Elevate Labs
Cybersecurity Internship Report

Task 2: Analyse a Phishing Email Sample

Submitted by: Namita Rana

Role: Cybersecurity Intern

Company: Elevate Labs

Internship Duration: 04 August 2025 – 18 September 2025

Date of Submission: 05 August 2025

Privacy & Ethical Use Notice

This report is intended strictly for academic, training, or internal cybersecurity awareness purposes. All information contained herein has been gathered and analysed ethically, with respect for privacy, data protection, and responsible disclosure practices.

The email sample analysed in this report was obtained lawfully and does not include any unauthorized or intrusive access to third-party systems or personal data. Personally identifiable information (PII), including names, email addresses, IP addresses, and other sensitive identifiers, has been redacted or anonymized where applicable to protect individual and organizational privacy.

This document is not to be used for malicious intent, reverse engineering of phishing techniques for harmful use, or the exploitation of identified vulnerabilities. Any reproduction, distribution, or public sharing of this report should be done with appropriate permissions and continued respect for the privacy of involved parties.

By using or referencing this report, readers agree to uphold ethical cybersecurity practices and ensure compliance with institutional, organizational, and legal guidelines.

Acknowledgement

I would like to express my sincere gratitude to **Elevate Labs** for their valuable guidance, encouragement, and support throughout the completion of this task and for providing the opportunity and resources necessary to carry out this task effectively.

My appreciation also goes to the online communities and open-source tools that support safe analysis and reporting of security incidents.

This phishing email analysis report was prepared as part of my cybersecurity learning journey, and it has significantly enhanced my understanding of real-world cyber threats, social engineering techniques, and the importance of email security awareness.

Lastly, I acknowledge the importance of ethical responsibility in handling suspicious emails and the sensitive nature of cybersecurity work. This task has deepened my commitment to responsible digital citizenship and professional integrity.

— Namita Rana

Table of Contents

Chapter 1: Executive Summary

1.1 Objective of the Report

The purpose of this report is to conduct a comprehensive technical and behavioural analysis of a suspicious job offer email suspected to be part of a phishing or scam campaign. The analysis was conducted as part of a real-world cybersecurity learning exercise aimed at improving threat identification, validation, and response reporting skills.

This report presents findings in a professional, structured format aligned with standard security analysis practices. It aims to educate users about how scammers exploit free platforms (like Gmail and Freelancer.com) and bypass traditional spam filters using personalized yet deceptive messages.

1.2 Overview of Tools and Methods

To assess the legitimacy of the email and uncover potential threats, the following tools and techniques were used:

- **Email Header Analysis** using tools like Google Admin Toolbox to extract routing paths, timestamps, and authentication (SPF, DKIM, DMARC) data.
- **WHOIS Lookup** to investigate the registration and ownership of the sending IP address and domain.
- **Manual Language & Tone Analysis** to identify signs of social engineering such as urgency, reward baiting, or impersonation.
- **Reverse DNS Resolution & IP Reputation Checks** to validate whether the sending IP address is owned by a reputable organization.
- **Link Hover & Verification** to check whether the email attempts redirection to unverified platforms (e.g., WhatsApp, external job sites).

Each tool helped verify a distinct component of the email's origin, technical legitimacy, or intent.

1.3 Original Email Sample

Below is the full content of the suspicious email that was analysed. This email is shown **strictly for cybersecurity awareness and education**.

From: Script Entry <scriptentryteam1@gmail.com>
To: [Multiple Recipients]
Date: July 29, 2025
Subject: We saw your profile and would like to invite you
Message Body:

Dear, Freelancer

Recently, our company has checked your profile on the Freelancer website. Your profile is exactly matching with the job offered in our company.

you drop Whatsapp message on our company Number With Screenshot Of Mail

If you're interested in collaborating on this project, please let us know your availability on WhatsApp. You can reach us at +91 XXXXX XXXXX We look forward to the possibility of working together to bring this project to successful completion.

