# A picture containing text, clock  AI-generated content may be incorrect.

# Can You Spot the Phishing Email?

**Instructions:** Below are four email screenshots. One of them is a phishing attempt designed to look legitimate. Review each email carefully and mark which one (1–4) you believe is the phishing email. For the email you select, list the clues that made you suspicious (e.g., sender address mismatch, unusual link, urgent language, grammar errors, unexpected attachment).

## There is an answer key at the end of the images but DO NOT CHEAT. This exercise is meant to test your knowledge and help you understand what to look for when identifying a phishing email.Email #1



## Email #2



## Email #3



## Email #4



# Answer Key

Phishing email: Image 3 (page 3 of the document)

Reasons:

- Sender domain mismatch: the display name shows 'Acme Utilities Support' but the sender address is support@acmewb.com (notice the misspelling of the domain).

- Suspicious visible URL: the link shown (http://acme-pay.verify-account.com/update) does not match the company domain and contains extra segments that are commonly used in phishing URLs.

- Urgent language and threats: the message pressures the recipient to act within a short timeframe (24 hours) to avoid disconnection — common phishing tactic.

- Inconsistent technical headers: the Reply-to and Message-ID fields suggest different domains (reply-to uses acmeutilities.com while the message ID uses acmewb.com).