Black Friday security checklist:
5 things to check before you buy

Black Friday is packed with discounts, distractions and more phishing attempts than you might expect. With inboxes buzzing and adverts popping up everywhere, it's easy to get caught out. A quick sense check before you click can make all the difference.

Use this checklist to help you stay safe whilst you shop:

1. Verify the sender's domain

- [ ] Does the email domain match the official retailer or company?
- [ ] Is the spelling correct? Swapped letters or extra characters are a big giveaway.
- [ ] Does the display name on the email match the email address?

2. Hover over links before clicking them

- [ ] Does the URL look legitimate when you hover over any links (without clicking on them)?
- [ ] Is the URL using "https://" and a trusted domain name?
- [ ] Does the link match what the email says it should be? Or the senders email address?

3. Look for spelling or grammar errors

- [ ] Are there odd word choices or formatting issues?
- [ ] Does the message sound odd? Or unlike the brand?
- [ ] Are there obvious mistakes you wouldn't expect from a major retailer?

4. Be cautious of urgent or "limited time" offers

- [ ] Is the message pushing you to act immediately?
- [ ] Does the offer seem unusually generous or unrealistic?
- [ ] Are you feeling rushed or pressured to click or buy?

5. Report anything that feels suspicious

- [ ] Does something feel "off" even if you can't explain why?
- [ ] Have you checked with a colleague if they've received something similar?
- [ ] Have you reported it to your IT or security team?