Best regards,

Script Entry Team

Contact Number: +91 XXXXX XXXXX

Disclaimer: *The above email content is shown solely for academic and security training purposes. Information has been partially masked to prevent misuse.*

1.4 Summary of Key Findings

The analysis of the email revealed the following key observations:

- **SPF, DKIM, and DMARC Passed**: The email was genuinely sent through Gmail's authorized infrastructure (mail-sor-f41.google.com) using the IP address 209.85.220.41, a legitimate Google mail server.
- **Suspicious Use of Free Gmail Domain**: The sender used a generic Gmail account (scriptentryteam1@gmail.com) rather than a domain-matching business email, which is common in phishing campaigns.
- **Bulk Recipient Behaviour**: The email was sent to more than 18 recipients simultaneously—suggesting mass mailing with a generic message.
- **Unusual Call-to-Action**: The message encouraged users to bypass email by contacting a phone number on WhatsApp, a platform where phishing and scams are harder to trace.
- **No Organizational Identity or Verification**: The email lacked clear company credentials, digital signatures, or verification details—raising doubts about its authenticity.

1.5 Outcome and Conclusion

The email was technically authenticated, meaning it passed SPF, DKIM, and DMARC checks, and was relayed through valid Google infrastructure. However, technical legitimacy does not guarantee sender identity trustworthiness.

Upon behavioural and contextual analysis, the email shows strong indicators of a scam or phishing attempt:

- Mass-targeting approach,
- Free and unverifiable Gmail address,
- Redirect to WhatsApp with no vetting,
- No job details, no credentials, and no verification.

Therefore, the email is classified as a **social engineering-based scam or phishing attempt** designed to exploit trust and manipulate freelancers into off-platform interaction, potentially for fraudulent purposes.

Through this task, we gain deeper insight into:

- The importance of cross-verifying authenticated emails,
- How scammers leverage legitimate infrastructure,
- Why analysing sender behaviour is as critical as technical validation.

This exercise sharpens the ability to dissect phishing campaigns and educates on how to protect oneself and others from similar threats.

Chapter 2: Introduction

2.1 Background on Phishing

Phishing is a form of cybercrime that uses deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as usernames, passwords, banking details, or other personal data. It is one of the most prevalent and successful forms of social engineering, targeting users' trust and exploiting human behaviour rather than technical vulnerabilities.

These attacks often impersonate trusted organizations, such as banks, service providers, or government agencies, to lure recipients into clicking malicious links or downloading harmful attachments. Phishing emails can also serve as the entry point for more advanced attacks like ransomware deployment, identity theft, or unauthorized access to critical systems.

With the increasing sophistication of phishing techniques, including spear-phishing, business email compromise (BEC), and clone phishing, individuals and organizations alike must remain vigilant and proactive in identifying and reporting such threats.

2.2 Purpose and Scope of the Task

This task involves conducting a comprehensive analysis of a suspicious email, with the purpose of identifying and documenting the characteristics that qualify it as a phishing attempt. The analysis includes evaluating the technical structure of the email (headers, sender address, authentication), the content (tone, grammar, intent), and any embedded resources (links, attachments).

The scope of the report includes:

- Verification of the sender's identity and domain.
- Inspection of the email header for SPF, DKIM, and DMARC results.
- Evaluation of hyperlinks and file attachments.
- Analysis of the language and tone used in the message.
- Identification of phishing traits and formulation of key takeaways.

This task aligns with the broader goal of enhancing email security awareness and applying defensive cybersecurity techniques in real-world scenarios.

2.3 Importance of Email Threat Analysis

Email remains the most common vector for cyberattacks, with phishing accounting for over 90% of data breaches globally, according to numerous security reports. Despite advances in spam filters and email security gateways, attackers continually evolve their tactics to bypass automated detection mechanisms.

Therefore, the ability to manually analyse and interpret the indicators of phishing is an essential skill for students, IT professionals, and any digital user. Email threat analysis empowers individuals to:

- Recognize phishing attempts that may evade filters.
- Understand how attackers structure and deliver deceptive messages.
- Make informed decisions when handling suspicious communications.
- Contribute to collective organizational security through proper incident reporting.

This report demonstrates how a single email can be reverse-engineered to uncover a broader phishing campaign and highlights the need for layered defences and user training in cybersecurity best practices.

