

7 RED FLAGS FOR EMAILS



URGENT CALLS TO ACTION

Legitimate companies will call you by your name. Criminals often can't. Look out for "Dear valued customer"

Criminals will try to rush you into clicking a link before you think about it. "Click here now!"



LACK OF PERSONALISATION

ACB POOR SPELLING AND GRAMMAR

Criminals frequently imitate reputable brands; be wary of outdated visuals or inconsistent designs.

Phishing emails frequently include spelling and grammar mistakes.



INCONSISTENT DESIGN



UNUSUAL EMAIL ADDRESS

Legitimate companies rarely request your data through email. Criminals aim to gather information about you to take advantage of you.

Look carefully at the email address of the sender. It might look legitimate but does it match prior communication from them?



PERSONAL DATA



UNEXPECTED LINKS

If the email is unexpected, legitimate companies will rarely include links. If uncertain, navigate to the company's official website away from the email.