



SHOPPING SAFELY ONLINE

10 tips for safer online shopping



Make sure the site is secure

Be careful when using sites that don't have 'https' at the start of the URL (the 's' stands for secure). There should also be a small padlock symbol in the browser bar.



Watch out for fake websites

Make sure the site is legit by checking the contact details and physical address. Look out for reviews written by other shoppers.



Don't buy from spam or phishing emails

Phishing messages are designed to appear from trusted organisations or known retailers to trick consumers into entering personal details.



Pay by credit card

Credit cards offer consumers more protection than other payment methods.



Avoid shopping on public wi-fi

Data sent through public networks can be easily intercepted. Avoid making financial transactions on public wi-fi and use a password protected network.



Use trusted online payment options

Use tried and tested payment methods such as Google Wallet, which offer buyer protection.



Add an extra layer of security

Register your credit card with Verified by Visa, Mastercard SecureCode or American Express SafeKey for added security.



Use security software

Look for a product that protects against viruses and spyware, blocks malicious websites, provides lost-device protection and offers automatic updates.



Log out when you've finished

Always log out after an online transaction instead of just closing the window.



Keep an eye on your bank account

Review your bank statements and check up on any suspicious activity.

Using mobile devices



UK shoppers spend more via their smartphones than any other European market, with over **70%** of shoppers now buying online.



Keeping your mobile phone secure

- ✓ Update your operating system
- ✓ Stick to official app stores
- ✓ Download a mobile security app
- ✓ Fine-tune your app permissions
- ✓ Take care when using public wi-fi

Additional security measures

TERMS AND CONDITIONS: Introduction. These Website Standard Terms and Conditions apply to the website and any services provided by the website. These terms will be applied fully and affect to your use of the website. If you disagree with any of these terms and conditions, you should not use the website. You agree that you own, under these terms, the intellectual property rights and materials contained on this Website. You are specifically restricted from all of the following: Publishing any Website material in any other media setting.

Check the small print

Read the retailer's terms and conditions, privacy and returns policy.

Be a password pro

One of the best ways to keep online accounts secure is to never use the same password more than once.

Always install updates

Make sure your security software is up to date.

Look for the green address bar

It shows visitors the transaction is EV SSL-encrypted and the site has been authenticated according to industry standards.

How to get your money back after a scam

Credit card payments

If you paid with a credit card, you're protected under Section 75 of the Consumer Credit Act or through the chargeback scheme.



Debit card payments

If you paid by debit card, you may be able to ask your bank to reverse the transaction through chargeback.

Bank transfers

If you've transferred your money into another bank account, contact your bank immediately. Your bank can try and recover the funds.



PayPal payments

If you paid via PayPal and didn't receive the item, you should be covered by PayPal Buyer Protection.

Reporting a scam

- 1
- 2
- 3

Action Fraud

Fraud and cybercrime reporting centre that help prevent scams and keep consumers safe. You can report online or by calling 0300 123 2040.

Citizens Advice / Trading Standards

You can also report online scams to Trading Standards via the Citizens Advice Consumer Helpline on 0345 404 0506.

Small claims court

You can take your dispute here as a last resort.