Financial Fraud Action UK

Working together to prevent fraud

ADVICE FOR PHONE AND ONLINE BANKING USERS

All banks in the UK offer different online and phone banking options. These allow you to carry out most of the day-to-day banking activities that you would have only been able to do in a branch.

The history of phone and online banking, also known as remote banking, dates back over 20 years to 1985 when the first online computer banking system, HOBS, was launched by Bank of Scotland. Three years later the first phone-only bank was launched by First Direct.

The remote banking revolution took another step forward in 1997 when the first internet banking service was launched by Nationwide. Nine years later another significant milestone was reached as the number of people banking online overtook those who banked over the phone for the first time ever. Most recently, in 2008, the Faster Payments Service was launched, which enables phone, internet and standing order payments to be processed within a few hours.

WHAT YOU CAN DO IF YOU BANK ONLINE OR OVER THE PHONE

Banks offer their phone and online banking customers some, or all, of the following services:

- Current balance and up-to-the-minute statement enquiries.
- Make payments and pay bills.
- Manage standing orders.
- Transfer money between your own accounts.
- Order chequebooks and foreign currency.
- Pay someone by Faster Payments (as long as this new payment system has been rolled out by your bank or building society and on the account you are sending money to – check participating sort codes at www.canipayfaster.co.uk).

TOP TIPS WHEN BANKING ONLINE

To help improve your security online follow these common sense precautions:

BEFORE YOU BANK ONLINE

- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- Install anti-spyware software on your machine.
- Download (from the internet) the latest security updates, known as patches, for your browser and your operating system. Set your computer to automatically download these updates if possible.
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are not always activated by default.
- Keep your passwords and PINs a secret – do not write them down or tell anyone what they are.

WHILST BANKING ONLINE

- Be wary of unsolicited emails or phone calls asking you to disclose any personal details or passwords. Your bank or the police would never contact you to ask you to disclose your PIN or your online banking password.
- Always access your internet banking site by typing the bank's address into your web browser.
- Never go to a website from a link in an email and then enter personal details.
- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or unbroken key symbol in your browser window when accessing your bank site. The beginning of the bank's internet address will change from 'http' to 'https' when a secure connection is made.
- Don't be conned by convincing emails offering you the chance to make easy money. If an offer looks too good to be true, it probably is.
- Never leave your computer unattended when logged in to your online account.
- When making a payment, always double check that you have entered the correct account number and sort code – if you enter incorrect details the payment will go to a different recipient and it may prove difficult to get the money back.

WHEN YOU HAVE FINISHED BANKING ONLINE

- Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café.
- Check your bank statements regularly and thoroughly. If you notice anything irregular on your account contact your bank as soon as possible.

COMMON ONLINE BANKING SCAMS

Online banking is a very safe and secure way to access your bank account. However, because the banks' own systems have proved difficult to attack, criminals have turned their attention to getting information directly from online banking customers themselves, by using the following methods:

PHISHING

This is the name given to emails that claim to be from your bank or other organisations but are actually sent to you by fraudsters. These emails typically urge you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify or update your personal security information but, by doing so, you are actually giving your information to the fraudster who has created the fake website. The fraudster then uses the details to access your online bank account and take your money.

One easy way to spot phishing emails is that they are usually addressed to "Dear valued customer" instead of using your name. This is because phishing emails are usually sent out at random as the fraudsters only have limited information such as your email address.

MALWARE

Malware (malicious software) is a computer virus that can be installed on your computer without your knowledge. It is capable of monitoring your PC activity, enabling fraudsters to capture your passwords and other personal information. To make sure you don't become a victim of malware, make sure you have up-to-date anti-virus and anti-spyware software installed.

WHAT IS A MONEY MULE?

Money mules are people who accept fraudulently obtained money into their account, and then withdraw the money and wire it overseas to a fraudster (as it is not possible to make cross-border transfers from a UK online bank account).

Money mules are often innocent people who have been duped into helping criminals transfer funds abroad. Criminals offer prospective mules the chance to earn some easy money - concealing the fact that the work is illegal by advertising the job as a 'UK representative', 'shipping manager' or 'sales manager' for an overseas company. However, money mules are liable for prosecution and anyone who thinks they may have been duped by such a scam should contact the police immediately.

