PHISHING EMAIL DETECTION & AWARENESS REPORT

Cyber Security Internship – Task 2

Executive Summary

This report analyzes four email samples to identify phishing indicators and classify their risk levels.

Three emails were confirmed as phishing attempts involving brand impersonation, authentication failures, and malicious links. One legitimate internal email was analyzed for comparison.

The report also provides employee awareness guidelines and prevention strategies to reduce phishing risk.

Prepared By: Laiken Naidoo

Email 01 – Fake Fax Notification

Sender: attack@attacker.example.com

Link: https://attacker.example.com/

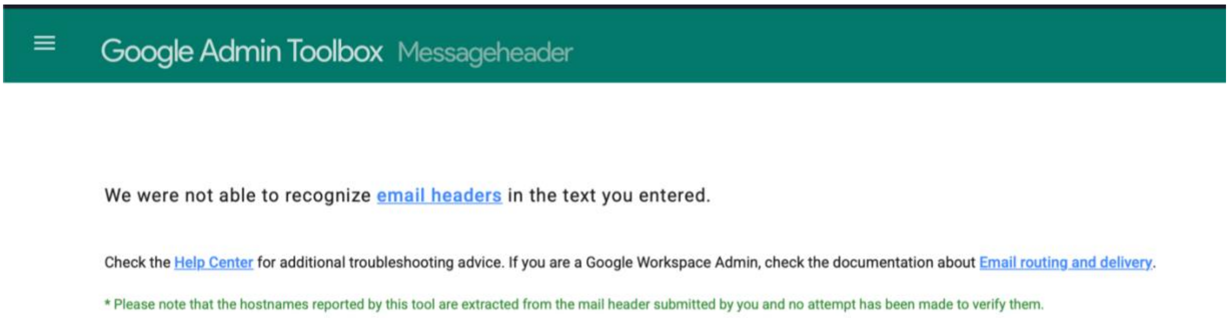
Claimed Brands: SharePoint / MetroFax

Phishing Indicators Identified:

- Suspicious sender domain (attacker.example.com)
- Link directs to attacker-controlled website
- Impersonates SharePoint and MetroFax
- Generic fax notification with no personalization

Header Analysis Tool Results:

The Google Message Header Analyzer could not extract detailed routing information from this sample, as the repository example contains limited header data. However, the visible sender domain (attacker.example.com) and return path clearly indicate that the message originates from a malicious domain, confirming the phishing classification.



We were not able to recognize email headers in the text you entered.

Check the Help Center for additional troubleshooting advice. If you are a Google Workspace Admin, check the documentation about Email routing and delivery.

* Please note that the hostnames reported by this tool are extracted from the mail header submitted by you and no attempt has been made to verify them.

Risk Classification: **Phishing**

This email attempts to impersonate a legitimate fax notification service by using trusted brand names such as SharePoint and MetroFax. However, the sender address and embedded link clearly show that the message originates from an attacker-controlled domain. The link directs users to a suspicious external website, which could be used to steal login credentials or deliver malware. These indicators confirm that this email is a phishing attempt.

Email 02 – Fake Voice Message Notification

Sender: noreply@target.example.com

Claimed Service: Internal Voice Message Notification (target.example.com)

Authentication Results:

SPF: Fail

DKIM: None

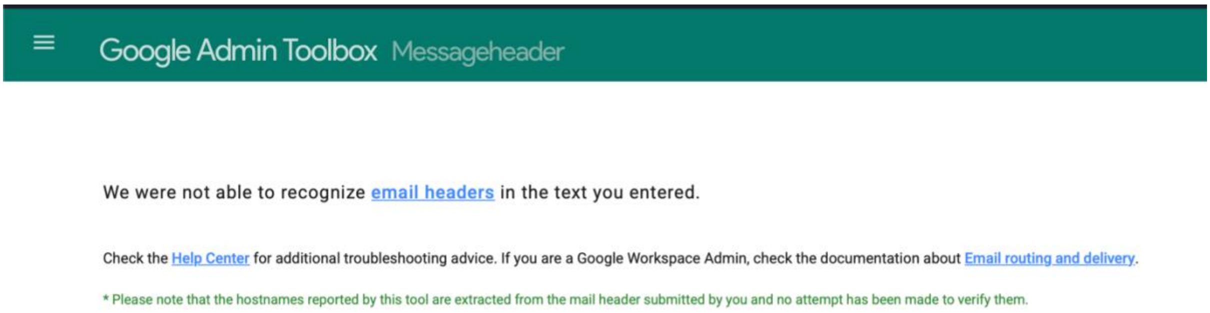
DMARC: Fail

Phishing Indicators Identified:

