Cybersecurity Internship – Task 2

Analyze a Phishing Email Sample

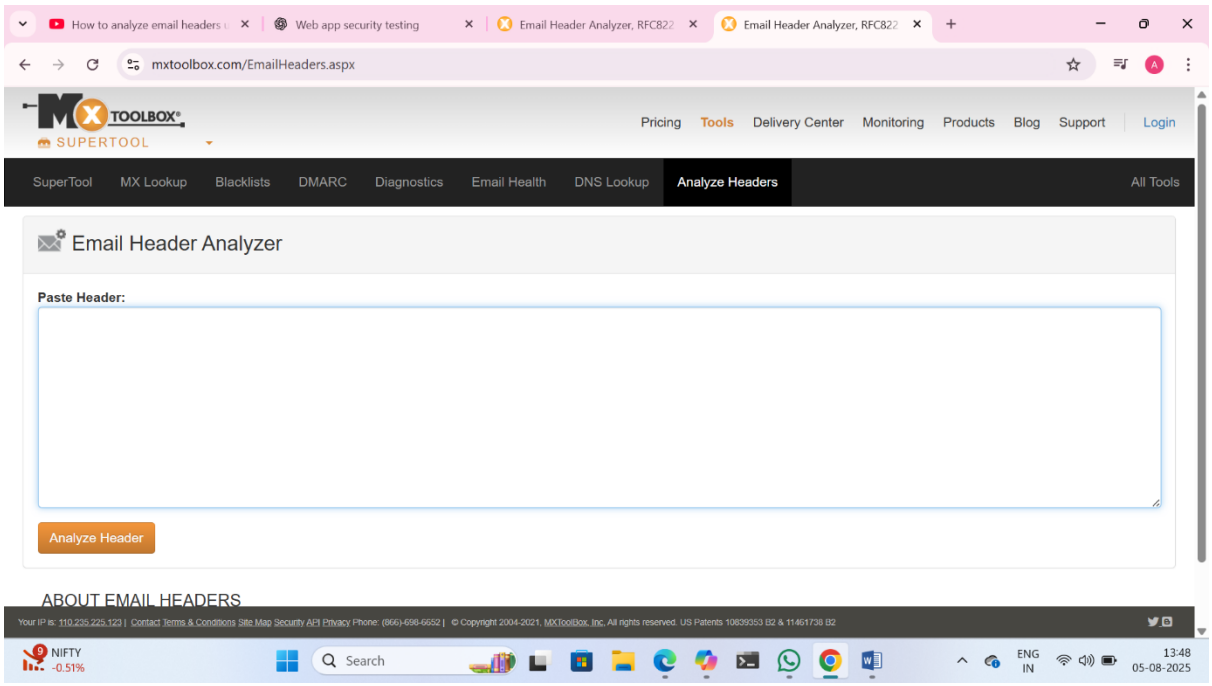
Objective: Identify phishing characteristics in a suspicious email sample.

Name : Bogi Arun

Date : 05/08/2025

Tools Used:

- MXToolbox Header Analyzer
- Email client
- Manual link and language inspection



Introduction

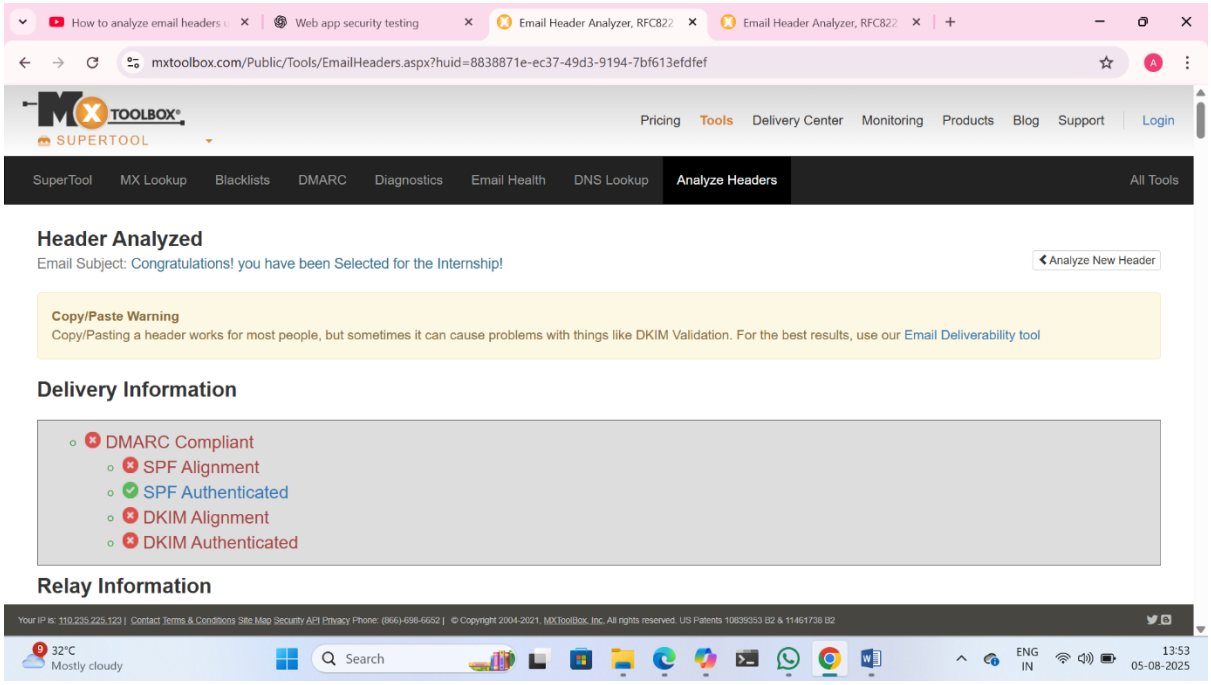
Phishing remains one of the most pervasive threats in the cybersecurity landscape, exploiting human psychology to compromise systems and steal sensitive information. This report presents a detailed analysis of a suspected phishing email, aiming to identify key indicators commonly associated with malicious intent. Through the examination of email headers, sender details, embedded links, attachments, and linguistic cues, this exercise demonstrates a methodical approach to detecting and understanding phishing tactics. The insights gained reinforce essential skills in threat analysis, email spoofing detection, and social engineering awareness critical competencies for cybersecurity professionals in safeguarding digital environments.

1. Obtain a Phishing Sample

- **Source**: Received via Gmail.
- **Subject**: “Congratulations! you have been Selected for the Internship!”
- **Sender shown**: contact@futureinterns.com
- **Reply-to**: internships.futureinterns@gmail.com
- **Verdict**: Suspicious — mismatch between sender and reply-to.

2. Check the Sender Address for Spoofing

- **Sender** claims to be futureinterns.com, but replies go to @gmail.com.
- **SPF Authenticated**: ✓ Yes
- **SPF Alignment**: ✗ Failed (domain mismatch)
- **DKIM Authenticated**: ✗ Not found
- **DMARC**: ✗ Failed
- **Verdict**: Likely spoofed — domain authentication failed or misaligned.



3. Analyze Email Headers (Using MXToolbox or Google Header Analyzer)

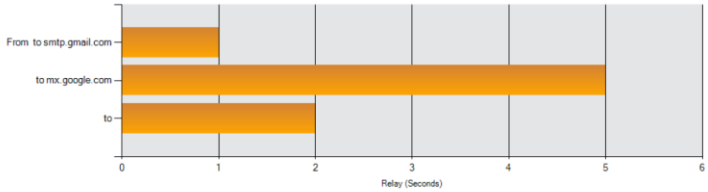
Header analysis results:

Protocol	Status	Notes
SPF	✓ Pass	Sent from an allowed IP
SPF Alignment	✗ Fail	Domain mismatch
DKIM	✗ Fail	No valid DKIM signature found
DMARC	✗ Fail	No strict policy set; failed overall check

- **Verdict**: Multiple technical failures confirm spoofing and impersonation.