COMMON TELEPHONE SCAMS

Fraudsters use a variety of methods to trick unsuspecting bank customers into revealing their personal financial details or parting with cards and PINs:

DECEPTION RUSE

Fraudsters cold call unsuspecting cardholders and dupe them into revealing their card details by claiming to be from the security or fraud department (of either a bank, card company or Visa or MasterCard) and saying that their records have flagged up a fraudulent transaction on the victim's card. By seeming to offer assistance, the caller hopes to gain their victim's trust.

The fraudster, who may already have some details about the person they are phoning - such as their address - is really trying to find out extra security details, such as the cardholder's PIN or the three-digit security code on the back of their victim's card. The conman may claim that the amount of the fraudulent purchase can be credited back if the individual divulges their PIN or the three-digit security number.

COURIER ALTERNATIVE

A recent variation on the above scam is that the fraudster goes through the above routine but, instead of asking for the security details, instructs the victim to write down their PIN and place it in an envelope with their card. The fraudster then advises that they will send a courier to make the collection. The fraudster then contracts a genuine courier company to collect the envelope that contains the victim's card and PIN. The courier, who is an unwitting pawn in the scam, then hands the envelope over to the fraudster who uses the card and PIN to withdraw cash at cash machines.

Supported by

THE UKCARDS ASSOCIATION

TOP TIPS WHEN PHONE BANKING

- Ensure that you cannot be overheard and that nobody is listening in as you say your security details.
- Never give your PIN to anybody over the phone. Your bank will never ask you to divulge your PIN – anyone who asks you for it is probably a fraudster.
- Be wary of unsolicited phone calls from anyone who claims to be from your bank or the police. As a rule of thumb you should only divulge personal financial information (logins, passwords etc) if you have made the call yourself, using a number you know to be correct.

WHAT TO DO IF YOU HAVE BEEN TARGETED

The advice below will help you if you think you are a victim of fraud.

IF YOU RECEIVE A PHISHING EMAIL:

Your bank will never send you emails asking you to disclose security details – if you receive an email of this nature you should delete it. Phishing emails can be reported to the banking industry by visiting www.banksafeonline.org.uk and clicking on 'Report a scam'.

If you have already disclosed details to a potential phishing site you should contact your bank immediately telling them when this happened and how you were contacted. This will enable your bank to investigate and help ensure that your account is protected.

IF YOU THINK YOUR COMPUTER HAS BEEN INFECTED BY MALWARE:

If you have used your online banking service prior to your computer becoming infected, you should contact your bank so that they can monitor your account for potentially fraudulent transactions.

In addition to contacting your bank you should try and remove malware from your machine as soon as possible using anti-virus software. Alternatively, you can seek help from your software or computer supplier.

IF YOU THINK YOU HAVE BECOME INVOLVED IN A MONEY MULE SCAM

Even if you have had nothing to do with the actual theft of funds from another person's account, by allowing your account to be used to receive and transfer such funds, you will be acting illegally. If you think you have become involved in a scam of this nature contact your bank straight away – they will advise you on what steps you should take.

PROTECTION FOR VICTIMS OF FRAUD:

The Banking Code states that you are not liable for fraud losses unless you have acted fraudulently or without reasonable care. One of the most recent amendments to The Banking Code ensures that customers who bank online get similar protection if they are victims of fraud.

FASTER PAYMENTS SERVICE

The Faster Payments Service was launched in May 2008. The service enables banks to process internet and phone payments 24 hours a day, seven days a week, normally within a couple of hours. Standing orders can also be processed on weekdays within a couple of hours. In the past, these payments have taken around three days to clear.

TOP TIPS WHEN MAKING A FASTER PAYMENT

- Make sure your bank or building society has rolled out the new service on your account.
- Ensure the account you are sending money to can receive Faster Payments - you can either ask your bank to check or you can use www.canipayfaster.co.uk.
- Check the value limit for Faster Payments set by your bank.
- If you want to pay a bill you should check the back of your bill and check the timescales.
- Always double check the account number and sort code, as once you have made a Faster Payment it can't be cancelled.
- Remember, if it is not possible to use the new service, you can still make your payment online or over the phone using the existing three-day Bacs service.