

Online shopping scams

Online shopping is a fast and convenient way to make many everyday purchases. There are some simple steps that you can take to protect yourself when shopping online.

What is an online shopping scam?

Online shopping is fast becoming the preferred method of purchasing goods and services for millions of consumers. Almost anything can now be bought online. Not only is it quick and convenient, but it can also offer some of the best deals available.

It is important that you protect yourself when shopping online. Increasingly, fraudsters are turning to the anonymity of the internet to rip-off unsuspecting consumers. But by following some simple precautions you can reduce your chances of becoming a victim of an online scam.

Common types of scams

- **Fake websites:** A website which either impersonates a genuine reputable online business (by using a very similar website address) or that pretends to be a legitimate business but is not. Both are set up with the sole purpose of defrauding unsuspecting shoppers.
- **Online auction scams:** You may receive goods which are counterfeit or that differ significantly from the original description and are of a lesser value. In some cases you may receive no goods at all. The seller may also try to persuade you to pay by means other than the preferred method of the auction website.
- **Weight loss or medicine scams:** A website which offers for sale alternative slimming aids or medicines to cure obesity, cancer and other medical conditions. These products are rarely properly tested and can even be harmful.
- **Ticket scams:** A website which offers for sale hard-to-get tickets to popular sports and music events. The tickets are either never received or are counterfeit.
- **Phishing emails:** You receive an email purportedly from a legitimate and well-known online business, auction or payment provider (such as PayPal and WorldPay) which contains a link to a fake

but credible-looking website where you are asked to update your personal and/or account information. Note: banks and other legitimate online businesses will not ask you to do this.

The warning signs

Be aware of some of the warning signs of an online shopping scam:

- Products are advertised at very low prices compared to other websites – if it sounds too good to be true, then it probably is!
- Sellers and initial bidders on online auction websites with poor ratings and/or feedback.
- Online auction sellers who ask you to pay by money transfer service or direct to their bank account rather than through the site's preferred payment method.
- Websites with no contact details such as a physical address or telephone number.
- Websites with limited or no information about privacy and their terms and conditions of use.

Steps to take before you purchase online

Make sure your online purchases are secure by taking some simple precautions:

- **Protect your computer:** Keep security software (such as anti-virus and anti-spyware) and firewalls up-to-date. Update your browser regularly. Exercise caution when using public computers to make online purchases.
- **Research the seller:** Check online reviews and customer feedback to find out if the individual and/or business are reputable. UK companies should have a physical address and telephone number listed on their website. Independently verify this information. Check company information on the Companies House website.

- **Use strong passwords:** Use strong passwords when setting up online accounts. Passwords should contain a combination of letters, numbers and other characters. Change them regularly and use different passwords for different accounts.
- **Know your rights:** Read and understand the business's terms and conditions and privacy policies before you purchase.
- **Review website security:** When you proceed to checkout make sure that a padlock symbol is displayed in either the bottom right-hand corner of the webpage or in the address bar. Click the padlock to make sure the security certificate is valid. The website address should begin with 'https'.
- **Take extra precautions for online auction websites:** Do not make payments directly to a seller's bank account – regardless of the reasons given. Use the auction website's preferred payment methods (eg. PayPal for eBay) to ensure access to their disputes resolution processes.
- **Use a credit card:** Purchases made with a credit card for goods valued over £100 and under £30,000 are protected by Section 75 of the Consumer Credit Act 1974. This means that if anything goes wrong, your card issuer is jointly liable with the retailer. Sign up to Verified by Visa or Mastercard SecureCode for additional security. Consider using a prepaid credit card for smaller purchases.
- **Keep a record:** Keep a record of your online purchases. Regularly monitor your bank, credit card, and store card statements for any unusual transactions.

Reporting scams

If you think you may have become the victim of a scam, report it to Consumer Direct by calling 08454 04 05 06 or visiting the website www.consumerdirect.gov.uk. This may help prevent others from being ripped-off by similar scams.

Report fraud to your local police station or Action Fraud by calling 0300 123 2040 or visiting the website www.actionfraud.org.uk.

Recovering your money

It may be hard to recover any money that you have lost to a scam, particularly if the seller is based overseas.

In most cases reporting the matter to the police or to Action Fraud will represent the most realistic prospect of recovering any money lost.

Further information

See our separate fraud factsheet on *Cybercrime – Email and Internet Scams* for more information.

Action Fraud

www.actionfraud.org.uk

Companies House

www.companieshouse.gov.uk

Consumer Direct

www.consumerdirect.gov.uk

Fraud Advisory Panel

www.fraudadvisorypanel.org

Get Safe Online

www.getsafeonline.org

SafeBuy

www.safebuy.org.uk

Scambusters

www.scambusters-uk.org

Shopsafe

www.shopsafe.co.uk

How to protect yourself

DO:

- ✓ Keep security software and firewalls up-to-date.
- ✓ Update your internet browser as and when a new patch is released.
- ✓ Research a seller before making an online purchase. Independently verify their contact details and other company information.
- ✓ Be wary of unsolicited emails from online businesses that you do not know.
- ✓ Use strong passwords which contain a combination of letters, numbers and other characters. Change them regularly and use different passwords for different online accounts.
- ✓ Read and understand the seller's terms and conditions and privacy policies.
- ✓ Check that a padlock symbol is displayed in either the bottom right-hand corner of the webpage or in the address bar when you proceed to checkout.
- ✓ Make sure the website address begins 'https' at the payment stage.
- ✓ Exercise caution when using internet auction websites and use their preferred payment methods to purchase items.
- ✓ Use a credit card for online purchases (or a prepaid credit card for smaller purchases).
- ✓ Keep a record of your online transactions and regularly reconcile them with your bank and credit card statements.
- ✓ Be wary of buying goods from overseas companies.

DO NOT:

- ✗ Shop online using public computers if you can avoid it.
- ✗ Pay for purchases with a debit card – use a credit card or prepaid card instead.
- ✗ Pay for purchases using money transfer services.
- ✗ Access websites via links embedded in emails. Type the website address into the browser yourself.
- ✗ Respond to unsolicited emails from people or businesses you don't know. Delete them.
- ✗ Divulge personal or financial information and passwords to anyone requesting them by email.
- ✗ Use the same password for all your online accounts and websites.
- ✗ Use 'easy' passwords (such as any word from a dictionary).
- ✗ Disclose personal or credit card information on a website unless it is secure.
- ✗ Believe everything you read – if it sounds too good to be true, it probably is!

The Fraud Advisory Panel gratefully acknowledges the contribution of Dr Stephen Hill (Snowdrop Consulting Ltd) and Mia Campbell in the preparation of this Fraud Facts.

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.
Registered Charity No. 1108863

Disclaimer

Dissemination of the contents of this Fraud Fact Sheet 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 Fraud Fact Sheet, 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 Fraud Fact Sheet accept no responsibility for any action taken by parties as a result of any view expressed herein. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

© Fraud Advisory Panel, 2010

Distributed by