

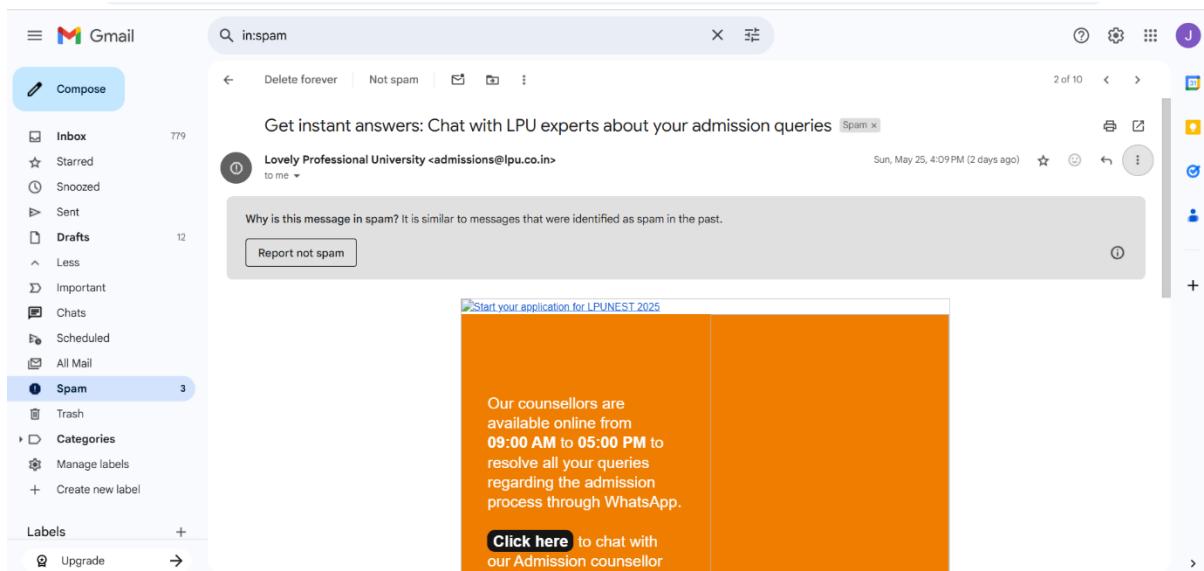
# Analyze a Phishing Email Sample

**Objective:** Identify phishing characteristics in a suspicious email sample.

**Tools:** Email client or saved email file (text), free online header analyzer.

**Deliverables:** A report listing phishing indicators found

## 1. Obtain a sample phishing email (many free samples online).



A screenshot of a Gmail inbox. The search bar at the top shows "in:spam". There are 6 of 10 messages in the list. The first message is from "Geeta University <admission@geetauniversity.edu.in>" with the subject "Join Geeta University Exclusive Webinar on Careers in M.Sc. Forensic Science.". A "Spam" button is visible next to the message. Below the message, there's a note: "Why is this message in spam? It is similar to messages that were identified as spam in the past." with a "Report not spam" button. The message was sent on "Thu, May 15, 10:28 AM (12 days ago)". The left sidebar shows the navigation menu with "Spam" selected.

I have mentioned two spam emails from my email list . These are the sample phishing email .

## 2. Examine sender's email address for spoofing.

A screenshot of a Gmail inbox. The search bar at the top shows "in:spam". There are 2 of 10 messages in the list. The first message is from "Lovely Professional University <admissions@lpu.co.in>" with the subject "Get instant answers: Chat with LPU experts about your admission queries". A "Spam" button is visible next to the message. Below the message, there's a note: "Why is this message in spam? It is similar to messages that were identified as spam in the past." with a "Report not spam" button. The message was sent on "Sun, May 25, 4:09 PM (2 days ago)". The right side of the screen shows a context menu with options like "Reply", "Forward", "Print", "Delete this message", "Block", "Report phishing", "Show original", "Translate message", "Download message", and "Mark as unread". The left sidebar shows the navigation menu with "Spam" selected.

Verify and use the show original option to identify the email sender , and easy to check the spoofing attack .

#### Original Message

Message ID	<kFx5J_7R12E0X5j8WCVsg@geopod-ismldp-8>
Created at:	Sun, May 25, 2025 at 4:09 PM (Delivered after 2 seconds)
From:	Lovely Professional University <admissions@lpu.co.in>
To:	jayavarshiniamarnath@gmail.com
Subject:	Get instant answers: Chat with LPU experts about your admission queries
SPF:	PASS with IP 50.31.42.16 <a href="#">Learn more</a>
DKIM:	'PASS' with domain lpu.co.in <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

[Download Original](#)

[Copy to clipboard](#)

```
Delivered-To: jayavarshiniamarnath@gmail.com
Received: by 2002:a05:7208:60d2:b0:a8:1d58:40b9 with SMTP id k18csp3629255rba;
      Sun, 25 May 2025 03:39:25 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IGswkeoD1ES10jd65hEb0eF5L31FrJYtcrN960XIm/jeIa1lu0Gjf681wOCzi/pVeBul
X-Received: by 2002:a05:6a21:3399:b0:1fs:769a:abf with SMTP id adf61e73a8af0-2188c3b49b3mr10735118637.36.1748169565267;
      Sun, 25 May 2025 03:39:25 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1748169565; cv=none;
      d=google.com; s=arc-20240605;
```

After clicking the show original option , it shows the clear history of the spoofing email.

