The voice of banking & financial services

Protecting yourself from online fraud

Advice for bank customers

More than 33 million people in the UK now regularly use the internet to access their bank accounts or to shop online, with an increasing number of adults (40 per cent) doing both. The internet remains a safe way to carry out banking or shopping transactions as long as a number of common sense precautions are taken.

Banking online

In the UK more than 21.5 million people now bank online – and this is a very safe and secure way to access your bank account. But, due to the banks' own systems proving difficult to attack, criminals have turned their attention to acquiring information directly from online banking customers themselves. Most fraud on online bank accounts involves a customer being duped into giving away their user passwords and security information or having their PC infected with spyware designed to steal the information. The two most common attempted scams currently used by online fraudsters are **phishing** and **malware**.

Phishing is an email that claims to be from your bank (or other organisation) but is 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 (malicious software) is a type of 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

The voice of banking & financial services

victim of malware, make sure you have up-to-date anti-virus and anti-spyware software installed.

Top tips to prevent online banking fraud

- **Be suspicious of emails which are supposedly from your bank.**
- **Never give your login details in full by email or over the phone** – your bank will never request these in this way.
- **Make sure your computer has up-to-date anti-virus software and a firewall installed.** Consider using anti-spyware software. Download the latest security updates, known as patches, for your browser and for your operating system (e.g. Windows).
- **Be wary of unsolicited emails requesting personal financial information.** Keep passwords and PINs safe; always be wary of unsolicited emails or calls asking you to disclose any personal details or card numbers. Your bank, building society or the police would never contact you to ask you to disclose your PIN.
- **Ensure your browser is set to the highest level of security notification and monitoring**. The safety options are not always activated by default when you install your computer.
- **Know who you are dealing with** - always access internet banking sites 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.
- **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.

For further advice visit www.banksafeonline.org.uk

The voice of banking & financial services

Online shopping

The incidence of computer hackers stealing and using cardholder data from retailer websites is low. Similarly, the vast majority of online businesses are honest and legitimate and comply with their obligations to carefully protect and securely dispose of cardholder information. Most internet card fraud involves a criminal obtaining genuine card details in the real world that are then used to shop online.

Top tips to avoid online shopping fraud

- **Be aware that your card details are as valuable as cash in the wrong hands** so store your cards securely at all times and try not to let them out of your sight.
- **Sign up to Verified by Visa or MasterCard SecureCode** whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you being a victim of online fraud. More information on how to sign up can be found at www.shopsafeonline.org.uk
- **Only shop on secure sites.** Before submitting card details ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer 7 or Firefox 2.) The beginning of the online retailer's internet address will change from 'http' to 'https' when a connection is secure. In some new browsers, such as Internet Explorer 7 and Firefox 2, the address bar may also turn green to indicate that a site has an additional level of security.
- **Never disclose your PIN to anyone and never send it over the internet.**
- **Print out your order** and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number).
- **Ensure you are fully aware of any payment commitments you are entering into**, including whether you are instructing a single payment or a series of payments.
- **Consider using a separate credit card specifically for online transactions.**

For more information on different types of fraud targeting banks and their customers go to www.bba.org.uk