Chapter 3: Tools and Methodology

3.1 Tools Used

In this investigation, a combination of freely available, industry-trusted tools and manual inspection methods were used to conduct a comprehensive analysis of a suspicious email. The tools chosen enabled both technical dissection and behavioural assessment of the message, helping to identify signs of phishing or social engineering. Below is an overview of the tools utilized during the analysis:

3.1.1 Email Client

The email was accessed through a widely-used web-based email client that provides a "Show Original" or similar feature to view raw email headers. This feature was used to extract the full message header, which includes detailed metadata such as the sending IP address, authentication results (SPF, DKIM, DMARC), and routing paths.

3.1.2 Message Header Analyzer Tool

The extracted header was analysed using an online message header analyser tool. This tool provides a graphical timeline of the email's delivery path and verifies:

- **SPF (Sender Policy Framework):** Whether the sending IP was authorized by the domain.
- **DKIM (DomainKeys Identified Mail):** Whether the email content was signed and verified.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Whether the domain owner's policy was enforced correctly.
- **IP trace route and delivery delays:** Identifying the originating servers and detecting any unusual routing patterns.

3.1.3 WHOIS Lookup

The sending IP address was queried using public WHOIS lookup services. These tools revealed ownership and registration details of the IP, helping determine whether it belonged to a reputable organization. The findings confirmed that the IP was registered to a major cloud/email service provider, supporting the technical legitimacy of the sending server, while raising concerns about the sender's use of a free domain.

3.1.4 Manual Link Inspection and Behaviour Analysis

Although the email did not contain embedded hyperlinks or attachments, the body text requested contact via a third-party messaging app, a common redirection tactic used by scammers. The message was assessed manually for:

- Psychological manipulation (urgency, trust exploitation)
- Unverified contact methods (personal phone numbers instead of corporate emails)

- Absence of official links or company verification methods

This type of inspection is critical in identifying phishing attempts that rely on social engineering rather than malware.

3.1.5 VirusTotal and Other Online Scanners (not triggered in this case)

Although not required in this case (due to lack of file or URL attachments), VirusTotal and URLVoid were prepared to be used in case of:

- Suspicious URLs
- Attachments with high-risk file types (e.g., .exe, .zip, .html, .pdf)
- Embedded scripts or malware

These tools allow for safe scanning without executing potentially dangerous files.

3.2 Methodology and Step-by-Step Approach

A structured, investigative workflow was followed to ensure consistency and objectivity during analysis. The steps were:

Step 1: Header Extraction

- The full email header was accessed using the email client's built-in tool.
- The header was copied and analysed using an online message header tool.

Step 2: Sender and Domain Verification

- The “From” field was reviewed, and the sender’s domain was extracted.
- WHOIS queries were run on the originating IP to check ownership and hosting details.

Step 3: SPF, DKIM, and DMARC Evaluation

- Authentication results were interpreted using the header analyser.
- All results passed, confirming the message was sent through legitimate mail infrastructure.

Step 4: Content and Language Analysis

- The email body was reviewed for tone, intent, and language quality.
- Red flags such as lack of job details, generic greetings, and urgency to move to a messaging app were noted.
- The sender's name appeared informal and unverified.

Step 5: Recipient Behaviour and Pattern Recognition

- The message was sent to a large number of recipients—indicating a bulk phishing attempt.

- This pattern mimics scam campaigns targeting multiple individuals with identical content.

Step 6: Evidence Documentation

- All findings (headers, screenshots, domain/IP ownership, and metadata) were documented and categorized.
- Indicators of Compromise (IoCs) were listed in a structured manner to support the final classification.

3.3 Ethical Considerations and Data Handling

The analysis was conducted in a controlled, educational environment, ensuring no interaction with the sender, no clicking on links, and no exposure to possible malicious payloads. Sensitive recipient data has been anonymized or excluded from any public documentation.

3.4 Relevance of Methodology to Real-World Scenarios

This investigation simulated an entry-level cybersecurity triage workflow. The tools and steps used mirror those employed by incident responders, email security analysts, and SOC (Security Operations Centre) personnel. Mastery of this methodology is essential for professionals tasked with identifying and mitigating email-based threats in enterprise environments.

