At FG Bank We take security seriously
We're continually striving to make banking safer. Our security guides give you information and advice on staying secure, as well as details on how to contact us if you suspect there has been fraud on your account

Protect Yourself
Security of your credentials (Protect Yourself)

You apply to use our services online, we will set up security credentials for you. Your credentials give you access to Barclays Online services, and you should take adequate steps to make sure that this online information remains secret. To safeguard these details you should:

- Memorise your passcode and memorable word, and remember to destroy your passcode letter once you have memorised your passcode
- Ensure that you do not tell anyone your passcode or memorable word, and ensure that they are kept secret by taking appropriate steps to prevent disclosure to a third party
- Never keep details of your passcode or memorable word with your membership number in the same place
- Avoid using the same passcode or memorable word on other websites

Logging out
If you have logged in to the secure area of the site and then choose to finish your session, you should always log out to prevent unauthorised access to your account.

Public computers
Be extra vigilant if using public computers, including internet cafés, or wireless hotspots, where there is an increased risk of your online details being compromised. It is recommended that you use computers which you directly control, or at least consider to be secure, to access Barclays Online.

Do not select options to remember your details on a computer other people may use.

Completely close the browser, clearing private data, when you've used a computer that other people may use.

Protect your computer
Anti-virus protection

Anti-virus software is used to prevent, detect and remove known viruses.
When you use anti-virus software, ensure that you carry out regular software updates to keep it as up to date as possible. If your anti-virus software has a virus scanner option, it is recommended that you schedule regular scans of your computer. If a virus is ever found, it is recommended that you follow the instructions provided by your anti-virus software.

Updates and patches
Software patches work to close a hole or weakness in your computer's software. Keep your operating system (e.g. Windows 7 or Apple OSX) and your web browser (e.g. Internet Explorer or Firefox) up to date by regularly checking the manufacturers' websites.

- For Windows and Internet Explorer updates go to: windows.microsoft.com/en-us/windows/windows-update
- For Mac updates go to: www.apple.com/uk/support
- For Chrome updates go to: www.google.com/chrome
- For Opera updates go to: www.opera.com/

Personal Firewall
Personal firewall software works in the background to manage traffic to and from your computer according to its security policy.

It is recommended that in addition to using anti-virus software, you use a personal firewall. This will help to protect you from online threats by acting as a barrier between the public internet and your personal computer, provided that you carry out regular updates.

Downloads
There are many internet frauds that rely on people downloading software to their computer often without their knowledge or consent. Do not download any software onto your computer unless it is from a trusted source or site.

Email attachments
Be vigilant when receiving attachments by email, even if they appear to be sent from your bank.

Email Security
To help protect your personal email accounts, try to use a strong password that contains at least eight characters with a combination of upper and lower case letters, numbers and keyboard symbols (for example $ecurePassword1).

If you believe an account has been compromised, sign in and change your password immediately. If you cannot access your account because a password has been changed, contact your email service provider immediately.

Spyware
Spyware is a program that can secretly gather information about you as you use your computer. It is commonly downloaded without the knowledge or consent of the user. It can slow down your computer, alter your homepage, produce lots of adverts or links to websites and even include keystroke loggers to record details such as passwords and user names. If your security software detects a threat on your computer, it is recommended that you follow the instructions provided by your software.

Trojan programs
Trojan programs are hidden programs, again commonly downloaded without the knowledge or consent of the user, that can give control of your computer to a hacker or gather information about you as you use your computer. A trojan is a type of computer worm or virus that is installed on your computer without your knowledge or consent.

Typically, the fraudster will send you an email that tries to trick you into following a website link and downloading a piece of software or opening an attachment. If you take this action, the trojan can be installed.

Trojans can be capable of recording passwords and other personal details by capturing keystrokes or taking screen shots of sites you visit. These details can then be sent to the fraudster.

What we're doing to protect you
Our website security

The security of your financial and personal information is very important to us and we take appropriate steps to protect you online. We use proven technology to ensure that our online services are provided in a safe and secure environment. This includes:

Secure Socket Layer
Our web based services use a technology known as Secure Socket Layer (SSL) which means that the information sent across the network is scrambled. To support this technology, you need an SSL-capable browser. A symbol on your browser, usually a lock or key, tells you if you are on a secure site.

