

Christmas security checklist:

5 checks before you click

Before clicking on any festive deals, take a moment to check the sender, links and look out for any spelling or grammar mistakes. Be cautious of urgent or “limited time” offers and report anything that feels suspicious. Following these simple steps can help you and your team enjoy a safer, stress-free Christmas period.

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

1. Check the sender carefully:

- Confirm the email address or phone number matches the official retailers.
- Look for subtle misspellings or extra characters in the domain, email address or link.
- Verify the message by visiting the retailer’s website directly, instead of clicking through links.

2. Carefully inspect links:

- Hover over links to see the actual URL before clicking them.
- Is the URL using “https://” and has the padlock symbol in the browser?
- Avoid clicking shortened or suspicious links from unknown sources.

3. Watch out for unusual language:

- Check for spelling mistakes or poor grammar.
- Be cautious of generic greetings like “Dear Customer”.
- Look for inconsistencies in branding, logos or message formatting.

4. Don't rush into “limited time” offers:

- Pause and think before acting on urgent messages.
- Verify the offer on the retailer's official website.
- Avoid sharing personal or financial information under time pressures.

5. Flag suspicious messages immediately:

- Report the message to your IT or security team.
- Inform colleagues or family who might have also been targeted.
- Delete the message after you've reported it to avoid any accidental clicks.