Phishing Email Detection & Awareness System

Cyber Security Internship – Task 2 (2026)

Prepared by: Dhanush Kumar
Internship Program: Future Interns – Cyber Security
Task Type: Security Awareness & Email Threat Analysis
Submission: Task 2 – Phishing Detection & Awareness Report
Date: January 2026

Executive Summary

Phishing is one of the most common social engineering attacks used by cybercriminals to trick users into revealing sensitive information such as passwords, OTPs, and financial details. These attacks rely on deception rather than technical exploitation, making employees and end users the primary targets.

This report presents a phishing email analysis and awareness assessment conducted as part of the Future Interns Cyber Security Internship Program. The objective is to identify phishing indicators in suspicious emails and provide clear guidance to help users recognize and avoid such attacks.

Scope & Methodology

Scope

- *Analysis of phishing email samples*
- *Email header inspection*
- *Sender domain and link analysis*
- *User awareness and prevention focus*

Methodology

- *Collected phishing email samples*
- *Inspected email content for phishing indicators*
- *Analyzed email headers using online tools*
- *Classified email risk levels*
- *Created user-focused awareness guidelines*

Phishing Email Analysis

Email 1 Analysis – Account Verification Scam

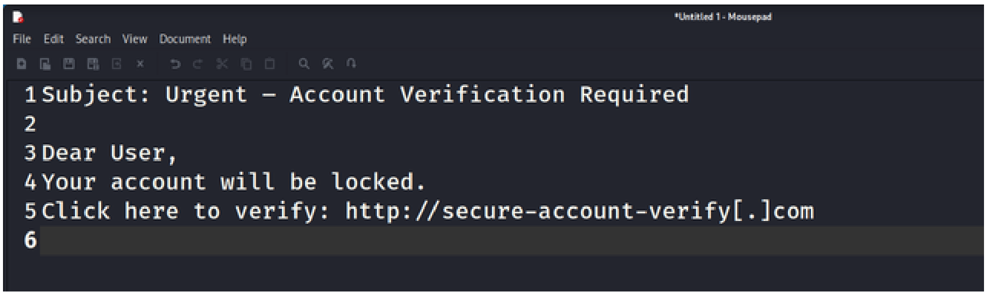
Description:

This email impersonates a security team and creates urgency by claiming suspicious activity on the user’s account.

Phishing Indicators Identified:

- *Suspicious sender domain*
- *Urgent and fear-based language*
- *Fake verification link*
- *Generic greeting*
- *Threat of account suspension*

Risk Classification: Phishing



```
Subject: Urgent – Account Verification Required

Dear User,
Your account will be locked.
Click here to verify: http://secure-account-verify[.]com

```

Caption:

Figure 1: Phishing email requesting urgent account verification

Subject: Urgent – Verify Your Account Immediately

Sender: security@secure-check-support.com

Email Body:
Dear User,

We detected unusual activity on your account.
To avoid temporary suspension, please verify your account immediately.

Click here to verify:
http://secure-account-check[.]com

Failure to act within 24 hours may result in account lock.

Regards,
Security Team

Email 2 Analysis – Fake Invoice Scam

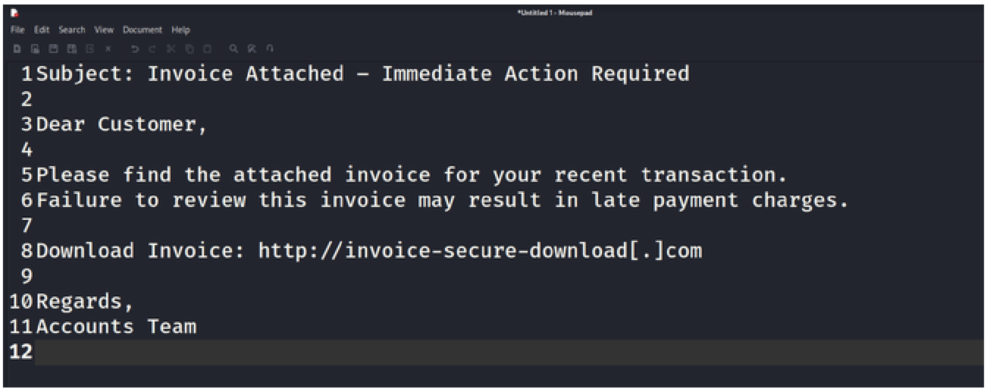
Description:

This email pretends to be a billing department and attempts to trick users into downloading a malicious attachment.

Phishing Indicators Identified:

- *Unknown sender domain*
- *Unexpected payment failure message*
- *Malicious attachment lure*
- *Generic greeting*

Risk Classification: Phishing



```
Subject: Invoice Attached – Immediate Action Required

Dear Customer,

Please find the attached invoice for your recent transaction.
Failure to review this invoice may result in late payment charges.

Download Invoice: http://invoice-secure-download[.]com

Regards,
Accounts Team
```

Caption:

Figure 2: Phishing email using fake invoice attachment

Subject: Invoice Payment Failed

Sender: billing@finance-support.net

Email Body:
Hello,

Your recent invoice payment has failed. Please download the attached document to retry the payment.

Regards,
Finance Department

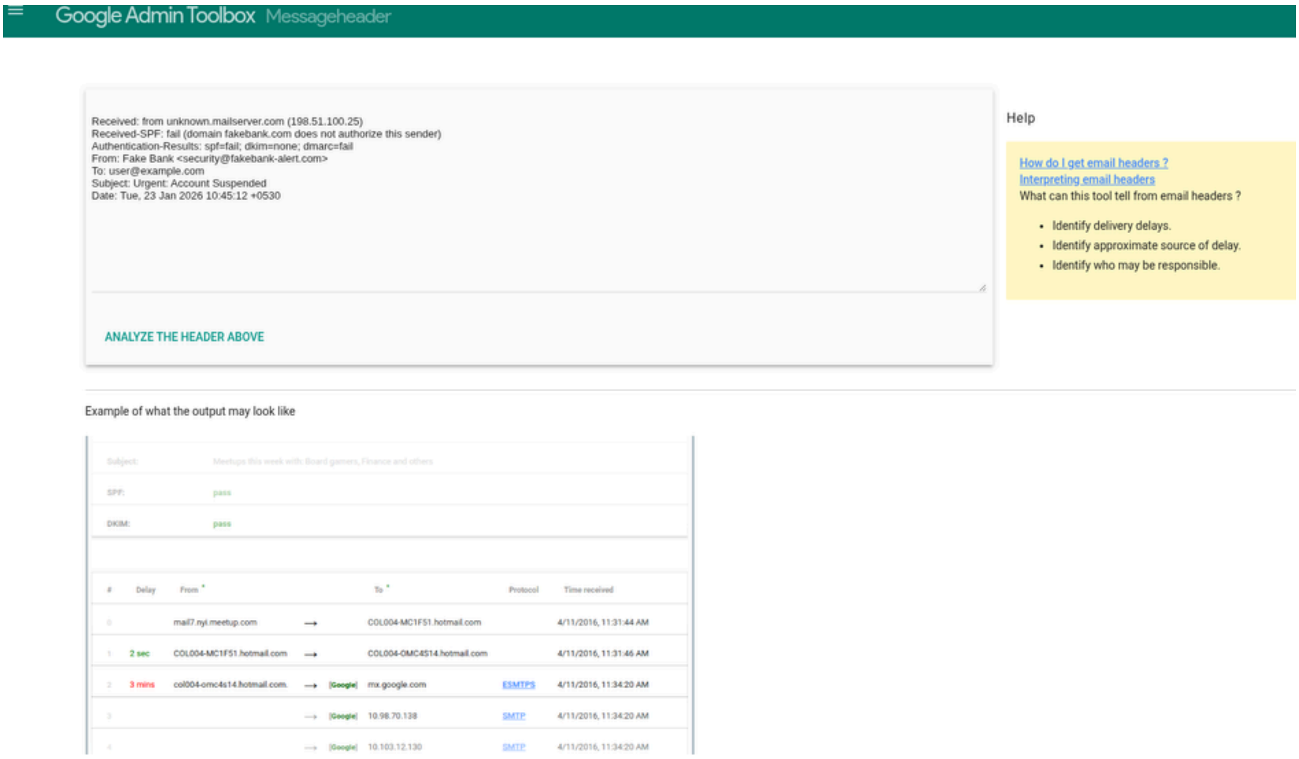
Email Header & Link Analysis

Header Analysis Findings:

- *Sender domain mismatch*
- *No proper authentication (SPF/DKIM issues)*
- *Suspicious routing paths*

Link Analysis Findings:

- *Fake domains resembling legitimate services*
- *Non-secure HTTP links*
- *Redirection to untrusted domains*



```
Received: from unknown.mailserver.com (198.51.100.25)
Received-SPF: fail (domain fakebank.com does not authorize this sender)
Authentication-Results: spf=fail; dkim=none; dmarc=fail
From: Fake Bank <security@fakebank-alert.com>
To: user@example.com
Subject: Urgent: Account Suspended
Date: Tue, 23 Jan 2026 10:45:12 +0530
```

Help

[How do I get email headers ?](#)
[Interpreting email headers](#)
What can this tool tell from email headers ?

- Identify delivery delays.
- Identify approximate source of delay.
- Identify who may be responsible.

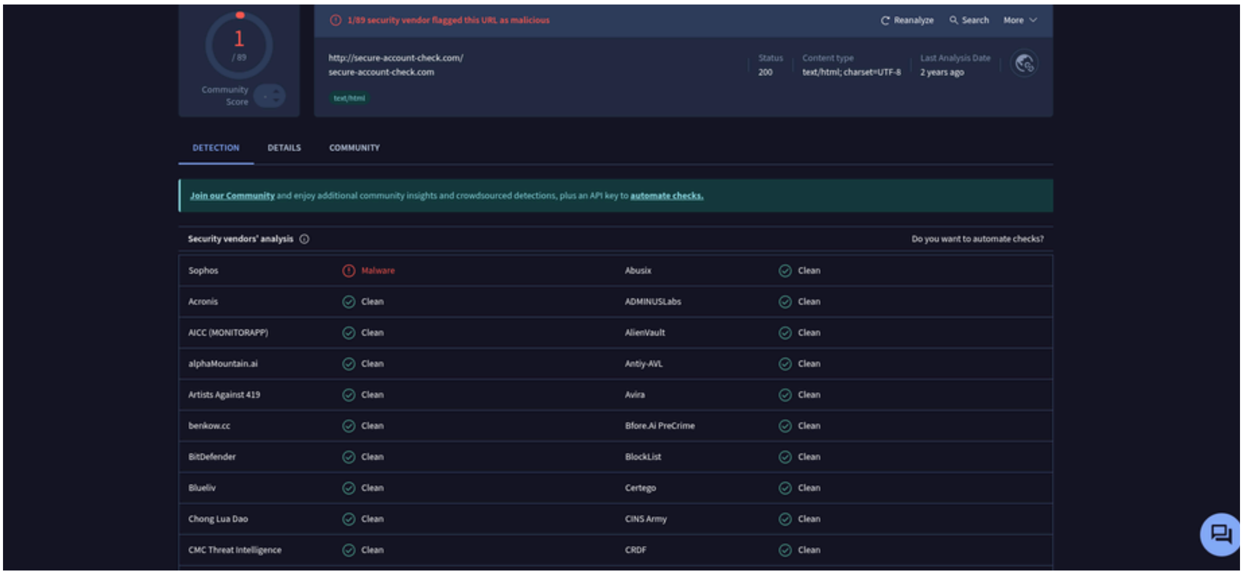
Example of what the output may look like

Subject:	Meetups this week with: Board gamers, Finance and others
SPF:	pass
DKIM:	pass

#	Delay	From *			To *	Protocol	Time received
0		mail7.nyi.meetup.com	→		COL004-MC1F51.hotmail.com		4/11/2016, 11:31:44 AM
1	2 sec	COL004-MC1F51.hotmail.com	→		COL004-OMC4S14.hotmail.com		4/11/2016, 11:31:46 AM
2	3 mins	col004-omc4s14.hotmail.com	→	[Google]	mx.google.com	ESMTPS	4/11/2016, 11:34:20 AM
3			→	[Google]	10.98.70.138	SMTP	4/11/2016, 11:34:20 AM
4			→	[Google]	10.103.12.130	SMTP	4/11/2016, 11:34:20 AM

Caption:

Figure 3: Email header analysis showing spoofed sender details



1/89 security vendor flagged this URL as malicious

http://secure-account-check.com/
secure-account-check.com

text/html

Status
200

Content type
text/html; charset=UTF-8

Last Analysis Date
2 years ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Sophos	Malware	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AICC (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CMC Threat Intelligence	✓ Clean	CRDF	✓ Clean

Caption:

Figure 4: Malicious link inspection showing suspicious domain

Common Phishing Techniques Observed

- *Impersonation of trusted organizations*
- *Urgency and fear tactics*
- *Malicious links and attachments*
- *Generic greetings*
- *Fake sender domains*

Prevention & Awareness Guidelines

DO’s

- *Verify sender email addresses carefully*
- *Hover over links before clicking*
- *Report suspicious emails to IT/security teams*
- *Use strong and unique passwords*

DON’Ts

- *Do not click unknown or suspicious links*
- *Do not download unexpected attachments*
- *Do not share passwords, OTPs, or personal details*
- *Do not trust fear-based messages*

Conclusion

Phishing attacks exploit human trust rather than system vulnerabilities. By improving user awareness and educating employees about common phishing techniques, organizations can significantly reduce the risk of successful attacks. Security awareness is a critical layer of defense in modern cyber security strategies.

Disclaimer

This report was created for educational purposes as part of the Future Interns Cyber Security Internship Program. All email samples analyzed are simulated examples, and no real users or organizations were affected.