If the symbol is unbroken or in the locked position then you are using a secure connection to the server.

Time-outs
Following a period of inactivity we apply a time-out to your session in case you forget to log out.

Top anti-fraud tips
Protect yourself from fraud

Fraud crime is growing and everybody needs to be aware of it. We hope you find the following tips useful and informative. Keep your details safe. Keep your cards, passwords, PINs, documents and personal information secure.

Be suspicious of any unsolicited communications that ask for your personal details. Although unsolicited phone calls, letters, emails or texts can look or sound legitimate, chances are they're fraudulent. Don't respond to these kinds of communications until you've contacted the company concerned to check that they're genuine.

Be careful
Never download software, open attachments or follow links that you've been sent by email unless you're sure they're safe. If in doubt, delete the email immediately. These tricks are commonly used by fraudsters to install trojans or spyware. Check your bank and credit card statements carefully

Contact us straight away if you spot any transactions you don't recognise.

Be vigilant and up to date

- Check your bank statements regularly, particularly if you've recently changed your contact details.
- Keep your computer and mobile software up to date
- Keeping your computer and mobile's operating systems, applications, virus checkers, firewalls and software up to date is the best proactive protection for your computer, mobile and data.
- Be vigilant when using cash machines.
- Move to another machine if someone behind you is behaving suspiciously or attempts to distract you.
- Check for signs of tampering, as this could mean that the machine has been fitted with a skimming device.
- Never leave receipts behind - keep them until you've checked them against your statements and then dispose of them safely, preferably by shredding them.
- If you are concerned about the security of your account contact us immediately

Security of your credentials
Identity theft now costs the financial world more than 5billion Euros a year. Avoid falling victim to this fraud by following our simple tips. If you are concerned about the security of your account, contact us.

Identity theft?
Identity theft occurs when fraudsters use your personal information without your knowledge or consent to take out bank accounts, credit cards, loans, state benefits and documents such as passports and driving licenses in your name. It can have a terrible impact on your personal life and finances. For example, you may have difficulty getting loans, credit cards or a mortgage until the problem is sorted out. We list below some ways in which you can protect yourself from identity theft.

Keep your personal information secure

- Cancel any lost or stolen cards immediately. Make a list of all your card issuers' emergency numbers and keep them handy.
- Protect your details when shopping in store, online or by phone. Make sure other people can't hear or see your card details or personal information.
- Never carry documents or plastic cards unnecessarily. Keep them in a safe place when you're not using them.

Keep your documents safe

- Keep your personal documents in a safe place, preferably locked away at home or your bank. If any of your documents have been lost or stolen, contact the issuing organisation immediately.
- Destroy unwanted documents, preferably by using a shredder. Never throw away entire bills, receipts, credit or debit card slips, bank statements, or even unwanted post in your name.
- Check account statements as soon as they arrive. If you spot any unfamiliar transactions, contact the company concerned immediately.

Keep your passcodes, PINs and memorable words safe
Never give personal or account details to anyone who contacts you unexpectedly. Be suspicious, even if they claim to be from your bank or the police. If they've called you, ask for their organisation's name and call them back via that organisation's switchboard. Be aware that banks, including ours, will never ask for your PIN or a whole security number or password.

Lost and stolen card fraud
This occurs when a lost or stolen card is used by a fraudster posing as you. Most lost and stolen card fraud occurs before you report the loss.
To protect yourself:

- Report any lost or stolen cards immediately
- Use chip and PIN cards where possible
- Only carry the cards you need
- Always shield your PIN from any observers when using cash machines

Counterfeit card fraud or skimming
A counterfeit card can be a fake card or a valid one that's been altered or recoded.
Most cases of this fraud involve skimming, the process by which the data on your card's magnetic stripe is electronically copied onto another card without your knowledge.

Skimming commonly occurs at retail outlets - particularly bars, restaurants and petrol stations - and at cash machines that have been illegally fitted with a skimming device. The stolen data is then used to create counterfeit cards.

To protect yourself:

- Don't leave your card with bar or restaurant staff for long periods
- Don't let retail staff take your card away to process payments
- Check cash machines for signs of tampering before you use them

Card-not-present fraud

This is the most common type of card fraud. It occurs when fraudsters steal your card details and use them to make purchases over the Internet or by phone, fax or mail. Always be aware of who you are dealing with.

