How to shop and pay safely online

National Cyber Security Centre
a part of GCHQ

Criminals are increasingly turning to web-enabled fraud to steal our money and personal details. The following tips will help you purchase items safely and avoid fraudulent websites.

Check the shop is legitimate

Research online shops to check they're legitimate, especially for stores you've not used before. Use consumer websites, or reviews from people that you trust.

If you receive a suspicious link to an online store, don't click on it, and instead:

- 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 check 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 protect online purchases as part of the Consumer Credit Act.
- Debit card payments offer less protection, but some provide refunds under a voluntary scheme called 'chargeback'.
- If using services such as PayPal, Apple Pay or Google Pay, check their 'terms & conditions' to see what cover they provide.

Only provide required details at checkout

- Unless you think you'll shop regularly, don't create an account for the store. Instead look for 'check out as a guest' option.
- Using online payment services (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, don't allow them to store your bank details for future purchases.

Keep your accounts secure

- Make sure your shopping, online banking and payment accounts are protected by strong passwords that you don't use for any other account.
- This NCSC infographic explains how you can create strong passwords and store them safely.
- Turn on 2-step verification (2SV) for all your shopping, banking and payment accounts. This can stop hackers from accessing your accounts - even if they know your password.

Watch out for suspicious links, reviews and websites

- Links in SMS text messages, emails, and on social media posts, often promote unbelievable offers with links to websites.
- These websites - which look identical to legitimate online stores - are managed by criminals, and are designed to trick people into making payments, or disclosing their bank details.
- 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.

What to do if you've been scammed?

If you you've been tricked into making a payment, tell your bank and report it as a crime to Action 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 using the official website or phone number.

If you don't receive an item you've purchased, Citizens Advice has some useful information about getting your money back if you paid by card or PayPal.

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre