# ALERT
# TRADING STANDARDS
# Date: 19/11/2026

## Classic signs that a Black Friday deal may be a scam are:

With bargain deals bombarding your inbox and social media feeds, it can be hard to weed out the legitimate offers from the scams.

Be additionally cautious with Black Friday deal emails landing in your inbox – double-check the sender's details and inspect all links before you click on them. Rather than following the link from the email, consider visiting the retailer's website directly as this will help you avoid clicking on any malicious links.

- Unrealistically low prices, so always check that the price of the item is consistent with other websites.
- Being promoted on a recently created website without a privacy policy, postal address or an 'about us' page. Use a domain checker like who.is to check when the website was created, a newly created website should ring alarm bells.
- Being posted from a newly created social media account.
- Only allowing you to pay via bank transfer which offers limited protection in the event of a scam, so opt for a credit or debit card or PayPal instead.
- Bad reviews can be a giveaway.
- An impersonated URL – check that the website URL is that of the official brand. It will only have one official website.

- **NEVER open attachments or links in unsolicited emails**
- **NEVER give out personal information**
- **DELETE spam emails from your mailbox**

## WHERE TO REPORT

**Protect others by reporting incidents like this.**

**Report suspicious texts** you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad

**Report suspicious emails** you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk

**If you, or anyone you know, have been affected by this fraud or any other scam, report it to Report Fraud by calling 0300 123 2040 or visiting www.reportfraud.police.uk**

**tradingstandards@royalgreenwich.gov.uk**