Stay safe online · Shopping safely

How to shop safely online this Black Friday and Christmas

Fraudsters use the Black Friday and Christmas rush to sell things that never arrive, through fake shops, social media adverts and messages that look real. Find shops yourself instead of following links, pay by credit card or a payment service with buyer protection, never pay by bank transfer, and ignore texts asking you to pay a delivery fee.

By the Cyberend team · Published and updated 26 November 2026

THE QUICK VERSION

- **Go to shops yourself:** type the address or search for it, rather than tapping a link in an advert, email or text NCSC.
- **Pay with protection:** a credit card, or a payment service like PayPal, Apple Pay or Google Pay. Never pay a stranger by bank transfer NCSC.
- **Ignore "pay a delivery fee" texts:** Royal Mail doesn't ask for payment for underpaid post by text or email. It leaves a grey card Royal Mail.
- **Act fast if it goes wrong:** call your bank on 159 or the number on your card, then report it Report Fraud.

Why scams rise at this time of year

Black Friday, Cyber Monday and Christmas mean lots of people shopping quickly, on lots of different sites, looking for a bargain. Criminals know that, and they build fake shops, adverts and messages to match Report Fraud.

Stolen from online shoppers

£18.3m

Reported to Report Fraud between 1 November 2025 and 31 January 2026 Report Fraud

Reports of shopping fraud

14,000+

Over the same festive period Report Fraud

Official guidance

Average loss per victim

£1,278

For each victim who made a report Report Fraud

Official guidance

Official guidance

Those numbers only count people who reported it, and many people don't. The good news is that a few simple habits stop most of these scams.

The scams to watch for

Fake shops

Websites that look like real retailers, often with huge discounts, built to take your money or card details. They can appear near the top of search results Report Fraud.

Scam adverts

Adverts on social media and websites for sold-out or popular products at prices that seem too good to be true NCSC.

Fake sellers on marketplaces

Profiles on social media and marketplaces selling sought-after items, who disappear once they've been paid Report Fraud.

Fake delivery texts

Messages claiming a parcel is waiting and asking for a small fee or for you to install a tracking app NCSC.

Counterfeits and swaps

Goods sold as genuine that turn out to be fake, or something of little value sent in place of what you ordered Report Fraud.

Order and account emails

Emails and texts pretending to be from a shop or bank, with a link to "check your order" or "fix a payment". The link leads to a page that steals your details NCSC.

Urgency is the giveaway

"Only 2 left", "ends in 10 minutes", "pay today or your parcel goes back". Scammers rush you so you don't stop to check Report Fraud. A real deal will still be there after a two-minute check.

Check before you buy

Especially with a shop you haven't used before, run through this first:

A TWO-MINUTE CHECK

- [ ] You found the shop yourself, by typing its address or searching for it, not through a link you were sent NCSC.

- [x] You've read reviews from sites or people you trust, not just the reviews on the shop's own page **Report Fraud**.
- [x] The web address is spelt exactly right. Fake shops often use a name that's one letter off, or an unusual ending.
- [x] The price makes sense. If a brand-new console or designer item is far cheaper than everywhere else, assume it's a scam.
- [x] The checkout lets you pay by card or a payment service. If it pushes you to pay by bank transfer, walk away **NCSC**.

When you do buy, only fill in what's needed, like your delivery address, and check out as a guest if you don't plan to shop there again. That's one less account to keep safe NCSC.

Pay the safe way

How you pay decides how easily you can get your money back if the item never turns up or isn't what was promised.

Credit card

IF SOMETHING GOES WRONG

For a single item over £100 and up to £30,000, you can claim from your card provider under Section 75 of the Consumer Credit Act **Citizens Advice**. Below £100, ask for a chargeback.

Debit card

IF SOMETHING GOES WRONG

Less protection, but you can ask your bank for a chargeback, a voluntary scheme for getting money back **NCSC**.

PayPal, Apple Pay, Google Pay

IF SOMETHING GOES WRONG

Your card details aren't shared with the shop. Check each service's buyer protection. With PayPal you have 180 days to open a dispute **Citizens Advice**.

Bank transfer

IF SOMETHING GOES WRONG

Very hard to get back. The NCSC's advice is never to pay by direct bank transfer when shopping online **NCSC**.

Section 75 doesn't usually cover things bought through a marketplace like eBay or Amazon from another seller, or paid for through PayPal, so use that service's own dispute process instead Citizens Advice.

Fake delivery texts

Around Christmas almost everyone is waiting for a parcel, which makes fake delivery texts very convincing. They usually say a parcel couldn't be delivered and ask you to pay a small fee or rebook through a link.

WHAT ROYAL MAIL SAYS IT DOES AND DOESN'T DO

- It only texts or emails you if the sender asked for tracking updates when they posted the item Royal Mail.
- It never asks for your bank details or passwords Royal Mail.
- If you owe money on underpaid post, it leaves a grey "Fee to Pay" card. It doesn't ask for payment by text or email. The one exception is customs fees, where it may message you as well as leaving the card Royal Mail.

Some fake texts ask you to install a "tracking app". These can be malware that steals banking details and passwords. To check a delivery, go to the courier's official website or use its official app from your phone's app store NCSC.

Got one? Forward it

Forward scam texts to **7726** for free so your provider can investigate. Forward scam emails to **report@phishing.gov.uk** NCSC. Then delete them.