Chapter 4: Email Sample Description

4.1 Overview of the Email

The email selected for analysis was received from the address **scriptentryteam1@gmail.com** on **July 29, 2025, at 4:55 PM IST**, bearing the subject line **"Data entry work."** The message was directed to over 18 visible recipients, all listed in the "To" field, which indicates that it was likely part of a mass-mailing effort.

The sender introduced themselves informally as **Muskan Sharma**, stating that they had reviewed the recipient's freelancer profile and were seeking data entry operators. The message instructed recipients to contact the sender on **WhatsApp** and submit a screenshot of their freelancer profile to initiate further discussion.

This type of unsolicited job offer, sent from a free email domain with a vague message body and an off-platform redirection (to WhatsApp), is commonly observed in phishing and scam campaigns targeting freelance professionals.

4.2 Message Characteristics

Attribute	Details
Sender Name	Muskan Sharma
Sender Email Address	scriptentryteam1@gmail.com
Subject Line	Data entry work.
Date and Time Sent	July 29, 2025, 4:55 PM IST
Contact Information	WhatsApp Number: +91 9354143590
Number of Recipients	18+ recipients visible in the "To" field
Message Body Summary	Short message offering data entry work, requesting contact via WhatsApp
Attachments	None
Hyperlinks	None (only a plain-text phone number)

4.3 Email Body

Dear, Freelancer

Recently, our company has checked your profile on the Freelancer website. Your profile is exactly matching with the job offered in our company.

you drop Whatsapp message on our company Number With Screenshot Of Mail

If you're interested in collaborating on this project, please let us know your availability on WhatsApp. You can reach us at +91 9354143590 We look forward to the possibility of working together to bring this project to successful completion.

Best regards,

Muskan Sharma

Contact Number: +91 XXXXX XXXXX

The language is informal, generic, and devoid of any professional signature or organization affiliation. There are no specific job details, no reference to the recipient's name or profile, and no contractual or identity verification information.

4.4 Red Flags and Suspicious Indicators

Indicator	Description
Use of a Free Gmail Address	Legitimate companies typically send emails from domain-specific accounts, not personal Gmail IDs.
Bulk Distribution	All recipients are listed openly in the "To" field, suggesting the email was not personalized.
Unverified Contact Method	The sender instructs the recipient to contact via WhatsApp, a common tactic to avoid traceability.
Lack of Company Branding	No organization name, website, or contact details are included.
Absence of Job Details	No information regarding role responsibilities, compensation, or application process.
Informal Tone and Structure	The message lacks professionalism and includes vague wording.

These characteristics are consistent with phishing and scam tactics that seek to exploit freelance job seekers and redirect them into private communication channels where fraudulent interactions may occur.

4.5 Email Header Analysis

The **email header** was examined using a secure header analysis tool. The extracted metadata confirmed the following:

Header Field	Value / Observation
Message ID	Masked for privacy

Sending IP Address	Redacted (Belonged to a major email provider)
Sending Host	Redacted (Authorized provider infrastructure)
SPF Authentication	Pass
DKIM Authentication	Pass
DMARC Policy	Pass
Delivery Delay	Within normal range

***Note** : Full header details are withheld here to preserve privacy and infrastructure security. Authentication results confirm the email was sent via a legitimate service, but this does not validate the **intent or identity** of the sender.*

4.6 IP and Domain Ownership Verification

The IP address associated with the email was verified using WHOIS lookup services. The results (sanitized here) showed:

Attribute	Value (Redacted for Public Sharing)
IP Organization	Large US-based internet company (name omitted)
NetRange	Redacted
ASN	Redacted
Location	Redacted
Domain Registration	Registered since early 2000s
Reverse DNS	Redacted (host associated with email infrastructure)

These results confirm that **email infrastructure was legitimate**, but highlight that **free accounts** from such providers can be exploited by attackers.

4.7 Interpretation

Despite passing **all technical validation checks** (SPF, DKIM, DMARC), the email exhibits strong **behavioural red flags**:

- Informal tone,
- Bulk targeting,
- Off-platform communication,
- Lack of verification or professional details.

This message aligns with known **freelance scam patterns**, relying on **human manipulation** rather than malware or attachments. The goal is to move the

recipient into a private, **less-regulated channel** where fraud may occur. This case underscores the need to evaluate **context and content**, not just technical authenticity.