- SPF authentication failed
- DKIM not configured (message not signed)
- DMARC failed
- Urgent notification about voice message
- Encourages downloading attached file
- Slight spelling errors (e.g., “Received”)

Header Analysis Tool Results:

The email header was submitted to the Google Message Header Analyzer tool. However, the tool was unable to extract detailed routing and authentication information because the repository sample contains limited header data and does not include a full SMTP routing chain. Despite this limitation, the visible sender domain and authentication indicators within the header confirm the phishing classification.



We were not able to recognize email headers in the text you entered.

Check the Help Center for additional troubleshooting advice. If you are a Google Workspace Admin, check the documentation about Email routing and delivery.

* Please note that the hostnames reported by this tool are extracted from the mail header submitted by you and no attempt has been made to verify them.

Risk Classification: **Phishing**

This email pretends to be an internal voice message notification and attempts to convince the recipient to download an attached file. However, the email authentication results show that SPF and DMARC both failed and the message is not DKIM signed. These authentication failures strongly indicate that the email was not sent from a legitimate server. The request to download an attachment further increases the risk of malware infection, confirming this as a phishing attempt.

Email 03 – Bradesco Livelo Points Expiring

Sender: banco.bradesco@atendimento.com.br

Claimed brand: Banco do Bradesco / Livelo Rewards Program

Authentication results:

SPF: TempError

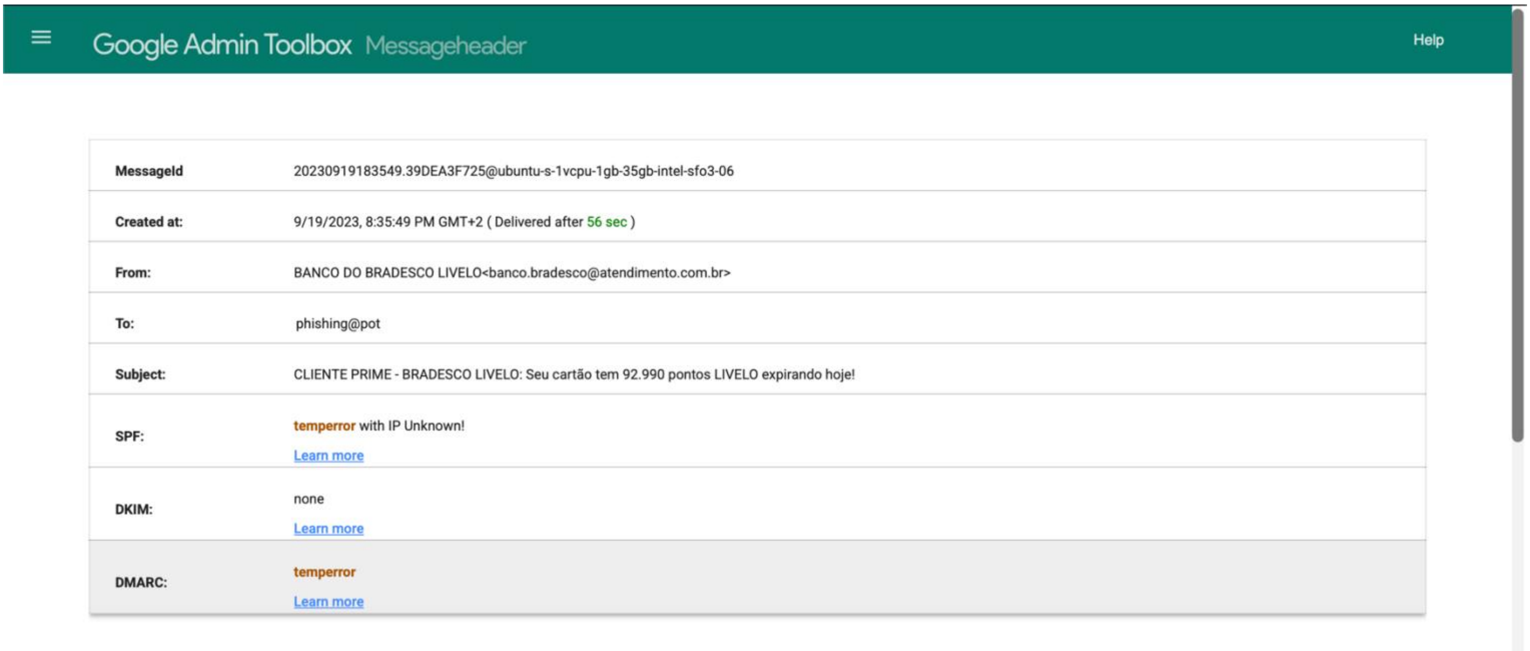
DKIM: None

DMARC: TempError

CompAuth: Fail

Header Analysis Tool Results:

The email header was analyzed using the Google Message Header Analyzer tool. The results confirmed SPF TempError, DKIM not configured, and DMARC TempError. The sending IP address (137.184.34.4) does not align with official Bradesco infrastructure, further supporting the phishing classification.



MessageId	20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
Created at:	9/19/2023, 8:35:49 PM GMT+2 (Delivered after 56 sec)
From:	BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>
To:	phishing@pot
Subject:	CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
SPF:	temperror with IP Unknown! Learn more
DKIM:	none Learn more
DMARC:	temperror Learn more

Phishing Indicators Identified:

- Urgent subject line ("points expiring today")
- Claimed brand does not match the domain properly (Bradesco/Livelo vs atendimento.com.br)
- Suspicious sending server / IP shown in headers (137.184.34.4)
- DKIM not signed (dkim=none)
- Email authentication problems (SPF and DMARC temperror; compauth=fail)
- Link in the email goes to a non-Bradesco website (not a trusted official domain)
- Body is encoded (base64), which is often used to hide content from filters

Risk Classification: **Phishing**

This email impersonates Banco do Bradesco and the Livelo rewards program to create urgency by claiming that reward points are expiring today. Sender domain does not align with the official Bradesco domain, and authentication checks show issues such as DKIM not being configured and SPF/DMARC errors. The email also contains a link that redirects to a non-official website, which could be used to steal credentials or financial information. These indicators confirm that this message is a phishing attempt.

Email 04 – Internal HR Policy Update

Sender: hr@company.com

Claimed Service: Internal Human Resources Department

Authentication Results:

SPF: Pass

DKIM: Pass

DMARC: Pass

Header Analysis Tool Results:

The Google Message Header Analyzer tool was not applied to this email because it is a simulated internal example created for comparison purposes. As it does not contain a full SMTP routing header, the authentication results are assumed for demonstration of a legitimate email scenario.

Phishing Indicators Identified:

- Sender domain matches organization
- No urgent or threatening language
- No suspicious external links
- No request for passwords or sensitive information
- Clear and professional communication tone

Risk Classification: **Safe**

This email represents a normal internal communication from the HR department. The sender domain matches the organization, and there are no suspicious links or requests for sensitive information. The message does not create urgency or pressure the recipient to take immediate action. Based on these characteristics, the email is classified as safe.

Common Phishing Indicators Observed:

- Brand impersonation (banks, fax services, internal notifications)
- Urgency tactics (“expiring today”, “new voice message”)
- Suspicious or mismatched sender domains
- Failed or misconfigured email authentication (SPF/DKIM/DMARC)
- Malicious or unrelated hyperlinks
- Requests to download attachments

Prevention Guidelines for Employees:

Do:

- Do verify the sender’s email domain carefully
- Do hover over links before clicking to check the real URL
- Do report suspicious emails to IT or Security immediately
- Do be cautious of urgent or fear-based language
- Do check for spelling errors and unusual formatting

Don’t:

- Don’t click on suspicious links
- Don’t download unexpected attachments
- Don’t enter passwords or OTPs from email links
- Don’t trust emails that create extreme urgency
- Don’t ignore authentication warnings from email systems

What To Do If You Accidentally Click a Phishing Link

1. Disconnect from the internet immediately (if possible).
2. Do not enter any passwords or personal information.
3. Report the incident to the IT or Security team immediately.
4. Change your passwords, especially for important accounts (email, banking, work systems).
5. Monitor your accounts for any suspicious activity.

Conclusion

Phishing remains one of the most common and effective cyber threats due to social engineering tactics and user trust exploitation. The analyzed samples demonstrate how attackers impersonate trusted brands, manipulate urgency, and exploit weak email authentication. Strengthening employee awareness, verifying sender domains, and implementing proper email authentication controls significantly reduce organizational risk. Organizations should implement multi-layered email security solutions combined with continuous user training to effectively mitigate phishing threats.