C. Hoare & Co.

PRIVATE BANKERS SINCE 1672

Staying Safe from Fraud

STAYING SAFE FROM FRAUD

Keeping your money safe is our priority, and it demands constant vigilance. While banks and other financial institutions develop ever more robust fraud-prevention systems, fraudsters find increasingly sophisticated ways to steal money and disrupt lives.

According to UK Finance, around £2,300 was stolen every minute in 2022, and in many cases bank customers were perceived as the weakest link in anti-fraud defences. We understand just how persuasive fraudsters can be – they exploit every opportunity to prey on their victims – and we want to help you protect yourself. Our Fraud team is constantly alert to new scams and malpractice, and we need you to be vigilant too.

This guide contains examples of scams in current circulation. Please take time to read the information carefully. If you have any questions or concerns, the Fraud team will be happy to hear from you (**CustomerFraudSupport@hoaresbank.co.uk**). Equally, if you feel a face-to-face advice session would be beneficial, your relationship manager will be happy to arrange this.

If you believe you have been the victim of fraud – even if you are unsure – it is important to let us know. The sooner we are alerted, the more chance we have of recovering your money, so please do not hesitate to call the bank on **020 7353 4522**. Day or night, there will be someone to help you.

PLEASE BE AWARE

Fraudsters are skilled in the art of impersonation. They can clone telephone numbers or email addresses so it looks like they are contacting you from an organisation you know and trust e.g. the bank, the Police, HMRC, the Royal Mail or your telephone/internet service provider.

Fraudsters are expert manipulators and will do everything in their power to make you divulge confidential information or perform actions that are not in your best interest. They can make you feel confident/anxious/pressurised as suits their purpose and know where to find chinks in your defence.

One-Time Passcodes (OTPs) – also known as security codes – are used to authorise online transactions or log in to your account.

Never use an OTP to authorise a transaction over the telephone. (The bank will never ask you to do this.) **Giving this code over the telephone will enable fraud – please hang up instead!**

Nor should you provide personal banking details over the telephone – neither the bank nor any reputable organisation will ask you to do this.

CURRENT SCAMS

Here are the most common scams seen by the bank.

1. 'Safe account' scam

You receive an email from 'Megamart', a global online shopping site you have used many times in the past. The email explains that your goods are stuck with customs; to release them, you will need to provide further information and pay a small fee of £0.99 via the link provided in the email.

A few days later, you receive a telephone call. The caller identifies himself as a member of the C. Hoare & Co. Fraud team and says he has concerns about a payment of £0.99 made from your account a few days earlier. Apparently, the bank has seen a number of cases where fraudsters use details from 'Megamart' payments to log into customer accounts.

Panicked, you ask what you can do to stop criminals emptying your bank account. The helpful fraud officer advises you to transfer all your money to a 'safe account'. Time is of the essence and he has taken the precaution of setting up a new account in your name at another bank. Once you have transferred the money, using payment details provided by the fraud officer, your relationship manager will be in contact to discuss next steps.

Some days later, you have yet to receive the promised call from your relationship manager, so you call the bank. At this point, fraud is detected, and it becomes clear you have moved your money to a fraudster's account.

Stop and think!

- Were you expecting a delivery from the supplier mentioned in the email? If so, check the original purchase agreement for a delivery date and verify whether a delivery/customs fee is required.
- Are you being put under pressure to move a large amount of money? This is a clear indication something is wrong.

Stay safe

- **Never** click a link in a text or email unless you have verified it with the company who sent it. Telephone them on the number given on their website (a fraudulent email is likely to contain a fraudulent telephone number).
- **Never** transfer money to a bank account at the request of a third party, unless it is for services rendered and you have confirmed the details via an independently sourced telephone number.
- **Never**, in any circumstance, transfer money to a 'safe account'. No bank will ask you to do this. If there are concerns, they can simply place a block on your account until the matter has been thoroughly investigated.

2. ‘Fraud on your account’ scam

You receive a call on your mobile and recognise the number as the bank’s. The caller introduces himself as a member of the bank’s Fraud team and alerts you to suspicious activity on your credit card. Large sums are going out of your account and immediate action is required to block further spending.

