Fraud and scams

Learn to protect yourself online, face-to-face and over the phone.

HSBC UK

Contents

You might think that fraud is something that happens to other people...

...but scams can affect anyone, even you. The key to beating the fraudsters is to slow down, spot the signs and challenge what you're being told.

Signs that things aren't quite right…

Going with your gut instinct is important when it comes to recognising fraud. Banks and other trusted organisations won't ask you to share security details, or personal information.

We will never:


Persuade you to withdraw money for safekeeping, or to investigate a crime.


Ask for your PIN or password, even if it is safe to tap them into your phone.


Request you share a one-time passcode generated by text, email, or your HSBC Secure Key.


Ask you to move money to another account.


Ask for cash, cards, or cheque books to be sent to us by courier, even if you are a victim of fraud.


Tell you to pay for goods or gift cards, and then hand them over to us for safekeeping.

If you're asked to do any of these things – STOP. It's a scam.

Top tips to help you protect yourself from fraud

- **Always question unexpected approaches**
  Scammers may pose as bank officials or even the police. No bank or police force will ever ask you to help with an investigation, or move money to a 'safe account', or purchase high value items and hand over for 'safekeeping'. Contact the organisation directly using an email address or phone number that you can check is genuine.
- **Don't share personal information**
  Be careful with the level of detail shared on social media sites and check your privacy settings.
- **Be honest about what your payment is for**
  Criminals may try to persuade you to mislead the bank about the reason for your payment. They may suggest it will go through more smoothly, or the bank may stop the payment otherwise.
- **Update 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 your account regularly**
  If there are any transactions that you don't recognise, always contact us on a trusted number, for example, the one on the back of your bank card. Using our app is a clever way to see payments as they come and go, keeping you alert to any unusual activity.
- **Shred important documents**
  Anything that reveals personal information like bank statements, card details or other sensitive data could be used by scammers to target you.
- **Check your credit report at least once a year**
  Look out for any unusual activity. If someone has used your name to take out a loan or credit card, it may not show on your statements.

- **Update your software**
  Install system updates regularly on your computer, tablet and smartphone, and take advantage of anti-virus software.
- **Shop safely online**
  If you're buying 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 you don't know knocks on your door, and offers to do work on your house, be wary. What's sold to you as a small job like clearing the gutters, or fixing some tiles on a roof, can quickly escalate to overpriced and unnecessary work. Always ask for quotes from trustworthy tradesmen.

Have you registered for Voice ID?
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.

Common scams – and how they trick you

Fraud comes in many forms. From emails and phone calls to in-person scams and online schemes, scammers will exploit your trust to trick you out of your personal information, identity or money.

Email scams

Email fraudsters want to steal personal information or gain access to your bank account. They do this by sending clickable links and attachments which contain unsafe software. This can compromise your computer or smartphone's security without you realising it.

Often, they send links to fake websites or PDFs containing spyware. Until you look more closely, their links and websites can look like the real thing. So have a close look at the full email address or web address. 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 a fraudster pretending to be your bank's fraud department or claiming to have 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 provides new bank details for your house deposit.
- You're offered special sale items at 'too good to be true' prices.

> Criminals may know that legitimate payments are due and 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. Always check with the company directly by using a telephone number from a trusted source, for example, an internet search, before making payments to new bank details.

Signs that an email may be a phishing fraud:

- You're 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.
- You're asked 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. Often the text offers vouchers, a tax refund or ask you to confirm the delivery of a parcel. You should delete and block these messages on your phone.

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.
- Criminals pose as loved ones and send messages out of the blue, often asking for money urgently or asking for sensitive information. Be cautious and verify the identity of the sender through a trusted phone call.
- Stay vigilant when downloading apps and only use trusted sources. Be cautious of requests for personal information or payments through apps.

Social media scams

- Sometimes criminals pose as loved ones. They send you messages pretending to be a child or relative who has lost their phone. Or they might ask you to share a code that has 'accidentally' been sent to you. Always double check and don't be pressured into acting too quickly.
- WhatsApp, Facebook Messenger, Instagram, and Telegram are popular instant messaging apps, which fraudsters try to exploit.
- Always take care when using online platforms to talk to family or friends. Is it secure?
- 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, and not a number advised in the message.

