Phishing email analysis:

1.

sample phishing email

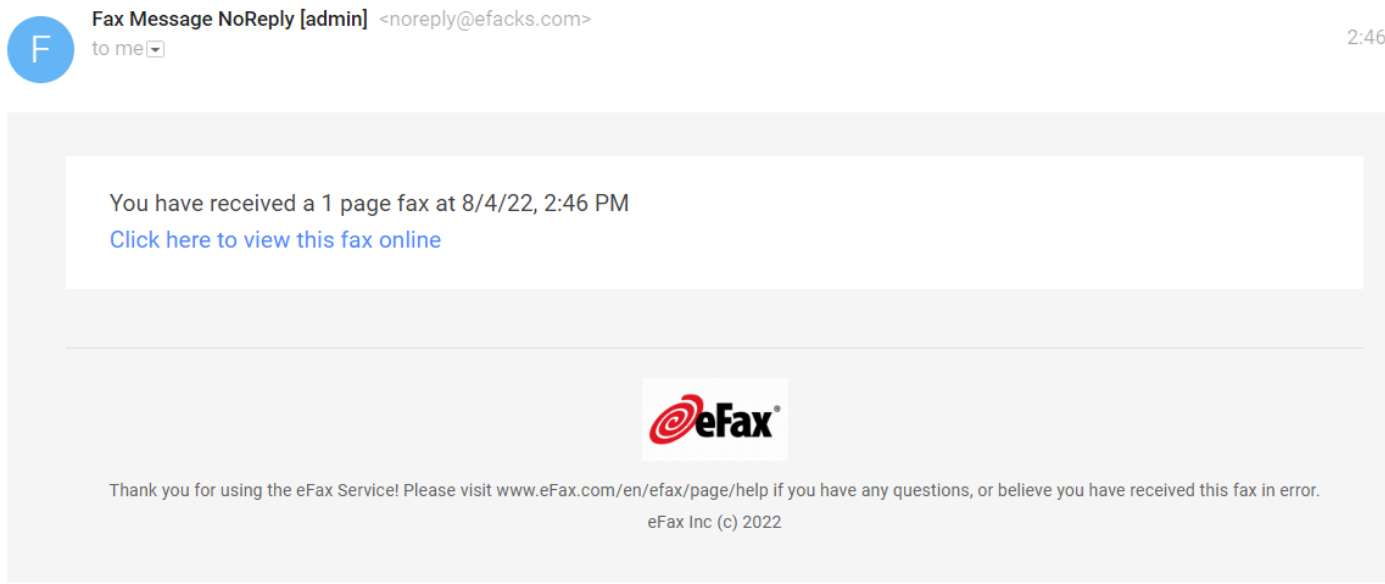
-sender's email address for spoofing: efacks.com

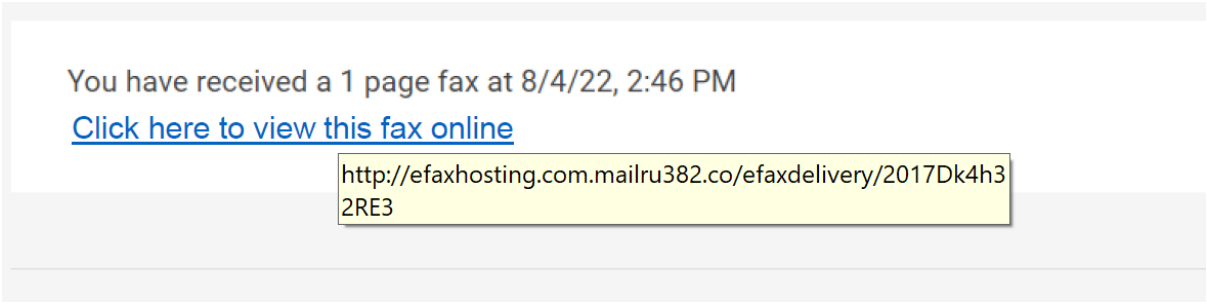
-original email: efax.com

-presence of suspicious links or attachments :yes

-urgent or threatening language in the email body: No sense of emergency, grammatical error seen.