Lock down your accounts

Your shopping, bank and email accounts are worth protecting properly, especially when you're signing in to lots of sites in a short time NCSC.

Use passkeys

If a site offers a passkey, use it. It signs you in with your face, fingerprint or phone PIN, and can't be phished like a password.

One password per site

Never reuse a password. A password manager, or the one built into your phone or browser, remembers them for you.

Turn on 2-step verification

A code or prompt on your phone means a stolen password alone isn't enough to get into your account.

The NCSC also suggests letting your browser, phone or password manager save your card details rather than saving them on each shop's website NCSC.

If you've been scammed

It happens to careful people too, and scammers are good at what they do. What matters is acting quickly.

STEP 1

Call your bank

Dial 159 or the number on your card

STEP 2

Report it

Report Fraud, or Police Scotland on 101

STEP 3

Change passwords

On any account you used, starting with email

STEP 4

Ask for a refund

Section 75, chargeback or a PayPal dispute

Call your bank first. It can block your card and may be able to stop the payment Report Fraud. **159** connects you directly to most UK banks and can't be faked by scammers Stop Scams UK. Otherwise, use the number on the back of your card or in your banking app.

Report it. In England, Wales and Northern Ireland, report it to Report Fraud at reportfraud.police.uk or on 0300 123 2040. Report Fraud replaced Action Fraud in December 2025. In Scotland, call Police Scotland on 101 Report Fraud.

Ask for your money back. If you paid by card or PayPal, Citizens Advice explains how to claim, depending on how you paid Citizens Advice.

Watch out for a second scam

After a scam, some people get calls offering to "recover" their money for a fee. Your bank will never ask you to move money to a "safe account". If someone calls claiming to be your bank, hang up and call 159 yourself Stop Scams UK.

KEY TAKEAWAY

Find the shop yourself, pay with protection, ignore delivery-fee texts, and if something feels off, stop and check. Share this with anyone you know who's shopping online this Christmas.

Common questions

Does the padlock in my browser mean a website is safe?

No. The padlock means your connection to the site is encrypted, so nobody can read what you send on the way. Scam websites can have a padlock too. It tells you nothing about whether the shop is genuine.

Is it safe to buy from sellers on social media?

It can be, but fake seller profiles are one of the most common tricks at this time of year Report Fraud. Never pay a private seller by bank transfer, and be very wary of anyone who asks you to pay outside the platform.

I clicked a link in a delivery text. What should I do?

If you entered card details, call your bank straight away. If you entered a password, change it, and change it anywhere else you use it. If you installed an app from the link, the NCSC has step-by-step advice on what to do next NCSC.

Is Action Fraud still the place to report fraud?

Action Fraud was replaced by Report Fraud on 4 December 2025. If you try to use Action Fraud you'll be redirected. In Scotland, report to Police Scotland on 101 Report Fraud.

Where can I find more advice?

The government's Stop! Think Fraud campaign has advice on every kind of fraud Stop! Think Fraud, and the NCSC's guide to shopping and paying safely online goes into more detail NCSC.

Sources and method

This guide is based on advice from the National Cyber Security Centre, Report Fraud (the UK's national fraud reporting service), Citizens Advice, Royal Mail and Stop Scams UK. The figures on losses come from reports made to Report Fraud, so they count only the people who reported what happened to them.

It's general advice, not legal or financial advice. If you've lost money, speak to your bank first, because it can act faster than anyone else.

Report Fraud (City of London Police): Have a Fraud Free Xmas

Official guidance

Reports of online shopping fraud made to Report Fraud between 1 November 2025 and 31 January 2026, and the most common methods used. Published 23 November 2026.

National Cyber Security Centre: Shopping and paying safely online

Official guidance

Official advice on checking shops, reporting scam emails, texts, websites and adverts, securing accounts and choosing a payment method. Reviewed 24 November 2026.

Report Fraud (City of London Police): Shopping fraud

Official guidance

How to protect yourself from online shopping and auction fraud, and what to do if you've paid a fraudster.

Citizens Advice: Getting your money back if you paid by card or PayPal

Consumer advice

How Section 75, chargeback and PayPal disputes work, including the £100 to £30,000 limit and the 180-day PayPal deadline.

Royal Mail: Royal Mail scam advice

Consumer advice

When Royal Mail does and doesn't text or email, how it asks for fees, and where to report fake Royal Mail messages.

National Cyber Security Centre: Scam 'missed parcel' SMS messages

Official guidance

How fake delivery texts push malware disguised as tracking apps, and how to check a parcel safely.

Report Fraud (City of London Police): Report Fraud service goes live

Official guidance

Report Fraud replaced Action Fraud on 4 December 2025 for England, Wales and Northern Ireland. People in Scotland report to Police Scotland on 101.

Stop Scams UK: 159 phone number

Consumer advice

The 159 short number, which connects customers of most UK retail banks directly and safely with their bank.

UK Government: Stop! Think Fraud

Official guidance

The government's national campaign against fraud, with advice on spotting and reporting scams.

Every figure and link in this guide was checked against its source on 26 November 2026. Live job listings update every few hours.

This is a PDF copy of a free Cyberend guide. Read it online, with today's live UK cyber security jobs, at cyberend.io/stay-safe-online/black-friday-christmas-shopping-scams.