

Protecting yourself

Always make sure that the internet payment provider you choose is bona fide and able to guarantee the safety of your money and personal information.

■ Check the FSA Register

The Financial Services Authority (FSA) regulates eMoney providers that issue most of the eMoney in the UK. If the provider is not regulated by the FSA and things go wrong, you may not have access to complaints procedures or compensation schemes. Regulated firms are listed on the FSA Register online at www.fsa.gov.uk/register.

■ Check the authenticity of the payment system

You should never access an internet payment system via a link embedded in an email. Type the website address into the browser yourself, or access the website through a bookmark you have created.

■ Check the security of the website

Check that a padlock symbol is displayed in either the bottom right-hand corner of the webpage or in the address bar. Click the padlock for further information about the site. The website address should also feature a 'https' prefix. For more information visit www.getsafeonline.org.

■ Know the recipient

Never send money to people or organisations that you do not know or for goods or services that you are unsure about. Read the security pages of websites offering internet payment services to understand their liabilities when making payments to other users.

■ Check the Electronic Money Association website

Many of the leading e-Money providers are also members of the Electronic Money Association (EMA). For more information visit www.e-ma.org.

Further information

- Cardwatch
www.cardwatch.org.uk
- Bank Safe Online
www.banksafeonline.org.uk
- Electronic Money Association
www.e-ma.org
- Financial Services Authority
www.fsa.gov.uk
- Get Safe Online
www.getsafeonline.org
- Trade Online Project
www.electronic-payments.co.uk
- Metropolitan Police (Fraud Alert)
www.met.police.uk/fraudalert

Fraud Advisory Panel

Chartered Accountants' Hall, PO Box 433,
Moorgate Place, London, EC2P 2BJ
Tel: 020 7920 8721
Fax: 020 7920 8545
Email: info@fraudadvisorypanel.org

Or visit:

www.fraudadvisorypanel.org

Registered Charity No. 1108863

Disclaimer

Dissemination of the contents of this Guide is encouraged. Please give full acknowledgement of the source when reproducing extracts in other published works.

Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against you and/or your business.

The Fraud Advisory Panel and the contributors to this Guide accept no responsibility for any action taken by parties as a result of reading this Guide. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

Protecting Your Payments Online

An introduction to internet payment systems

September 2007



eCommerce is growing at an exponential rate. Increasingly, customers need to be aware of the risks of making payments online.

Internet payment systems

The internet is an effective and convenient way of buying and selling goods and services. Millions of people now use the internet regularly to access their bank accounts, to pay bills and to shop online. This Guide provides an overview of the main types of internet payment systems and how you can protect yourself against fraud when using them.

There are an increasing number of ways for people to pay for goods and services online. Most internet payment systems are integrated into the checkout process of online shops but other methods are also available.

Verified By Visa/MasterCard SecureCode

- Many large online businesses and banks use internet payment systems offered by the major international credit card schemes. These are:
 - **Verified by Visa** (www.visaeurope.com)
 - **MasterCard SecureCode** (www.mastercard.com)
- These internet payment systems work in the same way. A cardholder must register a secure password with their bank which is then used to confirm the cardholder's identity when goods or services are purchased online.

eWallets/eMoney Providers

- Electronic wallets or eWallets are largely designed for person to person (P2P) payments. A user must create an account with an eWallet provider which enables them to top up, send or pay cash as they choose using their preferred method to fund their account.
- There are a number of eWallet payment systems available on the internet. Some of the most well-known eWallets are:
 - **Moneybookers** (www.moneybookers.com)
 - **Neteller** (www.neteller.com)
 - **PayPal** (www.paypal.com)

Money Transfer Services

- Money transfer services enable a user to send money to another person in any part of the world. Some of the most common money transfer services are:
 - **Western Union** (www.westernunion.co.uk)
 - **MoneyGram** (www.moneygram.com)
- Money transfer services should never be used to send money to people or organisations that you do not know or for goods or services that you are unsure about. In particular, money transfer services should never be used to pay for items you buy in eBay or other online auctions.

Stored Value Cards/Prepaid Cards

- Stored value cards (also called prepaid cards) contain monetary value. They may be prepaid and disposable (once used, they are thrown away) or reloadable online, over the phone or through a user's bank.
- Stored value cards can be used for a specific use (such as at a particular store) or for general use (such as buying small price items). Some examples of stored value cards include:
 - **Gift cards**
 - **3V vouchers** (www.3vcash.com)
 - **Splash plastic** (www.splashplastic.com)

The Risks

- **Phishing** A fraudster will send an email to a large number of people claiming to be from a bank or other legitimate online business such as a shop or auction website. The email will usually contain a link to a fake but credible-looking website where the user will be asked to update personal information such as their passwords or account details which can then be used by the fraudster.
- **Viruses/Malware** Usually a fraudster will send an email containing a virus (also called malware or malicious software) to an unsuspecting computer user. Once the email has been opened the virus will be automatically downloaded onto their computer. Viruses can also be contained in downloads from the internet. Depending upon the type of virus it may enable the fraudster to capture personal information and passwords.

Personal Internet Banking

- Personal internet banking (also called online banking) is offered by most banks and building societies. It enables a customer to check their balances and make online payments directly to third parties from their bank accounts.
- Payments can be made to a variety of people and organisations including friends and family, utility companies and charities.

Protect your money and personal information when buying goods and services online