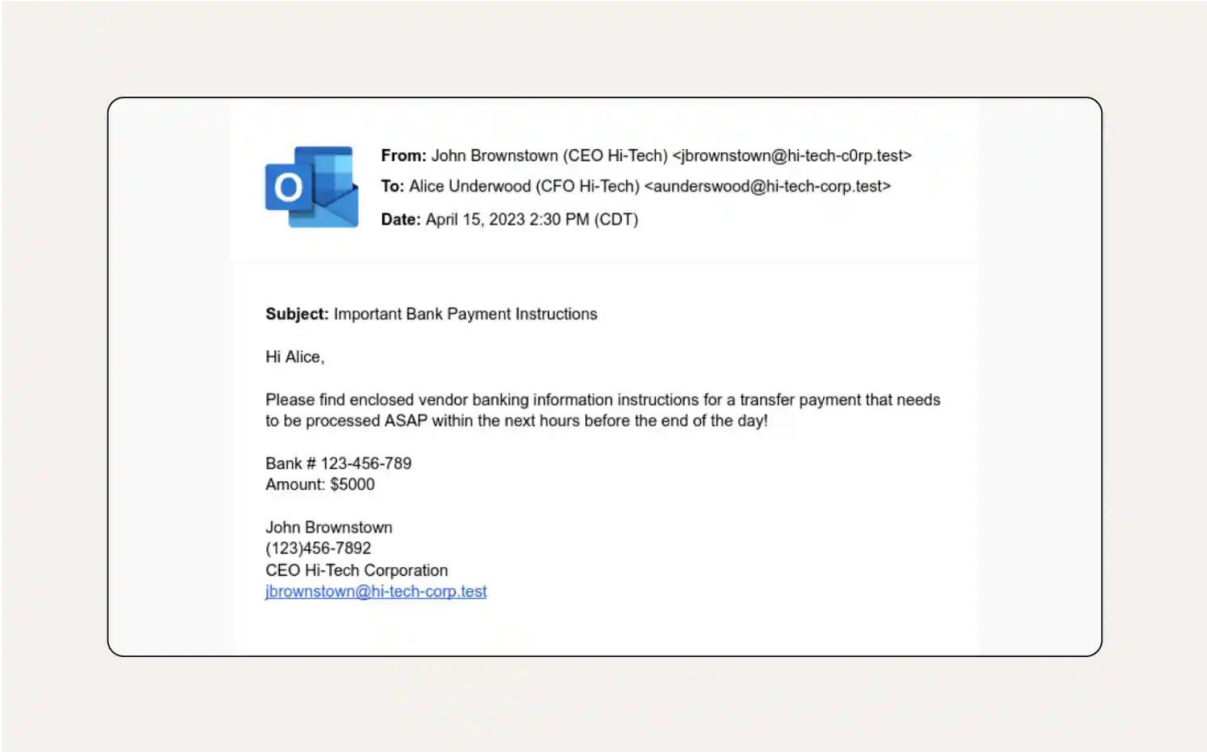
TASK 2

1.Obtain a sample phishing email



From: John Brownstown (CEO Hi-Tech) <jbrownstown@hi-tech-c0rp.test>
To: Alice Underwood (CFO Hi-Tech) <aunderswood@hi-tech-corp.test>
Date: April 15, 2023 2:30 PM (CDT)

Subject: Important Bank Payment Instructions

Hi Alice,

Please find enclosed vendor banking information instructions for a transfer payment that needs to be processed ASAP within the next hours before the end of the day!

