Shopping and paying safely online

Tips to help you purchase items safely and avoid fraudulent websites.

With so many of us now shopping online, it's no surprise that criminals are increasingly turning to web-enabled fraud to steal our money and personal details. The following tips will help you stay safe when shopping online for goods and services.

Check the shop is legitimate

You can research online shops to check they're legitimate, particularly if it's a store you've not used before. Use consumer websites, or reviews from people (or organisations) that you trust.

You might receive suspicious emails or texts (known as phishing messages) that contain links to fake shops, with promotions that seem too good to be true. These days it's easy for a criminal to duplicate the design of a legitimate website, which will often include logos, trademarks and products copied from a genuine store. Many will also use a deceptive website domain (for example, www.tescos-sales.com), that can be easily mistaken for a genuine domain (www.tesco.com).

If you're unsure about a link you receive, **don't** click on it. Instead you can:

- type the official website address of the organisation (if you know it) directly into the browser's address bar
- search for the organisation, and then take time to read the entries on the results page (don't just click the top item)

Use a credit card to pay

- Use a credit card for payments (if you have one). Many of these protect online purchases as part of the Consumer Credit Act.
- Debit card payments offer less protection, but you might be able to make a claim for a refund under a voluntary scheme called 'chargeback'.
- If you use payment services such as PayPal, Apple Pay or Google Pay, check their 'terms & conditions' to see what cover they provide.
- Never pay by direct bank transfer.

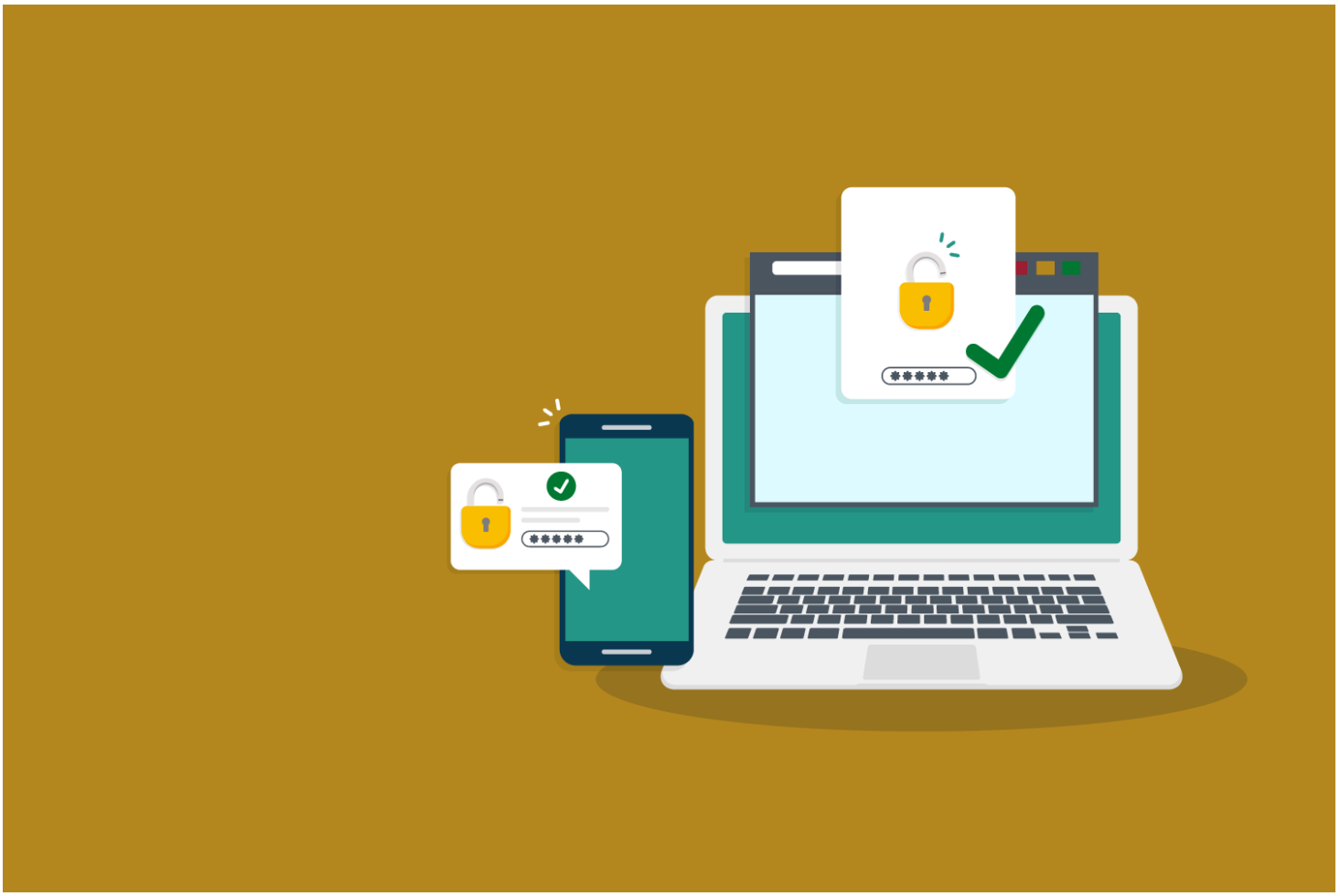
Only provide required details on checkout

When making your payment, only fill in the mandatory details (often marked with an asterisk) such as your address. Unless you think you'll become a regular customer, **don't** create an account for the store:

- there's often an option to 'check out as a guest', which means you don't need to create an account to complete the payment
- similarly, using an online payment platform (such as PayPal/Apple/Google) usually means you won't need to create an account
- don't let your browser remember your payment details (if you're prompted)
- if you decide to create an account for the store, don't allow them to store your bank details for future purchases

---

Keep your accounts secure



ISTOCK.COM/PAPERFOX

Make sure your shopping, online banking and payment accounts are protected by strong passwords that you **don't** use for any other account. If you're using the same password for lots of accounts, criminals could steal your password from one account, and use it to access your other ones.

