

10

Signs of a Phishing Email

Urgent or threatening language
– e.g. “Act now!”, “Your account will be locked”

Unexpected sender
– Someone you don’t normally deal with or weren’t expecting an email from

Generic greeting
– Like “Dear customer” instead of your actual name

Spelling or grammar errors
– Many phishing emails have mistakes or odd phrasing

Suspicious links or attachments
– Links may not match the legitimate website URL

Too good to be true offers
– Promises of prizes, refunds or free items

Requests for sensitive information
– Like passwords, card details, or login codes

Impersonating a trusted brand
– Fake logos, signatures, or email addresses

Strange email addresses
– Slight misspellings or extra characters in domains

Unusual requests
– Asking you to perform actions out of the ordinary (e.g. buying gift cards)

