to say you're owed a tax refund.
- you win a lottery you haven't entered.
- your solicitor providing new bank details for your house deposit.
- special sale items at 'too good to be true' prices.

Signs that an email may be a phishing scam:

- you are asked to make an urgent payment.
- the sender's email address doesn't match the website address of the organisation it says it's from – hover your cursor over the sender's name to reveal the true address.
- it asks you to share personal information.
- links in the email are not official addresses. Hover over the link to reveal its true destination.

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. They may tell you that there's been fraud on your account and ask you to share or update personal details. The text may offer vouchers, a tax refund or ask you to confirm the delivery of a parcel.

Typical examples of smishing:

- 'Your bank' tells you that your internet banking access has been restricted and asks you to click on a link to reinstate access.
- 'Your bank' asks you to move your money to a 'safe account'.
- a company tells you your payment has failed and to click on a link to update your bank details or make payment.
- a delivery company tells you that they couldn't deliver your parcel and to click on a link to pay a small fee and reschedule.

Instant messaging scams

Criminals pose as loved ones and send messages out of the blue, often pretending to be children who have lost their phone, asking for money urgently, or asking you to share a code that has 'accidentally' been sent to you.

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

Always remain vigilant when using online platforms to talk to family or friends.

If you're not sure that someone is who they say they are, the best way to check is to call them using a phone number you know to be genuine. By speaking to them verbally, you'll know it's their voice.

In the first half of 2021, over 106,000 people were scammed out of £355 million. This is an increase of over 70% on the same period in 2020.

Source: ukfinance.org.uk

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 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 15 seconds before making your call. You could also call a friend or relative first, to make sure a fraudster isn't listening in when you do make the call.

Typical examples of vishing:

- '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.
- 'HMRC' threaten jail unless unpaid taxes are paid immediately.

Fraud can happen at any place and any time and the fraudsters often look, sound and act like the bank, police or even your internet provider.

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.

Romance scams

A Romance scam is when somebody you have never met in person pretends to have feelings for you and then tricks you into sending gifts or money.

Look out for:

- emotional life story
- start with small requests but will ask for more

Typical examples of this would be:

- relative needs an urgent operation and has no health care.
- they have a large inheritance and are unable to access the money.
- don't have any funds to travel to the UK (with promise of marriage).
- setting up a business or needs help with cash flow due to new contract.

Online scams

Online fraud is on the increase. Fraudsters use sophisticated tactics to access your financial details and passwords, creating bogus links and retailer web pages, as well as fake pop-ups.

Protect yourself from online fraud

- always update the operating systems on your tablet, smartphone and computer as soon as they become available.
- install anti-virus software from a well-known and trusted company.
- when shopping online, always check that the website you are using is genuine and when entering your personal or payment details ensure that there is a padlock in the address bar that indicates that your connection is secure.
- if you're buying something online and you don't know the seller, research the retailer, looking for reviews. Never pay by bank transfer, always use a credit card, debit card or PayPal – or a payment option that offers some protection against fraud.

Investment scams

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

If you're investing in cryptocurrency, make sure you conduct your own research and understand the offer and how investment and trading works.

Ways to spot an investment scam

- you're approached by phone, email, text message or by someone calling at your house with an investment opportunity.
- the 'company' contacting you won't allow you to call back.
- you feel pressured into making a quick decision, for example if the caller states the offer is 'only available right now' or 'don't miss out'.
- the only contact you're given is a mobile phone number or a PO box address.
- it seems too good to be true – high returns for a low risk.
- the company wants to do everything for you, particularly around cryptocurrency.

Visit the FCA website where there is an approved list of companies and a known scammers and cloned companies list, together with more useful tips on staying safe.

Always call the company on the number provided on the FCA website to verify that you are dealing with the genuine company.

Account takeover fraud

This growing crime is a form of identity theft, where a fraudster gains control of a victim's bank or credit card account and then makes unauthorised payments.

How this could happen:
A fraudster calls, impersonating your internet provider. They tell you that you have some connection problems. To fix the problem, they ask you to log onto your computer and download a specific piece of software.

This software allows the fraudster to see your screen. They then ask you to log into your online banking account. The fraudster now has the opportunity to steal your banking details and move money out of your account.

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. They tell you that the bank details for your payment have changed and give you the new details to send your payments to. This could be a house deposit to your solicitor or a business customer's supplier. Always check with the company on a known genuine number before making payments to new bank details.