### 3. Check email headers for discrepancies (using online header analyzer).

Google search results for "email header analyzer":

- MxToolbox** [https://toolbox.googleapps.com/apps/messageheader](https://mxtoolbox.com>Email Headers</a><br/>Email Header Analyzer, RFC822 Parser<br/>This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and ...</li><li><b>Message Header Analyzer</b><br/>Message Header Analyzer · Insert the message header you would like to analyze · Summary · Received headers · Forefront Antispam Report Header · Microsoft ...</li><li><b>ToolBox Google Apps</b> <a href=)  
Messageheader - ToolBox Google Apps  
What can this tool tell from email headers? Identify delivery delays. Identify approximate source of delay. Identify who may be responsible. Example of what ...

I have choose the MxToolbox Online header to analyse the email spoofing .

#### ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, [just read this tutorial](#).

## MxToolbox inside

#### Original Message

Copied to clipboard!

Message ID	<kFx5J_7R12E0X5j8WCVsg@geopod-ismtpd-8>
Created at:	Sun, May 25, 2025 at 4:09 PM (Delivered after 2 seconds)
From:	Lovely Professional University <admissions@lpu.co.in>
To:	jayavarshiniamarnath@gmail.com
Subject:	Get instant answers: Chat with LPU experts about your admission queries
SPF:	PASS with IP 50.31.42.16 <a href="#">Learn more</a>
DKIM:	'PASS' with domain lpu.co.in <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

[Download Original](#)

[Copy to clipboard](#)

Copy the code to analyse the email, and verify it is phishing email or not.

#### Email Header Analyzer

```
Popen(runr-300001.R0eEj-2f-vQHM420fHGYGQRCLChH0dagDG44tqShr-ZXWzZ-2cH0lkPH-
-2FLMOSht2ZBzGzbUbxpONhyhD-Y-2FNH3tGv3x7ruHOZPDeH9L1vShMkIcA8AsEbuThzBKkzz=
QJn4/W75dy-2FYikkrAC2jjnnDInQLoLj8rfolgbVZyvAlsCltmYhgOnpD7S88m-2Fk-
-2FCBRTpxtvww/8MckSXd4/JGhk3JVMTjd8ldjHZPPSo0ebGok0gjW-2FqnjXHSpMkDQTVrd=
7k2B0CQ4m6QO1dXWpyqfIncJBM6A16jz2GA8m3ElZvdWxh6bt04DFydOeCRyk0VUQcCvXo8-
ZjJe0j9E6lB1nbEwyH-3D* alt=3D* width=3D* height=3D* border=3D* st=
yle=3D*height:1px !important; width:1px !important; border-width:0 !important=
:margin-top:0 !important; margin-bottom:0 !important; margin-right:0 !important=
nt; margin-left:0 !important; padding-top:0 !important; padding-bottom:0 !impot=
rant; padding-right:0 !important; padding-left:0 !important;"></body></html>
>
```

[Analyze Header](#)

Click the Analyse Header to check the email.

**MX TOOLBOX**

SUPERTOOL

Pricing Tools Delivery Center Monitoring Products Blog Support Login

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools

**Header Analyzed**  
Email Subject: Get instant answers: Chat with LPU experts about your admission queries

**Copy/Paste Warning**  
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

**Delivery Information**

- **DMARC Compliant**
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

**Relay Information**

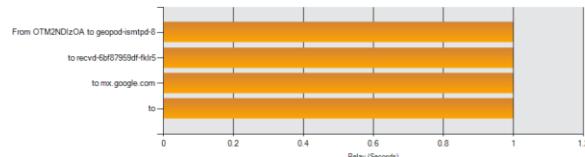
Received	0 seconds
Delay:	

It analysed the email and present their Delivery Information based on the email phishing .

1. DMARC COMPLIMENT
2. SPF ALIGNMENT
3. SPF AUTHENTICATED
4. DKIM ALIGNMENT
5. DKIM AUTHENTICATED

#### Relay Information

Received	0 seconds
Delay:	



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	OTM2NDIzOA	geopod-ismpd-8	HTTP	0	
2	*		recvd-6bf87959df-fkrl5	SMTP	0	
3	*	o31ptr2610.lpu.co.in.50.31.42.16	mx.google.com	ESMTPS	5/25/2025 10:39:25 AM	✓
4	0 seconds		2002.a05.7208.60d2.b0.a0.1d50.40b9	SMTP	5/25/2025 10:39:25 AM	

## RELAY INFORMATION

## SPF and DKIM Information

dmarc:lpu.co.in [Show](#)

v=DMARC1; p=Quarantine; rua=mailto:dmarc.rua@lpu.co.in,mailto:a28e85a0@mxtoolbox.dmarc-report.com; ruf=mailto:a28e85a0@forensics.dmarc-report.com; pct=100

spf:em5930.lpu.co.in:50.31.42.16 [Show](#) [Solve Email Delivery Problems](#)

v=spf1 ip4:50.31.42.16 -all

dkim:lpu.co.in:LPU [Show](#)

