

PHISHING CHECKLIST

Five checks before you click

Run through these before you act on any email, text or message you weren't expecting.



Who really sent it?

Read the full address, not just the name. Watch for lookalike domains and free email accounts.



Where does the link go?

Hover over it, or press and hold on a phone, and read the address before you click.



Were you expecting it?

Surprise invoices, shared files, voicemails and HTML attachments are common lures.



What is it asking you to do?

Sign in, pay, change bank details, buy vouchers, or hurry? Stop and check.



Does it fit?

If it isn't how this person normally asks, check by phone on a number you already have.



Not sure? Don't click. Report it.