- Note any mismatched URLs (hover to see real link). yes





sample phishing email

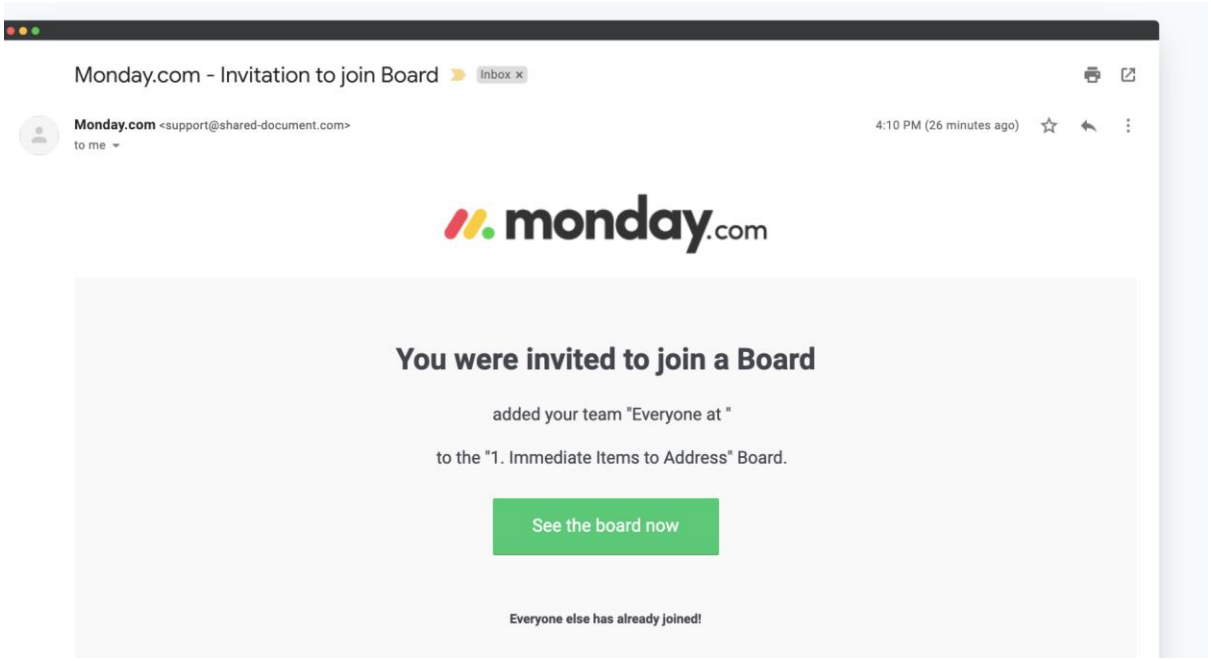
-sender's email address for spoofing: support@shared-document.com

