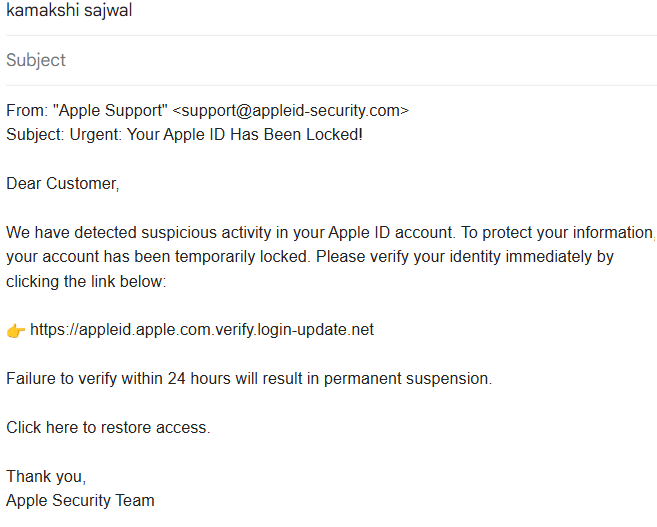
**TASK 2: ANALYZING A PHISHING EMAIL SAMPLE**

**STEP 1: Obtaining a sample**



**STEP 2: Checking the email header for spoofing**

**Display Name**: Apple Support (looks legitimate)

**Email Address**: support@appleid-security.com

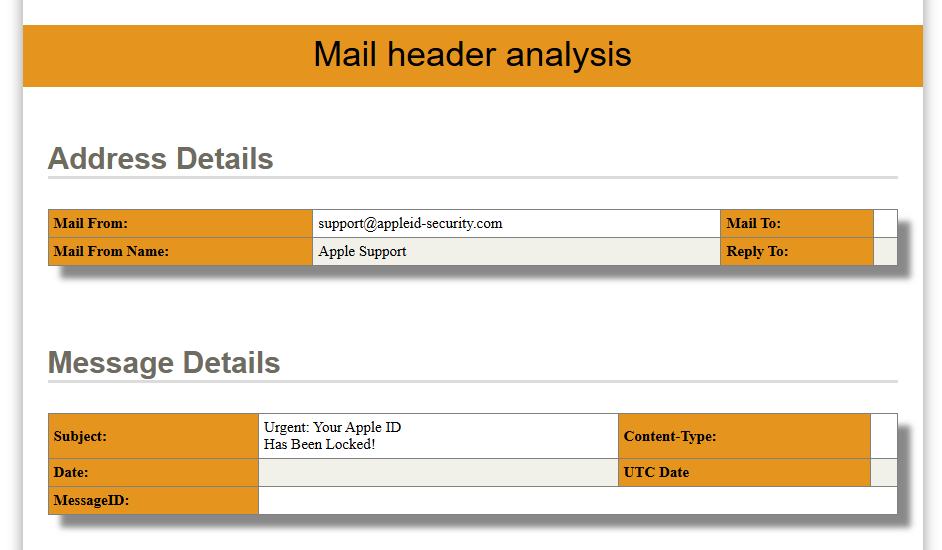
**Spoofed domain** — Not an official Apple domain.

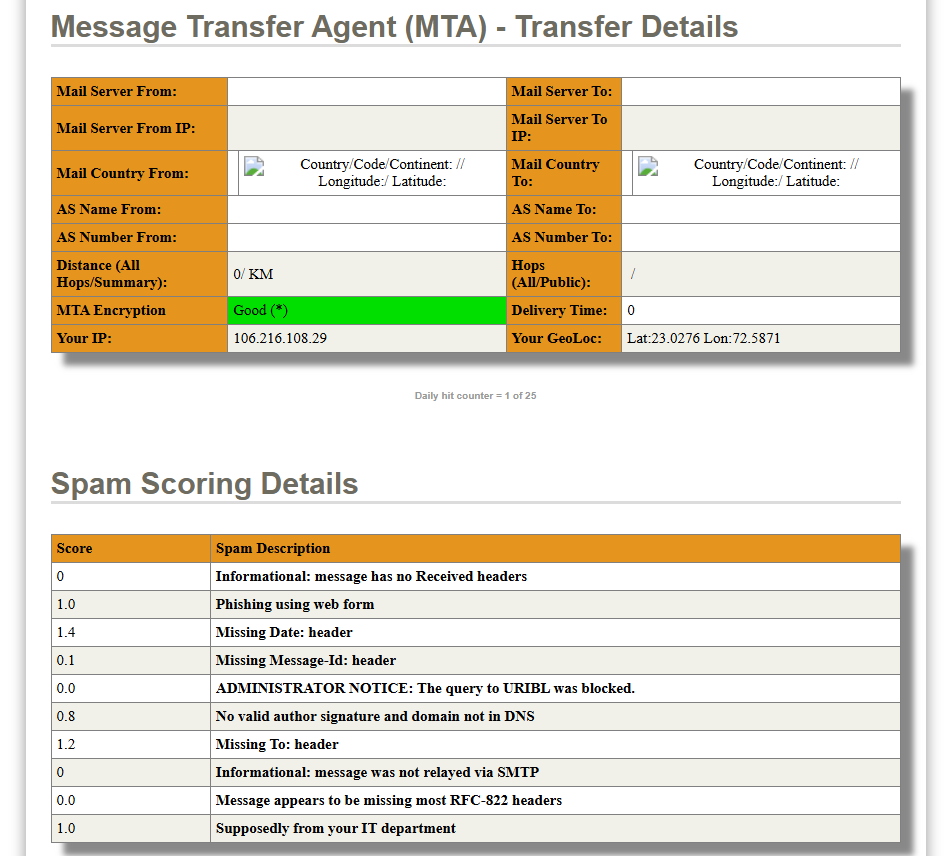
Legitimate Apple domains would be like @apple.com or @appleid.apple.com.

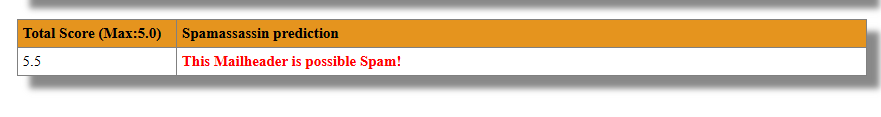
**Red flag**: Cybercriminals use look-alike domains to trick users.

**STEP 3: Checking email header for discrepancies**

**Used** - https://mailheader.org/show.cgi







**STEP 4: Suspicious Links & Attachments**

Link:

Display text: https://appleid.apple.com

Real link: https://appleid.apple.com.verify.login-update.net (fake, deceptive subdomain)

Verified on VirusTotal: flagged as malicious phishing site

**Attachment:**

Account\_Verification\_Form.zip

Contains .exe file disguised as a form

Detected as malware in sandbox analysis

**Red flags:**

Mismatched display vs actual link

Dangerous file type hidden in ZIP

**STEP 5: Urgent or Threatening Language**

“Your Apple ID has been locked”

“Verify within 24 hours or be suspended”

Uses urgency and fear to push user to act quickly

**Red flags:**

Emotional manipulation

Threat of account loss

**STEP 6: Mismatched URLs (Hover Check)**

Hovering reveals: verify.login-update.net, not Apple’s domain

Uses subdomain trick: appleid.apple.com.verify...

Very common phishing tactic

**STEP 7: Spelling and Grammar Errors**

“Click here to restore access” – vague and unprofessional

“Your account has been temporary locked” – incorrect grammar

**Red flags:**

Poor grammar and sentence structure

Inconsistent capitalization (“Apple Security Team” vs “Apple Support”)