Relay Information

Received Delay:	**5 seconds**



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	2405:201:d027:a007:a86d:111:13cc:41ec	smtp.gmail.com	ESMTPSA	8/4/2025 1:39:25 PM	✓
2	4 seconds	mail-sor-f41.google.com 209.85.220.41	mx.google.com	SMTPS	8/4/2025 1:39:29 PM	✓
3	1 Second		2002:a05:6402:3108:b0:615:e672:cc07	SMTP	8/4/2025 1:39:30 PM	

SPF and DKIM Information

dmarc:futureinterns.com

Hide | Solve Email Delivery Problems

```
v=DMARC1; p=none
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.

	Test	Result	
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

Reported by **ns1.dns-parking.com** on 8/5/2025 at **7:23:10 AM (UTC 0)**, just for you. Transcript

spf:gmail.com:209.85.220.41

Hide

```
v=spf1 redirect=_spf.google.com
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	redirect	_spf.google.com	Pass	The SPF record for Value replaces the current record.
	From Domain	futureinterns.com		The domain used in the From header field.

	Test	Result	
✗	SPF Alignment	Domain not found in SPF	More Info
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	SPF Record Published	SPF Record found	
✓	SPF Record Deprecated	No deprecated records found	
✓	SPF Multiple Records	Less than two records found	
✓	SPF Contains characters after ALL	No items after 'ALL'.	
✓	SPF Syntax Check	The record is valid	
✓	SPF Included Lookups	Number of included lookups is OK	
✓	SPF Recursive Loop	Nor Recursive Loops on Includes	
✓	SPF Duplicate Include	No Duplicate Includes Found	
✓	SPF Type PTR Check	No type PTR found	

Dkim Signature Error:
No DKIM-Signature header found - more info

Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info

4. Examine Links and Attachments

- **Links**:
  - Redirects to Canva (not a secure enterprise location).
  - Includes Telegram and LinkedIn — suspicious for formal internship offers.
- **Attachments**:
  - .pdf files are attached, often used in phishing to hide malware or fake documents.
- **Verdict**: Highly suspicious and potentially unsafe.

5. Identify Urgent or Manipulative Language

- Example: “Failure to share your Offer Letter on LinkedIn will result in termination.”
- Uses pressure and threats to rush the recipient.
- **Verdict**: Classic phishing manipulation tactic.

6. Spot Mismatched URLs

- Text shows “Future Interns” or “Offer Letter,” but:
  - Redirects to Canva design edit link
  - Domains don’t match organizational branding
- Hovering over links shows misleading destinations.
- **Verdict**: Mismatch confirms phishing intent.

7. Highlight Spelling and Grammar Errors

- Several capitalization and tone inconsistencies:
  - “Congratulations! you have been...” (inconsistent)
  - “Post Completion Updates” — vague, non-professional
  - Odd spacing in phrases
- **Verdict**: Poor language quality for a real company

8. Summary of Phishing Indicators

- Sender and reply-to mismatch (spoofing)
- SPF alignment, DKIM, and DMARC failures
- Threatening/urgent language to manipulate behavior
- Links redirect to Canva and Telegram, not official domains
- Unverified and unnecessary attachments
- Grammar and formatting inconsistencies
- Email uses free Gmail domain instead of corporate domain

Conclusion:

Phishing Email Confirmed

The analyzed email exhibits multiple strong indicators of phishing, including:

- Spoofed sender identity (mismatch between futureinterns.com and a Gmail reply-to address)
- Failed DMARC and DKIM checks, and SPF domain misalignment
- Urgent and manipulative language demanding public action (e.g., LinkedIn post)
- Suspicious links (e.g., Canva and Telegram instead of official websites)
- Inconsistent formatting and language errors
- Unverified attachments meant to appear official