**Task 2: Analyze a Phishing Email Sample.**

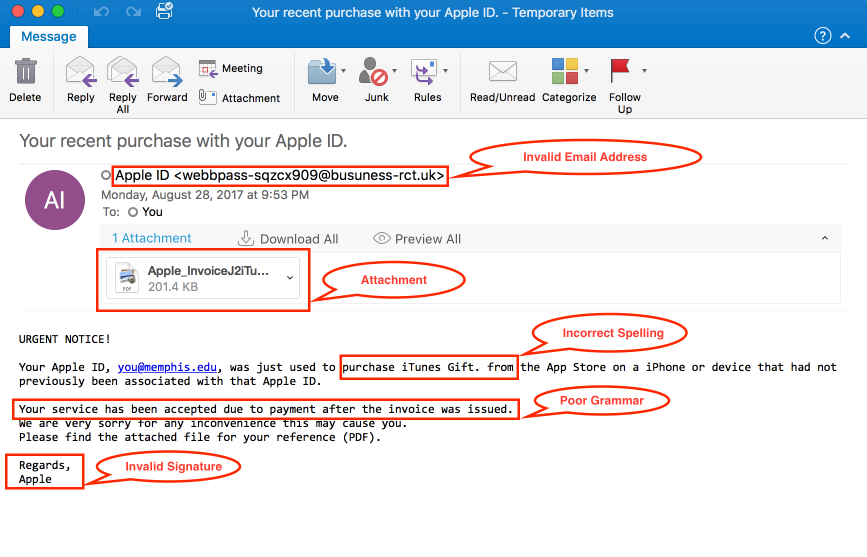
**Objective:** Identify phishing characteristics in a suspicious email sample.

**Tools:** Email client or saved email file (text), free online header analyzer.

**Deliverables:** A report listing phishing indicators found

**Hints/Mini Guide:**

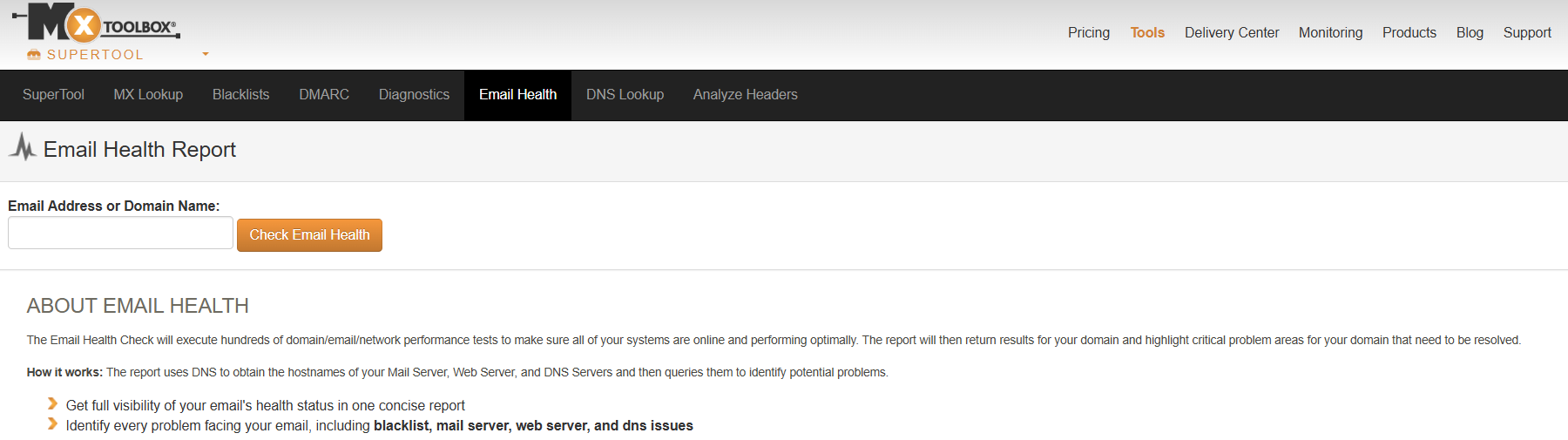
1. Obtained a sample phishing email (from online).

