

Avoid Black Friday turning into Black Fraud Day...

BLACK FRIDAY 27 NOVEMBER 2026 | CYBER MONDAY 30 NOVEMBER 2026

Black Friday and Cyber Monday sales now stretch across much of November. Genuine savings sit alongside fake websites, impersonated brands and increasingly polished scam messages. Annual Fraud Report 2025 (UK Finance) showed an increase of 620% totaling about £1.1 bn in 2025, so a quick pause before paying can make a real difference. Please find some tips below to keep you safe online.

✓ Shop through trusted routes

Go directly to a retailer using a trusted bookmark, app or independently searched web address. Avoid links in unexpected emails, texts and social media adverts, which can lead to cloned websites designed to steal payment details.

Check for brand impersonation

Criminals copied familiar logos, language and website designs throughout the 2025 campaign period. Check the exact web address, seller details, contact information, independent reviews and returns policy before buying.

⚠ Do not trust a message because it looks polished

AI-assisted adverts, emails, images and videos can appear convincing and professional. Poor spelling is no longer a reliable warning sign. Verify the offer through the retailer's official website or app.

? Question huge discounts, giveaways and mystery boxes

Limited-time prizes, "pay postage only" offers and mystery boxes may be used to create urgency and collect personal or card details. Compare the price with the usual selling price and do not be pressured into acting immediately.

Check the complete cost, including delivery

An item may appear reasonably priced, or unusually cheap, but a very large delivery charge can appear at checkout. Check the final total, published delivery terms, taxes and add-ons before paying. If the charge is unclear or disproportionate, leave the site.

Beware of fake delivery messages

Unexpected messages claiming that a parcel is delayed, an address is incomplete or a small fee is due may link to a fake courier page. Do not follow the link. Check any delivery directly through the retailer or courier's official website.

Avoid counterfeit or unsafe products

Very low prices on branded goods can indicate counterfeits. Check the seller, independent reviews, returns information and product-safety details. Report suspected counterfeit or unsafe goods to Gloucestershire Trading Standards.

Use safer ways to pay

Use a credit card where appropriate, or a reputable payment service, and check what buyer protection applies. Avoid direct bank transfer. Check out as a guest where possible and do not allow unfamiliar websites to store card details.

Secure important accounts

Use strong, unique passwords and turn on 2-step verification for email, shopping and payment accounts. Keep devices and apps updated and monitor bank and card statements for transactions you do not recognise.

Act quickly if something goes wrong

If money or banking details may be at risk, stop the payment and contact your bank immediately using a trusted route. For a suspicious call about your finances: stop, hang up and call 159 to connect securely to a participating bank.

Report fraud or cyber crime in England, Wales or Northern Ireland to Report Fraud online or on **0300 123 2040.**

Forward suspicious emails to report@phishing.gov.uk and suspicious texts to **7726.**

If someone is in immediate danger, call 999.

Useful guidance

- Stop! Think Fraud
- Report Fraud: report fraud or cyber crime
- NCSC: report suspicious emails and texts
- 159: stop, hang up and call your bank securely
- Gloucestershire Trading Standards: product safety
- Glass Jar: Gloucestershire fraud advice and support

Counter Fraud Team | fraud@gloucestershire.gov.uk | 01452 427052

Happy shopping, and stay safe!