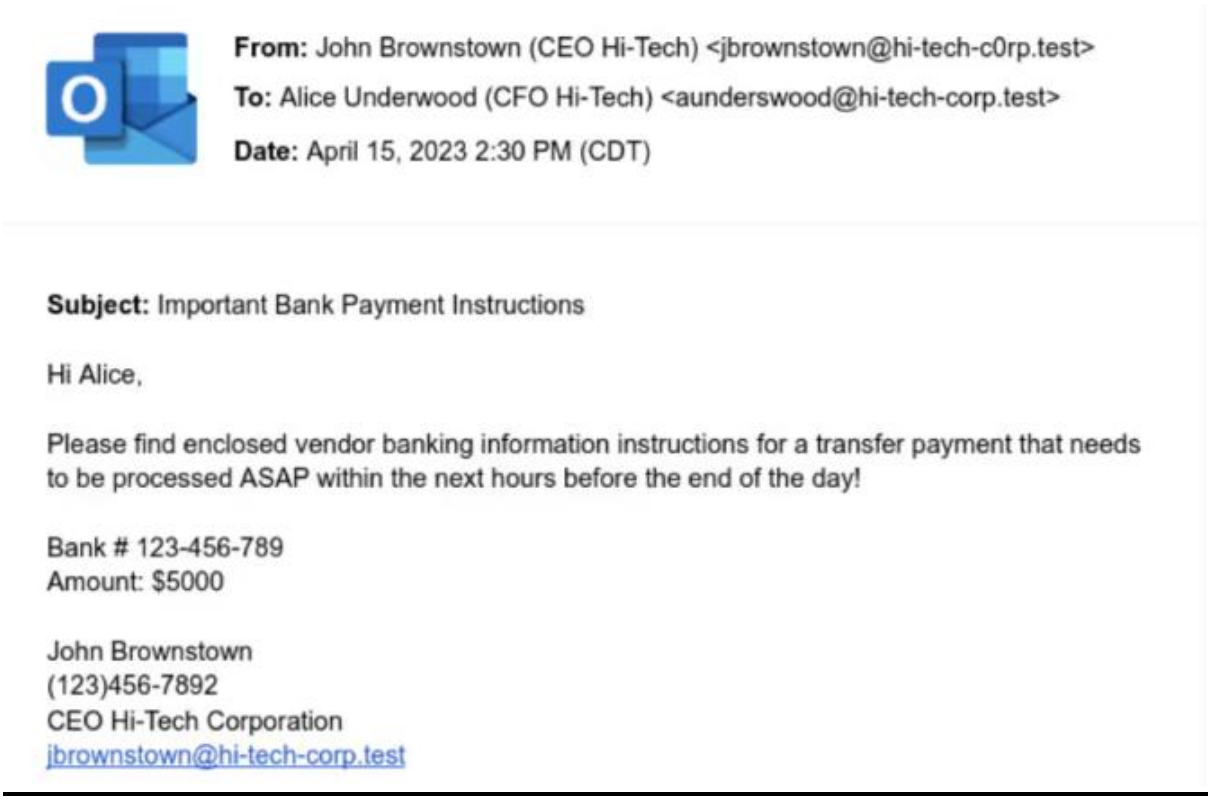
1. A sample phishing email



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!

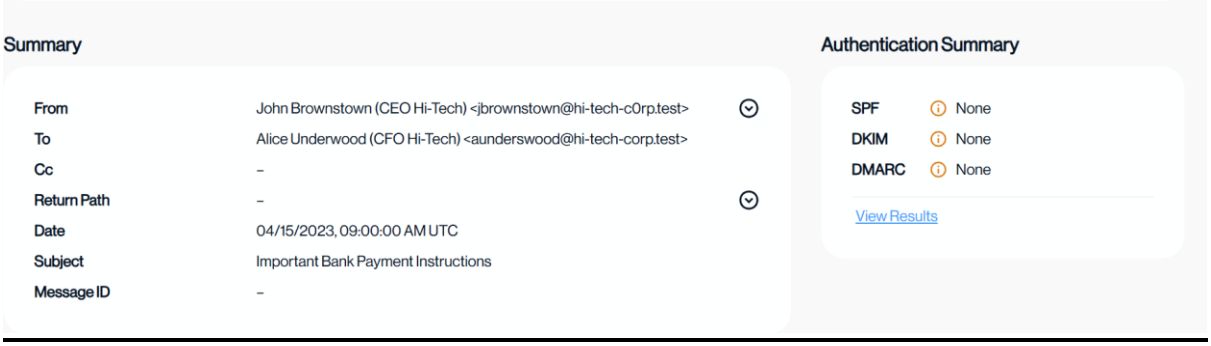
Bank # 123-456-789
Amount: $5000

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

2. Examining sender's email address for spoofing-

Sender using 0 in c0rp.test instead of corp.test to look legimitate to receiver and wanted to look to receiver as it came from a trusted source.

3. Checking email headers for discrepancies



Summary

From	John Brownstown (CEO Hi-Tech) <jbrownstown@hi-tech-c0rp.test>
To	Alice Underwood (CFO Hi-Tech) <aunderswood@hi-tech-corp.test>
Cc	-
Return Path	-
Date	04/15/2023, 09:00:00 AM UTC
Subject	Important Bank Payment Instructions
Message ID	-

Authentication Summary

SPF	None
DKIM	None
DMARC	None

View Results

4. Looking for urgent or threatening language in email

Sender threatening that information must be verified asap in next few hours so user easily give information without thinking too much because he is trying to create urgency.

"ASAP within the next hours before the end of the day!"

Classic urgency tactic to bypass rational scrutiny.

5. Presence of Spelling mistake or grammar errors.

Slightly awkward phrasing: "instructions for a transfer payment that needs to be processed ASAP within the next hours…"

- Subtle red flag

6. Summary phishing traits found in the email.

- Spoofed domain (c0rp.test)
- Urgent language
- Role impersonation (CEO to CFO)
- Financial request without proper protocol
- Signature mismatch (email domain vs displayed domain)