

Task 2 [Elevate labs]

Analyze a Phishing Email Sample

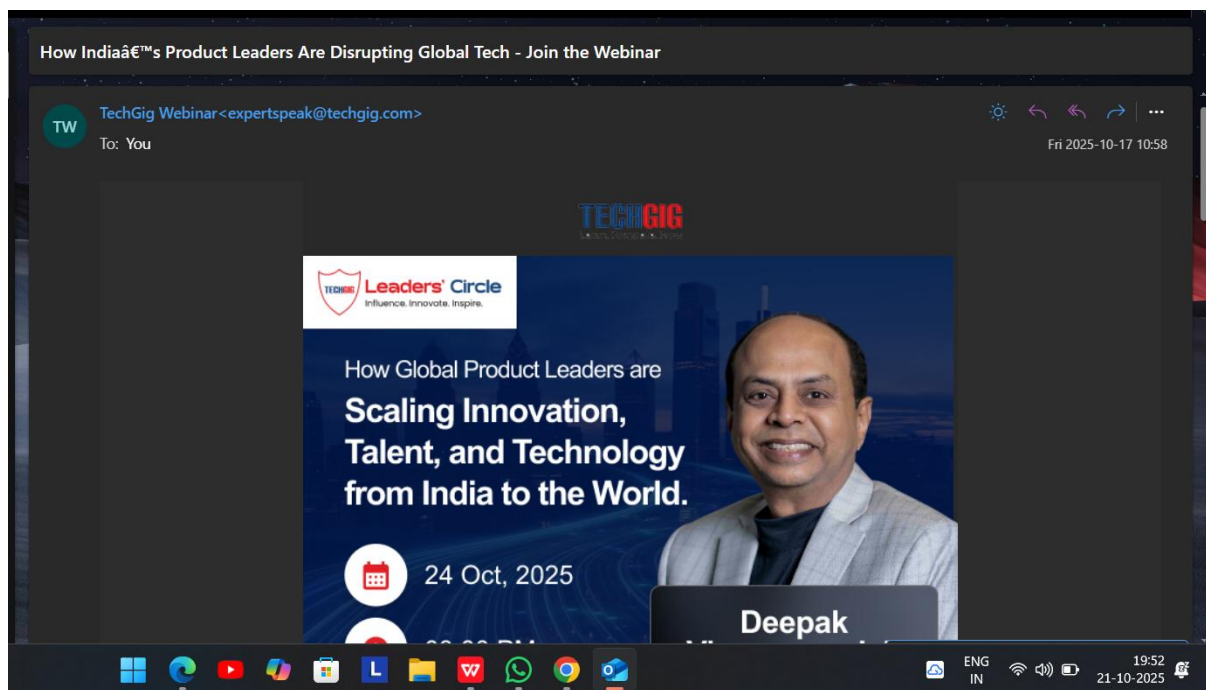
Aim:

To develop awareness of phishing tactics and gain practical skills in identifying, analyzing, and evaluating suspicious emails.

Tools Used:

- 1.Email Client – to view and copy raw email headers (Gmail, Outlook, etc.)
- 2.VirusTotal – to safely scan URLs and attachments
- 3.URLScan.io – to inspect suspicious links in a sandboxed environment
- 4.Text Editor / Spreadsheet – to document findings, phishing traits, and URLs

- 1.Obtained a sample phishing email. i took the spam one.



2. open the tool to analyse the header and fine if it is suspicious or not.

The screenshot shows a Bing search results page for the query 'google admin toolbox'. The search bar at the top contains the text 'google admin toolbox'. Below the search bar, there are tabs for 'ALL', 'SEARCH', 'VIDEOS', 'IMAGES', 'MAPS', 'NEWS', 'COPILOT', and 'MORE'. The search results show 'About 337,000 results' and a 'Date' dropdown. The first result is titled 'HAR Analyzer' with a URL 'https://toolbox.googleapps.com › apps › main'. Below this is a link to 'Google Admin Toolbox' with the description 'Use the Google Admin Toolbox to troubleshoot issues you have with Google Workspace services.' The second result is also titled 'HAR Analyzer' with a URL 'https://toolbox.googleapps.com › apps › dig'. Below this is a link to 'Dig (DNS lookup) - Google Search' with the description 'Google Admin ToolboxDig Help To make a DNS lookup: Enter domain name (trailing dot will be auto-appended). Lookup and enjoy the output.'