Phone scams

Phone scams, or vishing, happens when a fraudster calls you pretending to be your bank or another trusted organisation.

- They can sound very convincing and may already know some of your personal information, such as your account number or address.
- They can even make their call appear to come from a number you know and trust. This is known as phone number spoofing.
- Fraudsters can keep the line open and even fake 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.

> 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.

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.

If you think someone is trying to trick you into handing over money or personal details, stop, hang up and call 159 to speak directly to your bank. You can also register for the telephone preference service to cut down on unwanted calls tpsonline.org.uk/register.

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. This can be done through dating apps, websites, and messaging services like WhatsApp.

Things to look out for include an emotional life story and small requests for money which get larger over time.

Typical examples of this would be:

- A friend or relative needs an urgent operation and has no health care.
- They have a large inheritance and are unable to access the money.
- They don't have any funds to travel to the UK.
- Marriage proposals.
- Setting up a business but with cash flow problems.

Investment scams

Investment scams claim to offer high returns for very little risk. This could be in cryptocurrency, fake ISAs, gold, other precious metals or high-value items. 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. Scammers may give you an initial 'return' quite quickly to encourage you to invest more.

Ways to spot an investment fraud

- You're approached by phone, email, text message or by someone calling at your home 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.

You'll find an approved list of investment companies on the Financial Conduct Authority (FCA) website, along with a known scammers and cloned companies list.

If you're thinking of investing, 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. A fraudster gains control of your bank or credit card account and then makes unauthorised payments.

How this could happen:
A fraudster calls, pretending to be 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 can steal your banking details and move money out of your account.

Rogue trader scams (also known as doorstep scams)

Someone who looks like a tradesperson comes to your door and offers a service you haven't asked for or need. They may tell you that urgent work needs to be done, such as your roof or driveway. They may not start the work, or even complete the work, and they may even overcharge you. They could also ask you to pay in advance for materials.

How to protect yourself

- Don't feel rushed to get work done by someone knocking on your door. Take your time, do your research, read reviews about them online and get several quotes before making any decision.
- Don't believe anyone who unexpectedly tells you work needs to be done on your house. Talk to a friend or family member or ask a trader who you know is trustworthy.
- If you feel uncomfortable, close the door.

High value items

Fraudsters are tricking people into buying gold, other precious metals, or jewellery and then physically handing it over to criminals.

They may pose as police, bank employees or other government officials (or all of these together) to make you believe your money is not safe in the bank or to help with an investigation.

They ask you to buy gold or jewellery to stay safe, usually from a reputable supplier, but then ask you to hand over the items for safekeeping.

The police and government agencies will never ask you to buy gold.

How to stay safe

- Stop and think. If you are asked to buy gold or any other high value goods to stay safe, it's a scam. Legitimate fraud investigations will not ask you to do this.
- If someone contacts you or asks you to buy or hand over gold or jewellery, just hang up.

Business fraud

When it comes to CEO or business fraud, criminals sometimes impersonate a senior manager in a company to send an email to the accounts department. They request a large, urgent payment is made. They'll time this so the manager they are impersonating is away and the details are difficult to verify.

Always take the time to double check unusual requests.

What are we doing to combat fraud?

We're on it. Our experts, technology and smart tools work hard to keep you and your money safe day in, day out. From time to time, we may ask questions about your account or payments, to ensure we keep you safe from scams.

But you have a role to play too – staying alert to common scams and how to spot them can help prevent you falling victim next time.

Remember: Stop. Challenge. Protect.

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.

This page has intentionally been left blank

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, 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: hsbc.co.uk/accessibility or: hsbc.co.uk/contact.

hsbc.co.uk

HSBC UK Bank plc. Registered in England and Wales with number 09928412.
Registered Office: 1 Centenary Square, Birmingham, B1 1HQ, United Kingdom. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our Financial Services Register number is 765112.