Chapter 5: Detailed Analysis

5.1 Sender Verification

5.1.1 Display Name vs. Actual Email Address

- **Display Name:** Script Entry
- **Email Address:** scriptentryteam1@gmail.com

The sender used a **free Gmail address** rather than a domain-based corporate email (e.g., @companyname.com). While Gmail's infrastructure is technically secure and authenticated, using a **generic address for job offers** is considered suspicious. **Legitimate organizations** typically use verified domains and email signatures for recruitment communications.

5.1.2 Domain Authentication and Ownership

- **Domain Ownership:** Not applicable (free email service)
- **SPF (Sender Policy Framework):** Pass
- **DKIM (DomainKeys Identified Mail):** Pass
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Pass
- **Mailed-by / Signed-by:** gmail.com

These **email authentication results confirm technical legitimacy**, indicating the message came from an authorized Gmail server. However, **authentication protocols do not validate the sender's trustworthiness** or business legitimacy.

5.2 Header and Distribution Pattern Analysis

Analysis of the email header revealed:

- **Recipient Exposure:** The message was sent to at least 18 addresses, all openly visible in the **"To" field**.
- **Privacy Concern:** This **violates email etiquette** and exposes recipient data.
- **Bulk Behaviour Pattern:** No personalization or BCC usage, which is typical of **phishing or scam campaigns**.

Legitimate recruiters maintain **individual communication channels** and prioritize recipient confidentiality.

5.3 Content Analysis

5.3.1 Language and Tone

The body of the email is **brief**, **informal**, and **non-specific**. Example:

"We saw your freelancer profile. We're looking for data entry operators. Contact us on WhatsApp with your freelancer screenshot."

Key Observations:

- **No personalization:** Recipient name, profile reference, or location missing.
- **Grammatical issues:** Sentence structure is basic and lacks professionalism.
- **Non-professional redirection:** The request to move to Third-Party Messaging App for further discussion is unorthodox and suspect.

5.3.2 Omission of Key Job Information

The email **omits essential components** of a professional job offer, such as:

- Job title and responsibilities
- Employer name or website
- Salary or compensation details
- Official contact person or HR designation
- Application, interview, or onboarding procedure
- Email signature or disclaimers

These omissions are **common indicators** of fraud attempts that prioritize **quick engagement** over transparency.

5.3.3 Psychological Triggers and Manipulation Techniques

- **Curiosity and Opportunity:** Appeals to freelancers seeking work.
- **Urgency via minimal barriers:** No formal process; simply message on WhatsApp.
- **Deceptive Simplicity:** The message appears harmless and casual—intended to **bypass critical thinking**.

These are **classic social engineering methods** targeting emotional and opportunistic triggers rather than technical vulnerabilities.

5.4 Link and Attachment Evaluation

5.4.1 Hyperlink and Redirection Behaviour

- **No clickable links** were present.
- Instead, a **plain-text phone number** was shared:
  +91 XXXXX XXXXX

- Recipients were **directed to Third-Party Messaging App** for follow-up.

This method:

- **Avoids spam filters** (which scan for malicious links)
- **Moves the conversation off-platform**, where:
    - Logs are harder to capture
    - Fraud is more difficult to track
    - Victims are more susceptible to manipulation

5.4.2 Attachment Behaviour

- **No attachments** were included in the original email.
- However, **phishing campaigns using WhatsApp** often continue with:
    - Suspicious file requests (.apk, .zip, .exe, etc.)
    - Requests for **personal documentation** (IDs, photos, banking info)
    - Demands for **"processing" or "registration" fees**

Thus, the **email acts as a gateway** to higher-risk interactions once off-platform.

5.5 Conclusion

Summary Table of Risk Indicators

Suspicious Trait	Implication
Use of a free email account	No organizational verification or sender accountability
Mass distribution to open list	Resembles impersonal spam/scam campaigns
Lack of job structure/details	No transparency or formal engagement process
Redirection to WhatsApp	Avoids traceability; increases risk of fraud
Informal and vague language	Reduces credibility; mirrors known scam language patterns

Risk Level: High

The evaluation of this email—its sender behaviour, content structure, and engagement method—clearly indicates it is a **phishing or scam attempt**. While the message is **technically valid** in terms of infrastructure, its **behavioural and contextual markers** reveal a deceptive intent.