3. Go to the investigate mail issues to analyse the email.

The screenshot shows the Google Admin Toolbox website. The header is green with the text 'Google Admin Toolbox' and a 'Help' link. Below the header, there is a message: 'Use the Google Admin Toolbox to troubleshoot issues you have with Google Workspace services.' The main content area is divided into several sections. The first section is 'Debug Browser issues' with links to 'Browserinfo' and 'Useragent'. The second section is 'Verify DNS issues' with links to 'Check MX' and 'Dig'. The third section is 'Analyze HAR and log files' with links to 'HAR Analyzer', 'Log Analyzer', and 'Log Analyzer 2'. The fourth section is 'Investigate mail issues' with a link to 'Messageheader'. The fifth section is 'Other debugging tools' with links to 'Additional Tools', 'Encode/Decode', and 'Screen Recorder'. The bottom of the page shows a Windows taskbar with various icons and a system clock showing 18:25 on 21-10-2025.

4.paste the header

The screenshot shows the Google Admin Toolbox Messageheader interface. The header details are as follows:

MessageId	b599fd515inha7@mgw11.techgig.com
Created at:	10/17/2025, 10:58:29 AM GMT+5:30 (Delivered after 9 sec)
From:	TechGig Webinar <expertspeak@techgig.com>
To:	'mahajanvistruti49@gmail.com' <mahajanvistruti49@gmail.com>
Subject:	How India's Product Leaders Are Disrupting Global Tech - Join the Webinar

#	Delay	From *	To *	Protocol	Time received
0		tgwebz1ap3079	→ mgw11.techgig.com	ESMTP	10/17/2025, 10:58:29 AM GMT+5:30
1	9 sec	mgw11.techgig.com	→ [Google] mx.google.com	ESMTPS	10/17/2025, 10:58:38 AM GMT+5:30
2			→ [Google] 2002:a17:907:2d09:b0:b46:2634:1074	SMTP	10/17/2025, 10:58:38 AM GMT+5:30

Below the table is a button labeled "ANALYZE ANOTHER HEADER".

5.The result

The screenshot shows the Google Admin Toolbox Messageheader interface with the "SHOW RAW HEADER" button clicked. The raw header content is displayed below:

```
Received: by 2002:a17:907:2d09:b0:b46:2634:1074 with SMTP id gs9csp6555044ejc;
Thu, 16 Oct 2025 22:28:38 -0700 (PDT)
Received: from mgw11.techgig.com (mgw11.techgig.com. [219.65.84.11])
by mx.google.com with ESMTPS id 98e67ed59e1d1-33bd7b98debsi874122a91.85.2025.10.16.22.28.37
for <mahajanvistruti49@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 16 Oct 2025 22:28:38 -0700 (PDT)
Received: from tgwebz1ap3079 (HELO localhost) ([172.29.30.79])
by mgw11.techgig.com with ESMTP; 17 Oct 2025 10:58:29 +0530
From: TechGig Webinar <expertspeak@techgig.com>
To: "mahajanvistruti49@gmail.com" <mahajanvistruti49@gmail.com>
Subject:
=?Windows-1252?Q?How_India=E2=80=99s_Product_Leaders_Are_Disrupting_Globa?=?
=?Windows-1252?Q?Tech_Join_the_Webinar?=?
```

6. For the URLs I have used the virustotal tool.

The image shows a Bing search result for 'virustotal' and a screenshot of the VirusTotal website. The Bing search results show 'About 325,000 results' and a 'Copilot Search' section. The Copilot Search section displays the VirusTotal logo, the URL 'https://www.virustotal.com', and the title 'VirusTotal - Home'. Below this, there are four links: 'Search', 'VirusTotal Enterprise', 'Read the article', and 'File'. The 'Search' link is highlighted. The 'VirusTotal Enterprise' link is also highlighted. The 'Read the article' link is highlighted. The 'File' link is highlighted. The 'Search' link is highlighted. The 'VirusTotal Enterprise' link is highlighted. The 'Read the article' link is highlighted. The 'File' link is highlighted.

