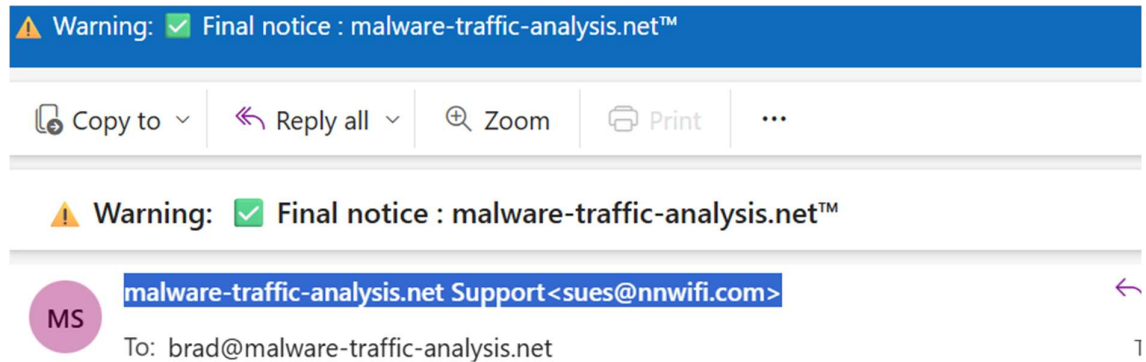


TASK -2

PHISING EMAIL

1. Using a phishing email and opening it in my outlook




Dear brad

To continue using your address confirm your ownership,

Confirm ownership

admin@malware-traffic-analysis.net setup team.

2. Analysing the email header using the tool

 Email Header Analyzer

Paste Header:
malware-traffic-analysis.net Support<sues@nnwifi.com>

[SuperTool](#) [MX Lookup](#) [Blacklists](#) [DMARC](#) [Diagnostics](#) [Email Health](#) [DNS Lookup](#) **Analyze Headers**

Header Analyzed
Email Subject:

Delivery Information

Relay Information

Received Delay:	0 seconds
-----------------	-----------

SPF and DKIM Information

Headers Found

Received Header

malware-traffic-analysis.net Support:sues@nnwifi.com

[Permanently forget this email header](#)

✓ Header Analysis (MxToolbox Summary)

- Sender Address: malware-traffic-analysis.net Support <sues@nnwifi.com>
- SPF/DKIM: Missing → Fails basic email authentication
- Delivery Time: 0s → Suggests spoofing or header tampering
- Sending Domain: nnwifi.com (not associated with target brand)
- Conclusion: Sender spoofed their identity; the message lacks authentication, indicating high risk of phishing.

Conclusion

This email is a clear **phishing attempt**. It fails email authentication, uses urgency and spoofing tactics, and includes a malicious link.

Actions Taken

- Analysed headers using [MxToolbox](#)
- Documented phishing indicators in email content

Recommendations

- Never click links in suspicious emails
- Always verify the sender's domain
- Report phishing attempts to IT/security teams
- Use header analysis tools to detect spoofed emails