This analysis highlights how **non-technical cues**, when assessed alongside message headers and server details, can help **detect socially engineered attacks**, even when no malware or links are used.

Chapter 6: Summary of Findings

6.1 Tabulated Indicators of Phishing

The following table consolidates all observable indicators that collectively classify the analysed email as a **phishing or scam attempt**. Each component was evaluated on its credibility, transparency, and alignment with professional standards.

Category	Observation	Assessment
Sender Email	Uses a free Gmail address	Suspicious (not professional)
Display Name	"Script Entry" – not linked to any verifiable organization	Ambiguous / Misleading
Domain Authentication	Sent from Gmail infrastructure; lacks custom domain	No verification possible
Recipients	Sent to bulk addresses in visible "To" field	Mass distribution / Privacy violation
Subject Line	"Data entry work." – vague and generic	Unclear / Lacks specificity
Greeting	"Dear Freelancer" – non-personalized	Bulk targeting
Language & Grammar	Contains grammatical errors and informal structure	Unprofessional
Job Description	Absent – no defined role, requirements, or process	Lack of transparency
Call to Action	Asks recipient to connect via WhatsApp using a phone number	Redirection to unverifiable channel
Links / Attachments	No clickable links or files; provides a phone number for offline engagement	Suspicious (alternate delivery vector)
Company Information	No name, address, registration, or domain-based presence	No organizational credibility
Signature Block	Only includes a name and phone number	Weak / Non-corporate signature

---

6.2 Severity Assessment

This email demonstrates clear **social engineering tactics** and exhibits characteristics often seen in **phishing scams**. Although it avoids traditional spam

indicators (such as failed SPF/DKIM), it violates almost every **behavioural indicator of a legitimate job offer**.

Risk Level: High

Potential Threats:

- **Financial Exploitation:** The user may be manipulated into transferring money (e.g., for "registration fees").
- **Identity Theft:** Scammers could solicit sensitive documents (e.g., government IDs or banking information).
- **Malware Risk:** Upon further engagement via a third-party messaging platform, malicious files could be shared.
- **Privacy Breach:** Redirection to personal messaging apps increases vulnerability to social exploitation.

6.3 Overall Risk Evaluation

The table below summarizes key indicators and the assessed phishing risk:

Evaluation Parameter	Status
Sender Credibility	Not verifiable – public/free email used
Language and Tone Professionalism	Poor grammar and non-specific messaging
Technical Email Security	Standard authentication (SPF/DKIM/DMARC) – no organizational trace
Redirection Method	Off-platform contact method (messaging app)
Possibility of Legitimate Offer	Extremely low
Impact if Recipient Engages	High risk – financial, personal data, or system compromise

---

Chapter 7: Recommendations and Defensive Measures

7.1 Immediate User Actions

Based on the findings in this report, the suspicious email in question exhibits multiple red flags indicative of a phishing or scam attempt. Users who have received such emails should take the following immediate steps to protect themselves and their information:

- **Do Not Respond:** Avoid replying or engaging in any form of communication with the sender.
- **Do Not Share Personal Information:** Never provide identification documents, selfies, bank account numbers, or contact details through email or external platforms like WhatsApp.
- **Do Not Click or Download:** Do not click on any suspicious links or download files from unfamiliar or unsolicited sources, especially those shared via private messaging apps.
- **Report the Email:** Use the reporting tools to flag the email for review and improve detection algorithms.
- **Block the Sender:** Prevent further communication by blocking the sender directly .
- **Notify Others:** If the message was part of a larger bulk mailing (as in this case), inform peers and community forums to help others avoid falling victim.

7.2 Best Practices for Email Safety

To improve personal and organizational security against phishing threats, users are advised to follow these email security best practices:

7.2.1 Verify the Sender

- Check if the email is from a public domain instead of an official organizational domain.
- Use **WHOIS lookup tools** to check domain age and registration.

7.2.2 Review the Email Header

- Use tools like **Google Admin Toolbox** or **MXToolbox** to verify SPF, DKIM, and DMARC authentication results.
- Look for anomalies in mail servers, IP addresses, and timestamps.