To protect yourself:

- Avoid entering your card details on shared or public computers
- Always remember to log out of any websites where you've entered your card details
- Only enter your card details on secure sites that you trust, preferably with merchants using the 3-D Secure service (remember to check that the web page has the secured lock or key icon in the browser)
- Keep a close eye on your statements and report any fraudulent transactions immediately
- If you do a lot of online shopping you may wish to consider using a debit card with a low balance, or credit card with a low limit, specifically for online purchases

Mail-non-receipt fraud
This fraud occurs when you order a new card and it's stolen in transit. You're at particular risk of this fraud if you live in a property with a communal letterbox, such as a block of flats or a student residence hall.
To protect yourself:

- Find out how long it will take for any new cards to be mailed out to you and contact your card provider straightaway if they don't arrive on time

Identity theft on cards
This occurs when a fraudster uses your personal information to open or access card accounts in your name. There are two types:

More information about card fraud
If you're planning to travel, it's best to let us know in advance. This helps avoid problems with using your cards and accounts overseas, as well as helping to protect you from fraud while you're away.

Card Watch contains useful information about card fraud for consumers and businesses.

Be Card Smart Online is packed with tips for protecting yourself against online card fraud and is specifically designed for online shoppers.

The identity theft website developed by the Government, Metropolitan Police and various industry bodies contains detailed information about identity theft and how you can avoid it. Our guide to identity theft summarises some of the key points from this website.

Cheque Fraud
How does cheque fraud occur?

Cheque fraud takes place when a fraudster uses a stolen or counterfeit cheque to pay for goods and services. More than 90% of fraudulent cheques are stopped before any loss occurs. But even so, cheque fraud still costs millions of Euros a year.

These losses can be compounded when the fraud also involves an 'overpayment'. This occurs when the fraudster - who is often part of an organised gang - targets the seller of a high value item, such as a car, and offers to pay using a stolen or counterfeit cheque made out to more than the price of the goods. Once the cheque clears, the victim is asked to transfer this 'overpayment' to a third party, as well as handing over the item to the fraudster.

When the real cheque owner discovers that money has been stolen from their account, the victim can be obliged to repay the total sum - even if this happens several weeks later.

Common Scams
Social Engineering

Social engineering is the act of manipulating people into doing what you want. In terms of online fraud, it usually involves tricking people into disclosing passcodes, login details or other confidential information.

You can protect yourself by:

- Not disclosing confidential information over the phone unless you're sure that the caller is really who they say they are. If in doubt, ask for the caller's phone number, satisfy yourself that it is genuine, and only then call them back.
- Never sending confidential information by email. It can easily be intercepted by a third party, and companies like ours will never ask you to email personal details, account information or passcodes.
- Keeping your credentials (PINs, passcodes and memorable words) confidential at all times. Banks, including us, will never ask you to disclose this type of information.

Phishing, Vishing & Smishing
Phishing is the process of attempting to acquire confidential information by sending out emails that direct you to bogus websites or phone lines. These emails claim to be from a particular company, but are actually sent by fraudsters, often at random. Any information you disclose on these bogus websites or phone lines is captured by the fraudsters.

Similar techniques are used over the telephone using Voice (Vishing) or the use of SMS (Smishing).You can protect yourself by treating any unsolicited emails, calls or texts that ask for confidential information as suspicious. If in doubt, contact the company that supposedly sent you the message to make sure that it's genuine.

Courier Scam
The courier scam is when fraudsters call and trick you into handing your cards and PIN numbers to a courier on your doorstep. There are many variations of this scam:

Protect yourself against courier fraud:

- Your bank will never send a courier to your home
- Your bank and the police will never collect your bank card
- Your bank and the police will never ask for your PIN
- If you receive one of these calls end it immediately

Boiler room scams
Boiler room scams are scams where 'companies' contact clients generally out of the blue either by post, email or telephone and offer them shares in a company at a supposedly heavily discounted price. They will often use hard sell tactics to persuade the client to buy the shares e.g. creating a sense of urgency or using a persistent and aggressive style. This pressurised tactic is why they are referred to as boiler room scams.

The company that they are trying to sell may be listed on an illiquid market so the shares cannot be sold. Or they could be a small unquoted company that the broker claims is planning to list. In other cases the company itself may not exist or the share certificates delivered are fake.