For this reason, you should make sure that **all** your important online accounts (such as email, banking, and social media accounts) have unique, strong passwords. This NCSC infographic explains how you can create strong passwords and store them safely (so you don't need to remember them).

Download the NCSC's password infographic (pdf)

You should also turn on 2-step verification (2SV) for **all** your important online accounts. This can stop hackers from accessing your accounts - even if they know your password - by asking you to confirm your identity using a second method, for example by sending a confirmation code to your phone. Note that 2SV is sometimes called 'two-factor authentication' (or 2FA).

Watch out for suspicious links

Cyber criminals insert malicious links into SMS text messages, emails, and increasingly on social media posts. These can be difficult to spot, and will often include unbelievable offers for goods and services with links to websites designed to look like legitimate online stores.

These websites are managed by criminals, and are designed to trick people into making payments, or revealing their bank details, passwords, or other personal information.

If a text message, email, website or social media post doesn't feel right, follow the NCSC guidance on dealing with suspicious emails and text messages:

- If you have received an **email** which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**
- If you've received a suspicious **text message**, forward it to **7726**. It won't cost you anything, and allows your provider to investigate the text and take action (if found to be a scam).
- If you have visited a **website** you think is trying to scam you, report it to the NCSC and we'll investigate.
- If you come across an **advert** online that you think might be a scam, report it via the Advertising Standards Authority (ASA) website. This allows ASA to provide online service providers with the details they need to (if appropriate) remove these from websites.

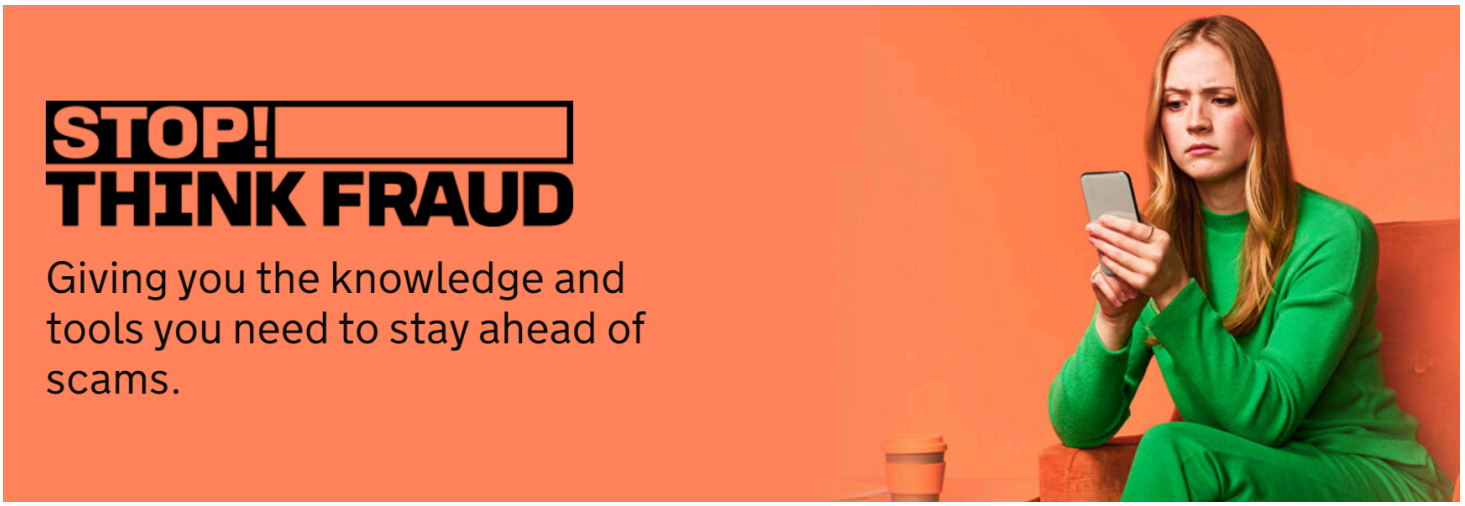
If things go wrong

If you you've been tricked into making a payment, tell your bank and report it as a crime to Report Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland).

If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it. Always contact your bank directly using the official website or phone number.

If you don't receive an item you've purchased (or it doesn't match the description given), Citizens Advice has some useful information about getting your money back if you paid by credit card, debit card or PayPal.

Further resources



- **Stop! Think Fraud** is the home of the UK government's national campaign against fraud. The website contains advice on how to protect yourself from all kinds of fraud - including online fraud.
- Consumer organisation **Which?** have published advice on how to spot fake reviews, which can help you to identify fake shops.
- Martin Lewis's team at Money Saving Expert have published advice on avoiding online scams.

Lead Scotland have produced the NCSC's advice on shopping online safely in the following formats: British Sign Language and Easy Read Versions, these are available from the Lead Scotland website.

View accessible formats of NCSC advice

PUBLISHED

/

17 January 2019

REVIEWED

15 July 2024

VERSION

2.0

WRITTEN FOR

You & your family