

## Your guide to banking safely with Hampden Bank

In this document, we outline **how to keep your finances safe from fraud**. If you would like to find out more, or if you have any concerns, please speak to your banker directly.

## Helping to protect you from fraud

Firstly, please be aware that **no one** at Hampden Bank will ever ask you for:

- > Your PIN.
- > Your Digital Banking password.
- > Your One Time Passcode which is generated for logging onto Digital Banking.
- > Your One Time Passcode which is generated when you are making a payment online. This is only for you to see. It should never be shared with anyone. It should only be input online if prompted when making a purchase. The only person that will ever ask you for this code will be a fraudster.
- > The 3 digits on the back of your debit card or charge card (CVV number).



We recommend that you add your banker's contact details and our 24-hour Cards Centre number to the contacts on your mobile phone so you can access these quickly if required.

---



When you call our Cards Centre, if you have lost your debit card for example, you will be asked for answers to the security questions which were set up for this purpose when you opened your account.

We will never ask you to move money to a so-called "safe" bank account or to a new bank account.

We do not send you confidential information by email unless it is encrypted.

If you are worried that you may have been a victim of fraud or if you have any concerns that your personal information, account details or mobile device may have been stolen, it is important that you contact our 24-hour Cards Centre or your banker immediately.

[www.hampdenbank.com/contact-us](http://www.hampdenbank.com/contact-us)

**24-hour Cards Centre:**  
**+44 (0)345 601 1107**

## Steps to help you protect yourself

There are some straightforward steps that you can take to minimise the risks from fraud attempts:

- › Keep your security details, passwords, PIN details or any Internet Banking details secure and do not share them with anyone else.
- › When making a card transaction, keep your card in your possession and do not let the card out of your sight. It is very unusual now to be asked to take your card away, and if this does happen, simply ask to join the person at the card machine.
- › Let your banker know if you change address, email or phone number so that the information we have is accurate.
- › Check your bank statements regularly and let us know of any transaction that you do not recognise.
- › Shred anything containing personal data when you want to throw it away.



If you have any concerns that you might have been a victim of fraud, please let your banker know or contact our 24-hour Cards Centre immediately.

- › At cash machines and when making payments, take care when others are close by as they may be trying to see you enter your PIN. If you think someone may have seen your PIN, you can change it at most cash machines.
- › Be aware that your post is valuable information in the wrong hands. If you don't receive a bank statement, card statement or any other expected financial information, contact us or the relevant organisation.
- › Do not respond to emails requesting information (account numbers, card details, PIN or passwords). We will never request information from you by email and it is our policy not to send personal data to you by email – there is more information on this type of scam, called “Phishing” on page 6.
- › Remember that email communication is not secure so please do not send us confidential information this way. Secure messaging is available within our Digital Banking system, or just give us a call.
- › We will never ask you to move money to a so-called safe bank account or to a new bank account.
- › We will never ask you to download remote access software (such as TeamViewer) on to your computer or mobile device.

# Steps to help you protect yourself (continued)

## a) Take care when making payments

Be careful when you make a payment online or give your banker a payment instruction. Pay attention to warnings and security measures (e.g. one-time passcodes) when:

- › setting up a new payee
- › amending an existing payee
- › immediately before authorising a payment

Before authorising your payment:

- › Check the payee is who you are expecting to pay.
- › Check the amount.
- › Ask yourself how confident you are that you are paying for genuine goods/services/investments.
- › Ask yourself if you have done enough to confirm that the person or business you are paying is legitimate.
- › Do not rely on the payment details you have been sent, for example in an email, as these could have been intercepted and changed. Call back the payee on a number you know.
- › If you are a micro-enterprise or charity you must follow your own internal procedures for the approval of payments.

Please remember that fraudsters are very good at tricking people. If we contact you by phone to confirm payment details of a new payee, please make sure you are entirely confident that the payment information is true and correct, otherwise we may not refund your money if it turns out to be a scam. There is more information on this type of fraud called an “authorised push payment scam” in Section 3 below, and how you can avoid them. If you have any doubts, don’t make the payment.

### Fraud refunds

- › The steps above help prevent you from authorising payments to fraudsters and give you the chance of a refund if the payment turns out to be a scam.
- › We look at all cases of fraud on a case-by-case basis. Where you meet the requirements for mandatory Reimbursement for Authorised Push Payment Fraud,

in most cases, you should receive a refund within 5 business days, up to the maximum reimbursable amount of £85,000. A £100 excess may be applied. Read the Authorised Push Payment Fraud Reimbursement Guide in Section 4 for full details.