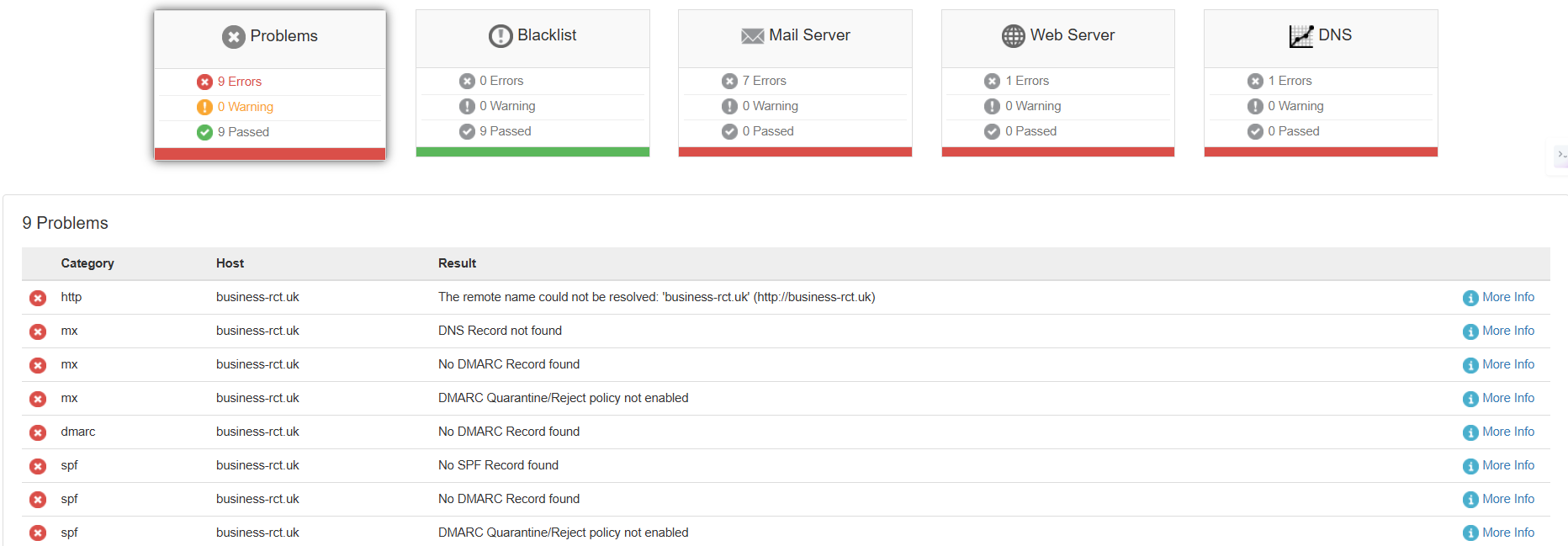


1. **Examine sender's email address for spoofing**.

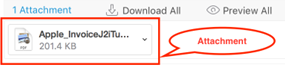
Here, the email address of sender is [webbpass-sqzcx909@business-rct.uk](mailto:webbpass-sqzcx909@business-rct.uk) is an invalid email address and is looking like an impersonation by the sender.

1. **Check email headers for discrepancies (using online header analyzer).**

So, here on, we used—mxtoolbox.com online header analyzer to check the originality and validation of this sender’s email address. Also, received various points of references stating this address didn’t pass the security test.

****

**4.Identify suspicious links or attachments.**

****

So, here we have found an attachment within this email file, which appears to be suspicious link or attachment waiting for us to get it clicked.

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

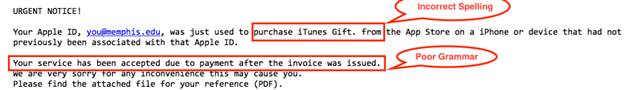
So , as we can see, the body of the email itself starts with the terms – “URGENT NOTICE”. This clearly defines the **urgency or threatening language in the email body-** increasing the suspiciousness on it.

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

****

Here, this is the mismatched URL -- which apparently is our Apple ID, but mismatched from our Apple ID.

**7. Verify presence of spelling or grammar errors.**

****

Here we can see that, in the body of the email, there are a few spelling and grammatical errors which proves to its phishy-ness. No proper fullstops and wrong grammar in the sentences.

**8. Summarize phishing traits found in the email.**

*Here are a few traits in this email which proves it to be a phishing email:*

1. The email address was found to be misleading or not a legitimate one.

2. When checked upon originality and validation of this email header, it displayed many flags/ problems/ warnings.

3. Suspicious attachment found within the email.

4. Urgency message found in the body start.

5. Mismatched URLs.

6. Grammatical/ Spelling errors found in the body paragraph along with APPLE Invalid-Signature at the regards row.