National Cyber Security Centre
a part of GCHQ

Shopping online securely

How to shop safely online

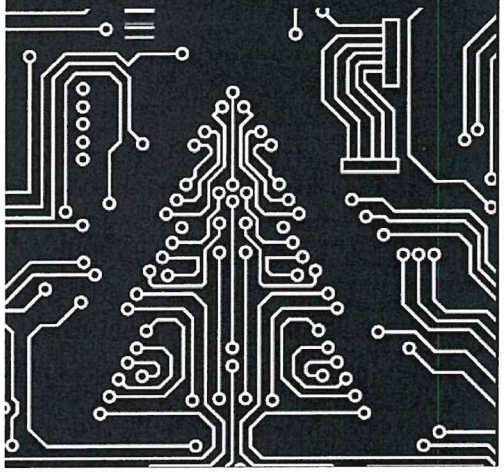
With the festive period approaching, many of us are spending more time than ever shopping online. The following tips can help you to avoid scam websites, and purchase items safely.

What to do if you think you've been scammed:

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 using the official website or phone number.

If you've lost money, tell your bank and report it as a crime to Action Fraud (0300 123 2040 for England, Wales and Northern Ireland) or Police Scotland (for Scotland). By doing this, you'll be helping to prevent others becoming victims of cyber crime.

If you don't receive the item (or it doesn't match the description given), Citizens Advice (0800 144 8848) has some useful information about getting your money back if you paid by credit card, debit card or PayPal.



Choose carefully where you shop

- Read feedback from people or organisations that you trust, such as consumer websites.
- Some of the emails/texts you receive about amazing offers may contain links to fake websites. If you're unsure, don't use the link, and either type a trusted website address directly into the address bar, or search for it (and follow the results).

Use a credit card for online payments

- Most credit card providers protect online purchases, and must refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected.
- Debit card payments and purchases are not covered by the Consumer Credit Act. But you might be able to make a claim for a refund under a voluntary scheme called 'chargeback'.
- Consider using an online payment platform, such as PayPal, Apple Pay or Google Pay. Using these platforms to authorise your payments means the retailer doesn't even see your payment details.
- When it's time to pay for your items, check there's a 'closed padlock' icon in the browser's address bar. It will look like this:

  https://www.ncsc.gov.uk

- If the padlock icon is not there, or the browser says not secure, then don't use the site. Don't enter any personal or payment details, or create an account.

Only provide enough details to complete your purchase

- You should only fill in the required details when making a purchase. These are often marked with an asterisk (*), and will typically include your delivery address and payment details.
- If possible, don't create an account for the online store when making your payment. You can usually complete your purchase by using a payment platform (such as PayPal, Google Pay or Apple Pay).
- If prompted, don't let the website store your payment details for a quicker check-out next time (unless you're going to shop with them regularly).

Keep your accounts secure

- Make sure your really important accounts (such as email, social media, banking, and shopping accounts) are protected by strong passwords that you don't use anywhere else.
- To create a memorable password that's also hard for someone to guess, you can combine three random words to create a single password (for example cupfishbiro).
- Turn on 2-step verification (2SV), which is also known as 'two-factor authentication' or 'multi-factor authentication'. Turning on 2SV stops hackers from accessing your accounts, even if they know your password.

If something feels wrong, report it

- If you have received a suspicious email, 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's free, and your provider can investigate 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.