- › If the payment does not meet the requirements, it will still be reviewed on a case-by-case basis to determine if a refund should be given. We may not give a refund if you do something dishonest, obstructive or careless that helps an instance of fraud take place.

## b) Keep your bank cards, cheque books and security details safe

- › Do not share your security details, passwords, PIN details and any Digital Banking details with anyone else (even a joint account holder).
- › Use passwords that are not easy for other people to guess.
- › If your card is retained by a cash machine or any other payment machine, please notify your banker or our Cards Centre immediately to block the card. You can also block your card using our card management app if you have downloaded this to your device from an App Store.

## c) Keep safe online

Install and keep up-to-date antivirus software on your computer and keep your operating systems up to date when rolled out by providers.

## d) Do not act as a money mule

Do not act as an intermediary for the receipt and payment of funds – you might become a “money mule” for criminals and be guilty of money laundering.

Further information on what is a money mule and how to protect yourself from becoming a mule can be found on:

[www.moneymules.co.uk](http://www.moneymules.co.uk)

## Examples of common frauds

There are several common methods that criminals use. Below are some examples to help you identify when you may be at risk from a fraud and the action you should consider taking. If you have any concerns that you might have been a victim of fraud, please let your banker know straight away so that they can help you. Or contact our Cards Centre if card related.

[www.hampdenbank.com/contact-us](http://www.hampdenbank.com/contact-us)

If you have been a victim of fraud or cyber-crime, you should think about reporting it to Action Fraud.

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)



### Payment fraud – Authorised Push Payments (APPs)

Scams involving APPs occur when someone is tricked into authorising an electronic payment from their bank account to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer.

Payments related to APP scams can be made over the phone, online, or in person, and most are completed instantly.

#### Examples of APP frauds

- > WhatsApp/Text scams – normally someone pretending to be a family member that has lost or damaged their phone and urgently needs money transferred to pay a bill or for themselves. Never send money without speaking to the family member.
- > Property transactions – criminals intercept the email chain between sellers, buyers, estate agents and solicitors. The fraudsters change the payment information related to transfer of funds so that payments are diverted to the fraudster’s account.
- > Fraudsters who convince people to move money to a “safe” account such as another bank account.
- > Invoice scams – where fraudsters send a false invoice, often pretending to be from a company from whom you are expecting a bill.
- > Romance scams – fraudsters form a relationship in order to ask for money, or for enough personal information to steal your identity.
- > Purchase scams – sending money to buy goods or services that do not exist.

This is one of the most prevalent frauds according to UK Finance. See their website for further information.

## Examples of common frauds (continued)



### Payment fraud – debit and charge cards

This is where fraudsters use stolen debit, credit or charge cards, or their details, to buy goods or services.

If your card is retained by a cash machine or any other payment machine, please notify your banker or our Cards Centre immediately to block the card. You can also block your card using our card management app if you have downloaded this to your device from an App Store. Your card may have been retained by the machine legitimately due to a fault but occasionally fraudsters will attach card trapping devices to cash machines and as soon as you leave the machine, the fraudster will remove the card from the slot and use it for fraudulent transactions. Our Cards Centre will cancel your card straight away and arrange for a new card to be ordered.

We provide an extra layer of security when you are shopping online with your Hampden Bank debit or charge card. You may be asked to enter a One-Time Passcode (OTP) in order to confirm that your purchase is genuine. We will send a unique OTP by text message which will then be entered by you into the website you are using for the purchase. If you receive an OTP that you are not expecting please advise us immediately. No legitimate person will call and ask you for this code. It is only used to approve online shopping purchases.



### Phishing

Phishing is the fraudulent practice of sending emails or phoning and claiming to represent reputable organisations (e.g. a bank, social media site, TV Licensing, HMRC etc) and requesting personal information such as your bank details for verification or recording purposes.



If you receive an OTP that you are not expecting please advise us immediately. No legitimate person will call and ask you for this code.



### Malware

Malware is short for “malicious software” which has been specifically designed to disrupt, damage or gain unauthorised access to a computer system. Any electronic device, including phones and tablets, can receive malware. Your device can become infected if you click on links or download software or files from suspicious websites and emails.



### Identity fraud

Identity theft occurs when a fraudster steals your personal information or possessions so they can use your identity for their own financial gain. Phishing and malware are often the means of capturing this data.

Once a fraudster has enough information, they can use your identity to:

- > open bank accounts
- > take over existing bank accounts
- > obtain genuine documents
- > borrow money

## Useful links

There is much more information available about how you can keep your data and your finances safe, and we have selected links to some of the best of these.

> **“Take Five” to stop fraud**

[www.takefive-stopfraud.org.uk](http://www.takefive-stopfraud.org.uk)

Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. It is led by Financial Fraud Action UK (part of UK Finance) and backed by the UK Government. Further advice and information can be found in the Take Five Customer Advice Guide.

> **Authorised Push Payment guide**

[www.takefive-stopfraud.org.uk/app-guide](http://www.takefive-stopfraud.org.uk/app-guide)

> **The Financial Conduct Authority**

[www.fca.org.uk/scamsmart](http://www.fca.org.uk/scamsmart)

Find out how to protect yourself from investment scams and how to check you are dealing with an authorised firm.

> **The Financial Services Register**

[www.register.fca.org.uk](http://www.register.fca.org.uk)

This is a public record of all firms, individuals and other bodies that are regulated by the Financial Conduct Authority.

> **Get Safe Online**

[www.getsafeonline.org](http://www.getsafeonline.org)

Get Safe Online is a source of unbiased, factual and easy-to-understand information on online safety. This contains lots of information on how to protect yourself online as well as the different types of scams that are currently active.

> **CIFAS**

[www.cifas.org.uk](http://www.cifas.org.uk)

CIFAS is the UK's leading fraud prevention service.

For individuals they offer increased security against identity fraud, as well as expert advice on how to protect your personal data in our increasingly tech-reliant world.

> **Action fraud**

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

This is the UK's national fraud and internet crime reporting centre. Action Fraud provides a central point of contact for information about fraud and financially motivated internet crime. Incidents reported to Action Fraud will be designated a police crime reference number.



Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. It is led by Financial Fraud Action UK (part of UK Finance) and backed by the UK Government.

---

# Current fraud trends

## Insolvency Service

Shareholders/Directors of companies are being contacted by fraudsters claiming to be the 'Insolvency Service'. They say that the business is being wound up and they require personal information and verification in the form of a Passport/Driving Licence. If you receive a call like this, do not provide any information and hang up.

## Computer company

Company calls to advise that the internet is running slow and they need to run some diagnostic tests. They may ask you to download a file which will have malware in it. Fraudsters may also call claiming to be a computer company advising you have malware and need to pay to remove it.

## Email interception

1. Request to pay an invoice. You are expecting an invoice but fraudsters intercept the email and amend the bank details. Always make contact via another means than email to ensure you have the correct details before you pay.
2. Fraudsters send emails from a contact asking you to purchase gift cards for a birthday, explaining that they are unwell and cannot do it at present but will pay you back. You obtain the gift cards and send them the codes via email. The emails have been intercepted and the gift cards are then in the hands of the fraudsters.

## Card fraud One Time Passcodes (OTPs)

One Time Passcodes are designed to prevent fraudulent activity on your account and should only be received when you are making a purchase online or when using digital banking.

Fraudsters contact clients advising they are from the Bank's Fraud Team or from law enforcement, the FCA or other organisations. They then request the client discloses a code they are sending them to verify their identity or to stop a fraudulent transaction. The code is then entered to make a purchase from a website. No one legitimate will ever ask you for this passcode. If asked for one, hang up and contact your banker.

## WhatsApp 'Dear Mum' scams

The 'Dear Mum' scam involves fraudsters posing as a person's child pretending they have lost or damaged their phone. The scammers then ask the parent to lend them money for a new phone or to cover their bills.

Always make contact with your family member in some other way e.g. landline, calling the mobile number you have (not the alleged new one).

Consider setting up a phrase only you and your loved one would know in the event of this type of request to protect yourself further.

### London

16 St. Martin's Le Grand  
Fourth Floor  
London EC1A 4EN  
020 3841 9922

### Edinburgh

20 | 21 Charlotte Square  
Edinburgh EH2 4DF  
0131 226 7300

[hampdenbank.com](http://hampdenbank.com)