7.2.3 Analyze Email Content Critically

- Be cautious of emails with vague subject lines, generic greetings, or poor grammar.

- Look for urgent call-to-action messages such as “respond immediately,” “click now,” or “limited time offer.”

7.2.4 Watch for Unusual Redirects

- Emails that redirect users to external platforms should be treated with suspicion.
- Hover over links to see their real destination before clicking.

7.2.5 Use Security Tools

- Scan links and attachments using **VirusTotal**, **PhishTank**, or other trusted reputation scanners.
- Employ browser extensions or email clients that detect phishing attempts in real-time.

7.3 Organizational Recommendations

For teams, institutions, or freelancer communities where such emails may be common, implementing organizational safeguards is critical.

7.3.1 Awareness Training

- Conduct periodic phishing awareness sessions for users, freelancers, or employees.
- Share real-world examples of phishing attempts and guide users on how to handle them.

7.3.2 Incident Reporting Framework

- Establish a simple and accessible system where phishing emails can be reported and logged.
- Maintain a centralized log of common scam emails for education and pattern tracking.

7.3.3 Technical Defenses

- Use advanced email gateways that offer AI-based phishing detection.
- Enforce SPF, DKIM, and DMARC policies for your domain to reduce spoofing risks.

7.4 Legal & Reporting Channels

If a phishing attempt results in or threatens financial fraud or identity theft, users should:

- **Report to Indian Cybercrime Portal**: https://cybercrime.gov.in

- **Notify Email Providers** (e.g., Gmail's Abuse Form)
- **Report Scam Phone Numbers** to telecom authorities or community verification platforms like Truecaller.

7.5 Long-Term Preventive Measures

Measure	Benefit
Enable two-factor authentication	Reduces risk of email hijacking
Use secure email providers	Enhanced built-in protection against phishing
Regular device scanning	Early detection of malware and trojans
Use separate emails for job hunt	Isolates potential scam reach from personal data
Keep OS and antivirus updated	Protects against evolving phishing techniques

---

Chapter 8: Conclusion

8.1 Conclusion

The analysis conducted in this case study confirms that the email titled **"Data entry work"**, sent from a **free email service provider** and requesting off-platform engagement, exhibits multiple red flags indicative of a **phishing or scam attempt**. Although the message did not contain hyperlinks or file attachments, its content, distribution method, and tone align with tactics frequently seen in social engineering campaigns.

One of the key insights from this investigation is that even **technically authenticated emails**—those passing SPF, DKIM, and DMARC checks—can still be deceptive. This email exploited behavioural loopholes such as urgency, informality, and emotional triggers while cleverly avoiding traditional spam filters by redirecting users to an unregulated messaging platform.

Using **freely available investigation tools** (such as email header analysers, WHOIS lookup services, and manual inspection), we dissected the email structure, verified technical legitimacy, and evaluated its intent through contextual cues. The process reaffirmed that **behavioural analysis is as critical as technical validation** in identifying phishing attempts.

8.2 Key Learnings

Learning Area	Insight Gained
Email Structure Analysis	Full headers can reveal hidden delivery patterns and sender information.
Authentication Protocols	SPF, DKIM, and DMARC success doesn't equate to sender legitimacy.
Content Evaluation	Poor grammar, informal tone, and generic phrasing are strong phishing indicators.
Social Engineering Tactics	Scammers exploit trust by moving conversations to apps like messaging platforms.
Tool Usage	Free tools like Google Admin Toolbox, WHOIS, and VirusTotal offer strong support.

8.3 Final Thoughts

In today's digital environment, **email remains one of the most exploited attack vectors**, particularly in phishing campaigns. This analysis demonstrates that phishing attacks don't always involve malware or complex code—they rely on **manipulating human behaviour**.

To mitigate such threats, it's essential to:

- Be skeptical of **unsolicited job offers** that lack clear details or organizational validation.
- **Verify sender identity** and communication channels before engaging.
- Use available tools to **analyse email headers and content**.
- Promote awareness by reporting incidents and educating peers.

This exercise not only sharpens practical cybersecurity skills but also promotes a proactive and vigilant digital culture. Whether for personal safety or professional defense, **identifying low-observability threats is a foundational skill** in today's cybersecurity landscape.