VirusTotal
https://www.virustotal.com

VirusTotal - Home

VirusTotal is a service that allows you to scan files, domains, IPs and URLs for malware and other threats. You can also share your submissions with the security community and access ...

Search
VirusTotal is a free online tool that analyzes files and URLs for viruses, wor...

VirusTotal Enterprise
VirusTotal is the world's richest, most interlinked and closest to real-time crow...

Read the article
VirusTotal helps you to automatically

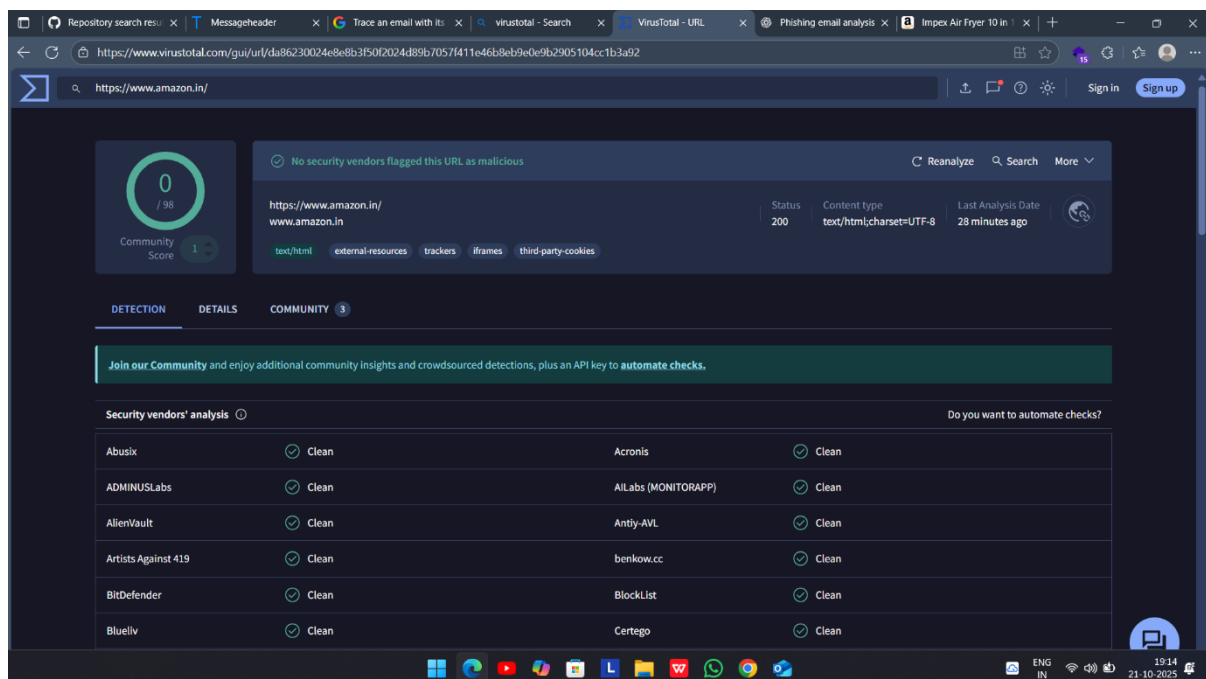
File
Explore our dataset visually, discover threat

The screenshot of the VirusTotal website shows the 'URL' tab selected. The search bar contains the text 'Search or scan a URL'. Below the search bar is a 'Search' button. The website footer contains a 'YouTube' link and a 'Want to automate submissions? Check our API, or access your API key.' link. The system tray shows the date '21-10-2025' and the time '19:12'.

7. I have used the amazon one for example.



8. The result



conclusion:

The analysis revealed phishing indicators such as spoofed sender addresses, failed SPF/DKIM/DMARC checks, mismatched or suspicious URLs, urgent language, and spelling/grammar errors. This exercise helped build practical skills for detecting email threats and understanding how phishing attacks operate.