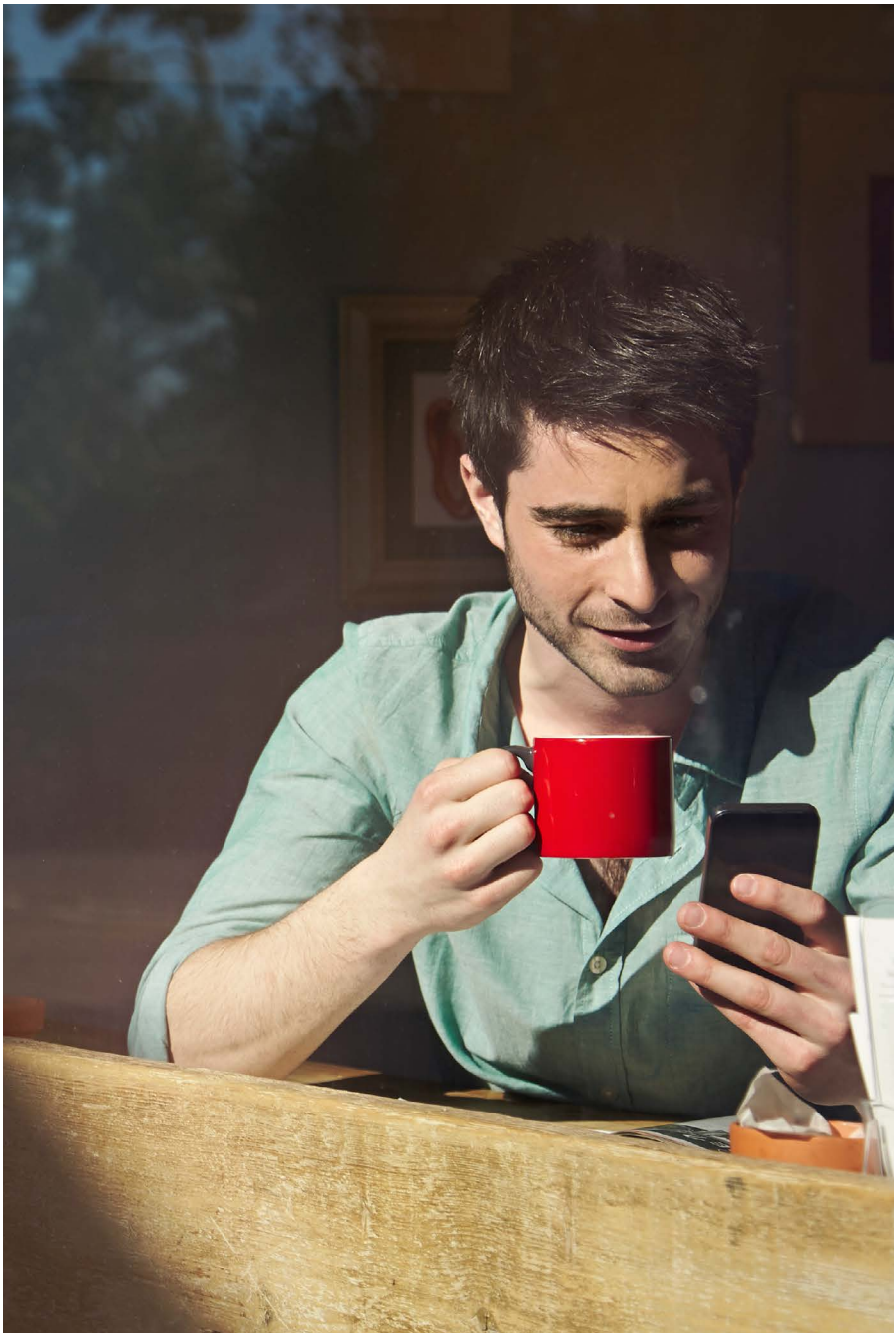
CEO Fraud

Criminals impersonate a senior manager in the company and send an email to the accounts department to make a large payment urgently. They often time this so that the manager they are impersonating is away and the details are difficult to verify.

Always take the time to validate the request.

If you run a business, email interception and CEO Fraud are the most common scams to be aware of.

For more information, visit: business.hsbc.uk/en-gb/gb/generic/fraud-guide



Take Five is a national campaign offering straightforward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

If you suspect fraud on your account pop into your local branch or call us on 03457 404 404.

More information about fraud can be found on our security centre at hsbc.co.uk/help/security-centre or business.hsbc.uk/en-gb/gb/generic/fraud-guide.

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 to us using the live chat on our website, 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: hsbc.co.uk/accessibility or: hsbc.co.uk/contact.

hsbc.co.uk