To prove the call is genuine, the fraud officer reads out the first four digits of your credit card and/or debit card. Reassured, you provide full card details, including the Card Verification Value (CVV) and receive a One-Time Passcode (OTP) via SMS. Providing this code, you are told, will enable you to cancel the fraudulent transactions.

You read back the OTP to the fraud officer, pleased you acted in time to prevent fraud on your account. However, when you check your bank statement, it displays a number of large payments you don’t recognise.

After full investigation, it is evident you have been scammed. Armed with your full credit card/debit card numbers, the ‘fraud officer’ has gone on a spree: OTPs you received from the bank were genuine, but they authorised expensive purchases, on your account, that you will never see.

Stop and think!

- Why would the bank need to know your card details? They have this on record. If they wanted to identify a particular card, they would give the last four digits, not the first four. Fraudsters, on the other hand, can easily access the first four digits of your card number – most frequently through a data breach.
- OTPs are used to authorise transactions. They are *not* used to cancel transactions.

Stay safe

- **Never** give out an OTP to authorise any activity on your account over the telephone. **Giving this code over the telephone will enable fraud – please hang up instead!**

3. Email Interception scam

You receive a telephone call from 'Speedy Cleaners', a firm you deal with regularly. Your usual contact is on holiday, but he has asked the caller, a close colleague, to let you know an invoice is due for payment.

The colleague is highly personable. She asks you to confirm a few details relating to bills you have settled previously and your preferred method of payment. The next day you receive an email from 'Speedy Cleaners'; it's from the usual email address but asks for payment to be made to a new account.

Just to be sure, you call the number given in the email and are pleased to find the same friendly woman answering the telephone. She explains that 'Speedy Cleaners' has changed bank recently and assures you all invoice information is correct. Satisfied you have carried out due diligence, you pay the bill.

A few weeks later, your usual contact at 'Speedy Cleaners' calls to say the firm has not received payment for its latest invoice. Nor, it turns out, have they changed their bank or hired a new female colleague. With sinking heart, you realise you have sent the money straight to the account of a fraudster.

Stop and think!

- Is the person asking for money someone you have dealt with before? (NB Email accounts of legitimate businesses can be compromised.)
- Are you being asking to send money to a new bank account?

Stay safe

- Always validate billing information received via email by calling the sender on an independently sourced number (e.g. the number displayed on a company website).

4. ‘Please help me’ scam

Example 1.
You receive an urgent message from your son via text or WhatsApp. It’s an unfamiliar number, but he explains he is calling from a friend’s phone as his own is damaged. This couldn’t happen at a worse time, as he’s out of funds and his rent is due. Can you please transfer money to the account number provided in the message?

You send the money, and the next day your son arrives for dinner with the family. He is perfectly solvent, and his phone is working fine. You have been scammed.

Example 2.
You receive a WhatsApp message showing an unfamiliar number. Your daughter is on a night out and has lost her mobile phone in a mugging. She is calling, on a borrowed device, to ask for money for a taxi home. Please can you send money to her bank account immediately, using details provided in the message?

You send the money and ask your daughter to let you know when she is safe at home. When no call comes, you telephone her home number and discover she spent the night on the sofa, watching television. You have been scammed.

Stop and think!

- Did the message come with a generic greeting (“Hi Mum, it’s me!”/”Hi there, hope you’re well”)?
- Are you being asked to transfer money immediately to prevent some kind of misfortune?

Stay safe

- Do not reply to the message.
- Call instead on the number you have saved for the family member/friend/business contact to check out the story.

5. Bank Card fraud

Example 1
You are about to use your bank card to withdraw cash from an ATM when someone taps you on the shoulder. They just found a £20 note lying on the ground – is it yours? It's not your money, so you return to your transaction only to find your card/wallet is missing. When you look around, the helpful stranger is nowhere to be seen.

When you next check your balance, it is clear someone has used your card details to make fraudulent purchases on your account. Looking more closely, you see these payments date to the time of the incident at the ATM.

Example 2
You are settling the bill in a restaurant. The waiter brings a card reader to your table and, just as you tap your card/enter your PIN, a colleague calls him over to another part of the restaurant. He apologises for the interruption, but returns quickly and completes the transaction. The next day, you discover unauthorised withdrawals on your account. The waiter, it turns out, spent the time away from your table cloning your card and is now making fraudulent purchases in your name.