-original email: Monday.com

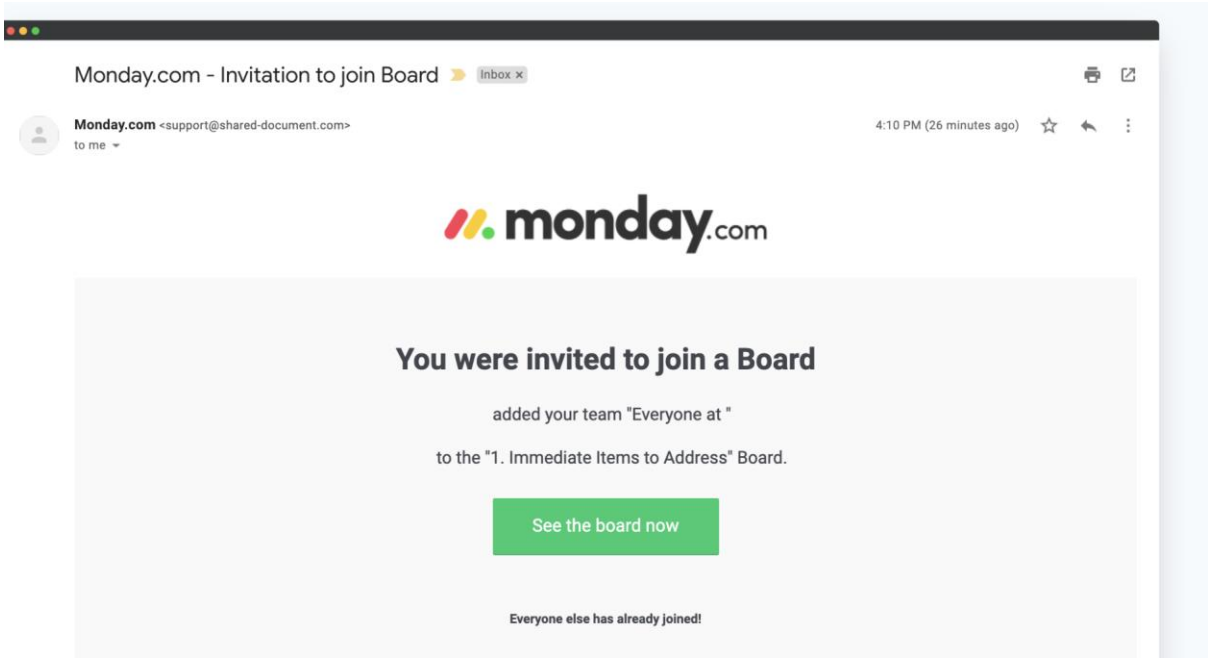
-presence of suspicious links or attachments :yes

-urgent or threatening language in the email body: yes sense of emergency, grammatical error seen.

- Note any mismatched URLs (hover to see real link): yes ,Suspecious link in email , sense of urgency is also seen , telling everyone has already joined.



2.



Summarize phishing traits found in the email.

Check email headers for discrepancies

Look for urgent or threatening language in the email body.

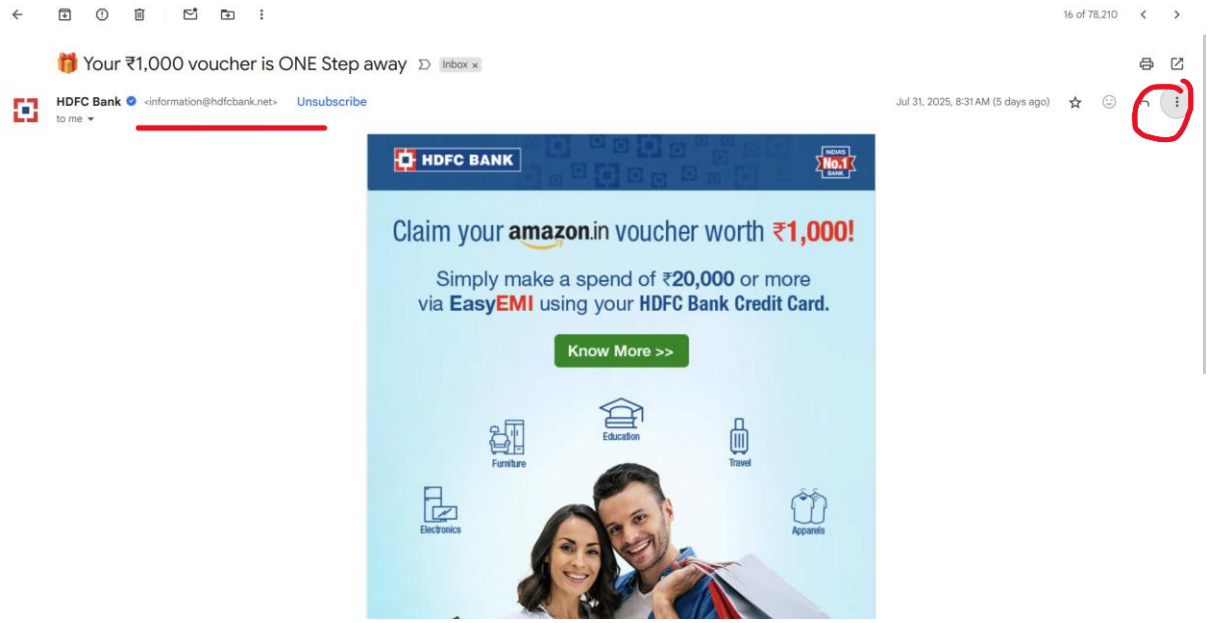
Note any mismatched URLs, malicious link in the email