Bank # 123-456-789
Amount: $5000

John Brownstown
(123)456-7892
CEO Hi-Tech Corporation
jbrownstown@hi-tech-corp.test

2. Examine sender's email address for spoofing

Element	Problem Detected
Domain name	hi-tech-c0rp.test instead of the likely legitimate domain hi-tech-corp.com. This uses a typo squatted domain: the letter "o" is replaced with a zero ("0") in "crop".
Top-level domain (.test)	.test is not used for real organizations. It’s a reserved domain used for testing, which makes it a red flag—legit companies don't send

	business emails from .test domains.
Display name spoofing	"John Brownstown (CEO Hi-Tech)" looks real, but this can be easily faked to trick users. The actual sender domain is what matters, not the display name.
No digital signature (DKIM/SPF/DMARC)	While not shown here, spoofing often bypasses authentication checks like SPF, DKIM, and DMARC if these are not enforced by the real domain.

3.Check email headers for discrepancies (using online header analyser)

Summary
From: John Brownstown <jbrownstown@hi-tech-c0rp.test>
Reply to: <fakepayments@protonmail.com>
Received
Hop: 1
From: unknownserver123.biz ([185.33.44.101])
Percent: 0
Other
<johnbrown@examplemail.ru>
FAIL (sender IP not authorized)
FAIL
FAIL

Header Field	What to Check
Return-Path:	Should match the **From** address. If different, this is a red flag.
Received: lines	Trace the path of the email. Look for **suspicious IPs**, servers, or geolocations.
From:	Display name may say “CEO,” but domain may be spoofed.
Reply-To:	Often set to a different, malicious address.
SPF:	Look for SPF: FAIL – means sender IP is not authorized.
DKIM:	Look for DKIM: FAIL – signature doesn’t match domain.
DMARC:	Look for DMARC: FAIL – domain policy not satisfied.
Message-ID:	If domain here doesn’t match sender’s domain, it’s suspicious.

4.Identify suspicious links or attachments. If this phishing email **did** contain links or files, here's how to spot them:

🔗 **Suspicious Links**

- **Mismatch in display vs actual link**:
  Click here to verify: [secure.hi-tech-corp.com] → Actually links to malicious-site.ru/payme.html

- **Obfuscated URLs** using link shorteners:
  e.g., bit.ly/3Gh9Xpay
- **Spoofed login pages**: e.g., a fake Microsoft 365 login

📎 **Suspicious Attachments**

- Files like:
  - Invoice.pdf.exe (double extension)
  - payment_instructions.docm (macro-enabled Word file)
  - banking_info.zip (compressed malware)
- Attachments with **urgent labels**: URGENT_TRANSFER.pdf

5.Look for urgent or threatening language in the email body.

Phrase	**Why It's a Red Flag**
" needs to be processed ASAP"	Creates a sense of urgency to make the recipient act without verifying.
" within the next hours"	Artificial time pressure — often used in phishing to bypass normal company protocols.
" before the end of the day"	Encourages rushing the task, which leads to mistakes.
No allowance for questions or verification	This is a classic manipulation technique to **cut out second opinions**.

6.Note any mismatched URLs (hover to see real link).

- **Misspelled domains** (hi-tec-corp.com, hi-tech-c0rp.com)
- **Unfamiliar top-level domains** like .ru, .tk, .xyz
- **IP addresses or URL shorteners** (bit.ly, tinyurl, etc.)

7.Verify presence of spelling or grammar errors.

Sentence or Phrase	**Issue**	**Suggested Correction**
“Please find enclosed vendor banking information instructions…”	**Awkward/unnatural phrasing**	"Please find the enclosed vendor banking instructions..."
“within the next hours before the end of the day”	**Grammatically incorrect / incomplete**	"within the next few hours before the end of the day"
Repetition: “completed” used twice in two sentences	**Poor writing style**	Rephrase one of the sentences to avoid redundancy.

8.Summarize phishing traits found in the email.

This email is a clear **attempt at Business Email Compromise (BEC)** using:

- CEO impersonation
- Domain spoofing
- Psychological manipulation (urgency + authority)

If received in a real environment, it should be:

1. **Reported to IT/security** immediately.
2. **Flagged and blocked** at the email gateway.
3. Used as part of **security awareness training**.