Stop and think!

- Was your attention diverted at any point before or during your card transaction? Fraudsters may use simple distraction techniques to steal your card or PIN.
- Are there signs of tampering on the ATM or hand-held card reader? (These may include a loose or blocked card slot, misaligned stickers or a 'spongy' keypad.) Fraudsters can fit 'skimming' devices to ATMs and card readers to clone your card. They then use your card information to make fraudulent purchases or steal your identity.

Stay safe

- Never engage in conversation with another person while you are using an ATM.
- Do not let your card out of your sight when paying in shops or restaurants.
- Check card and bank statements regularly for suspicious transactions; the faster criminal activity is picked up, the easier it is to remedy.

6. Workplace Fraud

You receive an email from your CEO asking you to pay a supplier immediately. She is just stepping into an important meeting and won't be available for the rest of the day, but she's very clear the payment needs to made right now or your company will face significant penalties.

Reading the email, you notice details provided for the supplier are different to those provided previously. It's unusual, too, that the supplier has asked for part of the payment via Google Pay vouchers. Nonetheless, the CEO's request was unambiguous and, with promotion in the offing, you don't want to disappoint. So you make the payment using banking details provided in the email.

You send the CEO an email confirming that that the payment has gone through. She is not in a meeting and did not ask you to pay anyone. The request was made by a fraudster.

Stop and think!

- Is it usual to receive this kind of request from your CEO? Would this kind of task generally fall to you?
- Is the request exceptionally urgent? Does it mention penalties for non-payment?
- Is the email sent from the CEO's usual address? Fraudsters can create an account that closely resembles the real thing.
- Does the email request payment to new beneficiaries and/or via new channels (e.g. payment vouchers)?

If any of the above apply, **do not action the request.**

Stay safe

- Any request to change the bank details of an existing supplier should be treated as suspicious. Do not reply to the email and verify the request by speaking to a known individual at the organisation in question.
- Regularly review internal procedures for requesting, approving and verifying transactions.
- Remember small businesses are as much at risk as individuals. Personal assistants or family offices may act on fraudulent instructions they believe have come from their employer.

WHAT TO DO WHEN YOU HAVE BEEN SCAMMED

If you believe you have been targeted or if you have fallen victim to a scam, as well as calling the bank, you can report the scam directly to Action Fraud on **0300 123 2040**.

Action Fraud is the UK's national reporting centre for fraud and cybercrime. Its website (**www.actionfraud.police.uk**) contains information and advice together with details of the latest fraud trends.

If you are worried your personal details have been stolen, you may wish to subscribe to the Cifas Protective Registration service. It will place a flag alongside your name and personal details in its secure National Fraud Database. Companies and organisations who are signed up as members of the database will see you are at risk and take extra steps to protect you and prevent fraudsters from using your details to apply for products and services.

For more information on the Cifas Protective Registration service, please visit **www.cifas.org.uk**.

Take Five

C. Hoare & Co. supports the Take Five campaign. This a national campaign, led by UK Finance and backed by His Majesty's government, that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

Take Five advises extreme caution in any situation where you are sharing personal or banking details. You should make sure you are confident that the organisation you share your information with are who they say they are. A genuine bank or organisation will never contact you unexpectedly to ask for your PIN, full password or to move money to another account.

If you do not know who you are talking to, or there is reason to suspect that the provider is not who they claim to be, do not disclose your banking security details, or other personal or financial information.

Take Five urges you to stop and consider whether the situation is genuine – to stop and think if what you are being told really makes sense.

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

2. **Challenge**: Could it be fake? Do not be afraid to reject, refuse or ignore requests. Only criminals will try to rush or panic you.

3. **Protect**: Contact your bank immediately if you think you have fallen for a scam and report it to Action Fraud.

For more information on the Take Five campaign, please go to its website: **www.takefive-stopfraud.org.uk**.

C. Hoare & Co.

PRIVATE BANKERS SINCE 1672

For further information please visit our website **www.hoaresbank.co.uk**