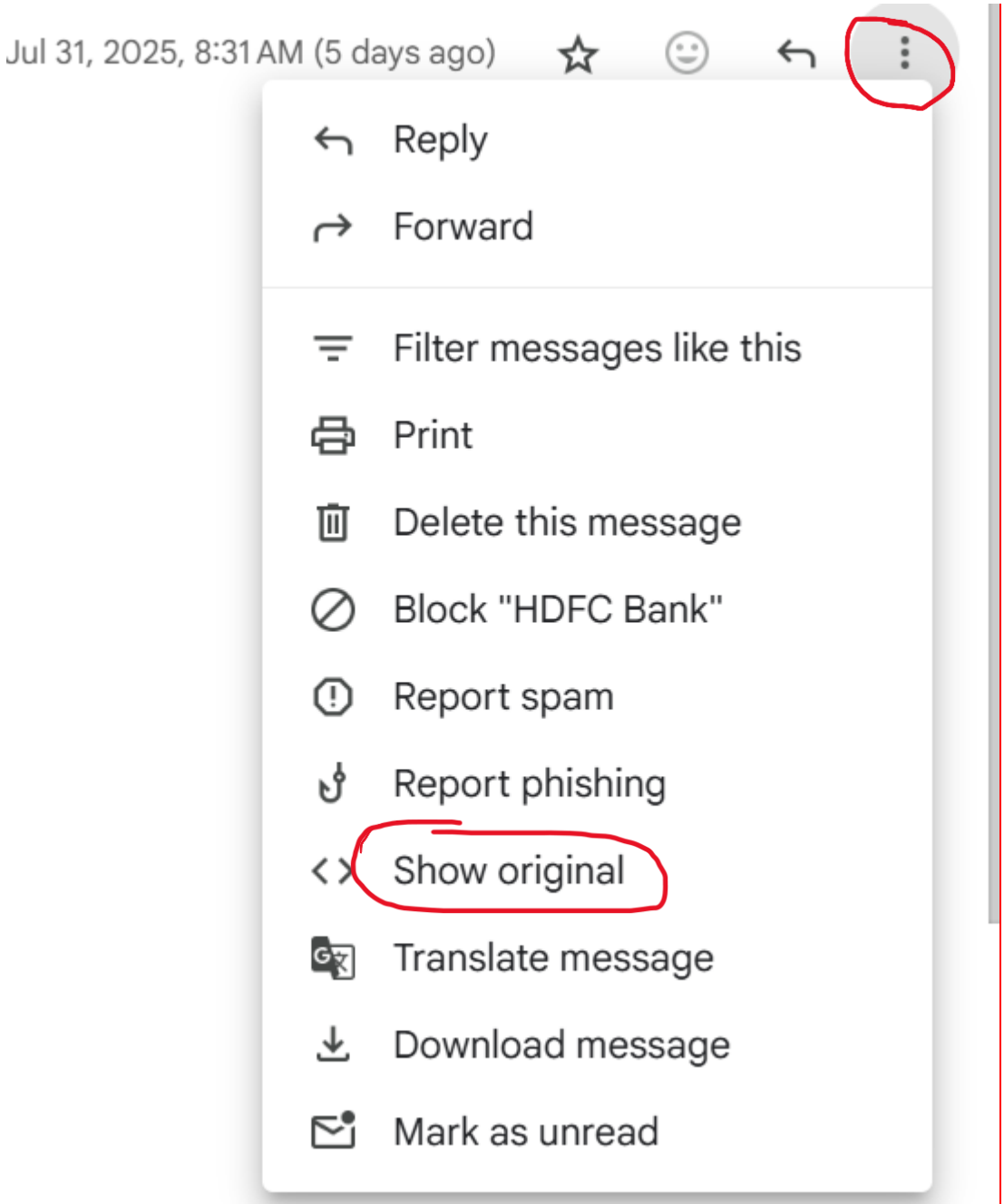
Verify presence of spelling or grammar errors.

the reputation of IP addresses. By looking up the SMTP address of the email

no URLs and files in the email does not mean that it is not malicious. The attacker may also send the malware as an image to avoid detection by the analysis tools.

3.Email header analysis:



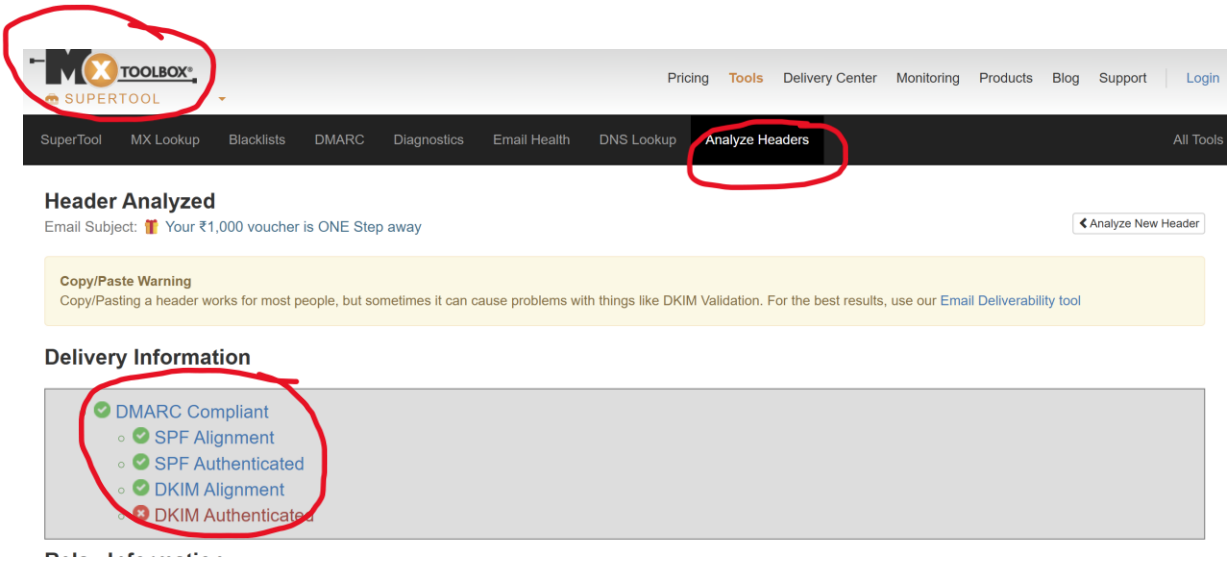


Original Message

Message ID	<77cf48d2ef4c844cb539189c2e6e6d22@hdfcbank.net>
Created at:	Thu, Jul 31, 2025 at 8:30 AM (Delivered after 29 seconds)
From:	HDFC Bank <information@hdfcbank.net>
To:	1mailtosm@gmail.com
Subject:	🎁 Your ₹1,000 voucher is ONE Step away
SPF:	PASS with IP 103.108.11.102 Learn more
DKIM:	'PASS' with domain hdfcbank.net Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard



Sender Policy Framework (SPF) records allow domain owners to publish a list of IP addresses or subnets that are authorized to send email on their behalf.

DomainKeys Identified Mail (DKIM) email signatures that help email service providers identify and authenticate your emails,

What tools can analyze email headers?

Mxtoolbox, urlscan.

What is an Email Header?

section of the email containing information such as sender, recipient, and date.

Allows you to identify the sender and recipient ,Allows You to Track an Email's Route ,if it came from the correct address.

Analysis

static:

email programs offer HTML support to grab the user's attention. downside to this feature. Attackers can use HTML to create emails that hide malicious URLs behind buttons or text that appear to be harmless.

Dynamic:

URLs and files in an email need to be checked to make sure they are safe. websites and files in the mail should be run in sandbox environments {AnyRun}, changes made to the system should be examined to see if they are harmful or not.

use online web browsers such as Browserling to quickly check the web addresses in the email. advantage of such services is that you are not burdened by a possible zero-day vulnerability that would impact browsers, as you are not visiting the website on your own computer.

Thank you.