


Internet security for financial transactions

I think that it is true to say that buying over the internet is safe providing you take some precautions against fraud, as outlined below. I have been making the following transactions involving money for the past six years or so and have never had any problems: hotel bookings; train, coach and air tickets; food and clothing shopping; banking and insurance; income tax and council tax; direct money transfers from bank accounts; charity donations; direct debits.

- 1 Use a single credit card with a relatively low maximum credit – say £500 or £1000 - to buy products and services on line. If you want to use a debit card linked into your bank account, it would be wise not to keep too much money in your current account as a precaution against fraud.
- 2 Ensure that you have an active anti-virus program installed – eg Norton or BitDefender – and that it remains subscribed to and active - see [SC41](#).
- 3 When you enter a website to which you are going to make a payment ensure that the URL (the www address) which probably began as <http://www.> now changes to <https://www.> Note the **s** – this **s** stands for **secure**. This should remain until the close of your transaction.
- 4 When the URL begins with <https://www.> There should appear alongside it a little closed padlock looking something like this . This should remain there until the close of your transaction.
- 5 Never respond to an email asking for details of your bank account, passwords or pin numbers even if it appears to be from your own bank. Genuine banks, building societies and financial institutions do not ask for such information by email, but internet crooks do, sometimes using similar headings to the genuine ones. If you receive such an email, either simply delete it or telephone your bank (using the number you normally use, or a number appearing on a bank statement you have received through the post) and tell them about the suspect email.
- 6 When you have done a financial transaction on the internet, always be sure to **log out** or **sign out** – don't just close the window by clicking on the **x** in the top left hand corner of the window.
- 7 Only do dealings or make transactions with people you feel that you can trust – in the same way that you would with any other kind of commerce.
- 8 If you are going to buy and sell using online marketplaces such as **ebay** and **Amazon**, it is a good plan to set up a PayPal account. This is another line of security. See www.paypal.co.uk .
- 9 Never disclose your financial information (bank account number, card pin numbers, etc) on an email. Emails are not secure: we don't know who sees them in transit.
- 10 Recommended reading: *Internet Security* a free booklet published by Age UK. Should be available from your local branch, or telephone 0800 169 65 65 (in the UK), or visit www.ageuk.org.uk/workandlearning
- 11 If you get an uninvited telephone call from someone, usually with a foreign accent, commenting that you may have computer problems and maybe purporting to be calling from Microsoft Windows, don't believe. It. Hang up! They are likely to begin by asking you to access your computer to help you resolve a suspected problem and eventually will invite you disclose bank or card details.
- 12 When composing passwords, use strong ones – a mixture of capitals and small letters and other symbols and punctuation marks on your keyboard. Here is a page on the Microsoft website which is helpful in relation to passwords:
<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>
Keep your passwords secret – never disclose them on an email. But remember them correctly, or you'll have problems accessing your favourite websites and documents.

PLEASE NOTE: This information is passed on freely and in good faith, as being a reflection of my own practice. However, I do not accept any liability for any losses incurred as a result of implementing the above suggestions.