Dkim Public Record:

```
rsa; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAQCAQ8AMIIIBCgKCAQEAE2vHkJpyRQ4aItstTetNFNOKC+WJzcmBLoJfrdNa1KfOak5t/ixudIjsqZLS1nvuQkOUi0PKF07+lyUocn9GupJgx/8xy8wVi7iRMObGu5R88izq4wIg/a4/LyO4YvvFYAKG9N
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=lpu.co.in; h=content-transfer-encoding:content-type:from:mime-version:subject: reply-to:to:list-unsubscribe:list-unsubscribe-post:cc:content-type:feedback
```

dkim:sendgrid.info:smtpapi [Show](#)

Dkim Public Record:

```
rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPth5impXVpiHFzJ7Nr18UsuY9zqqzjE0O1r04xDN6qwzidnmgcFNnfMewVN2D1O+239N14hRprzByFwfQit76yojh54Xu3uSbQ3JP0A7k8o8GutRF8zbFUAn0ZH2y0cIEjMliXY4
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.info; h=content-transfer-encoding:content-type:from:mime-version:subject: reply-to:to:list-unsubscribe:list-unsubscribe-post:cc:content-type:feedback
```

## PHISHING EMAIL EXPLAIN

4. Identify suspicious links or attachments.
5. Look for urgent or threatening language in the email body.

I have used Phishtank to verify the url whether its suspicious links or not.

**PhishTank** Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

**Join the fight against phishing**

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:  
Nothing known about <https://mail.google.com/mail/u/0/#inbox/FMfcgzbft...>  
[Add it to the Tank!](#)

[Is it a phish?](#)

**Recent Submissions**  
You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
9110771	<a href="https://hidedevelopments.com.au/khrgd/chameleon/index.html">https://hidedevelopments.com.au/khrgd/chameleon/index.html</a>	laerm
9110769	<a href="https://scanned.page/682be7434901e">https://scanned.page/682be7434901e</a>	D3Lab
9110767	<a href="https://279685369873209763d09387h0.mymeriva.com/89...">https://279685369873209763d09387h0.mymeriva.com/89...</a>	D3Lab
9110765	<a href="https://onedeal.top/">https://onedeal.top/</a>	segasec
9110764	<a href="http://galiboy.site/">http://galiboy.site/</a>	segasec
9110763	<a href="https://healthcare.worldcastlive.com/wp-content/plugins/">https://healthcare.worldcastlive.com/wp-content/plugins/</a>	kkalmus
9110762	<a href="http://healthcare.worldcastlive.com/wp-content/plugins/">http://healthcare.worldcastlive.com/wp-content/plugins/</a>	kkalmus
9110760	<a href="https://tracker-livraison.com/">https://tracker-livraison.com/</a>	Josua33
9110759	<a href="https://tracker-livraison.com/as.php">https://tracker-livraison.com/as.php</a>	Josua33
9110758	<a href="https://tracker-livraison.com/step/z.php">https://tracker-livraison.com/step/z.php</a>	Josua33

**What is phishing?**  
Phishing is a fraudulent attempt, usually made through email, to steal your personal information.  
[Learn more...](#)

**What is PhishTank?**  
PhishTank is a collaborative clearing house for information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.  
[Read the FAQ...](#)

## PhishTank Website

mail.google.com/mail/u/0/#spam/FMfcgzbft... [Spam X](#)

**Gmail**  [Compose](#)

[Compose](#)  [Delete forever](#) [Not spam](#) [Report abuse](#) [More](#) [6 of 10](#)

**Inbox** 779 **Drafts** 12 **Spam** 3 **Trash** **Categories** [Manage labels](#) [Create new label](#)

**Join Geeta University Exclusive Webinar on Careers in M.Sc. Forensic Science.** [Spam X](#) [Report abuse](#) [Print](#) [Forward](#) [More](#) [Thu, May 15, 10:28 AM \(12 days ago\)](#)

to me [Report not spam](#)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

[Reply](#) [Forward](#) [More](#)

Copy the url and paste the phishtank website to identify the suspicious link .

## Join the fight against phishing

**Submit** suspected phishes. **Track** the status of your submissions.  
**Verify** other users' submissions. **Develop** software with our free API.

What  
Phishing  
usually  
your pe  
[Learn](#)

Found a phishing site? Get started now — see if it's in the Tank:  
Nothing known about <https://mail.google.com/mail/u/0/#inbox/FMfcgzQbft...>  
[Add it to the Tank?](#)

[com/mail/u/0/#spam/FMfcgzQbflRMdkWwWMKTmrqCtJnCQg](https://mail/u/0/#spam/FMfcgzQbflRMdkWwWMKTmrqCtJnCQg) **Is it a phish?**

What  
PhishTai  
house fi  
phishing  
PhishTai  
develop  
integrat  
applicat  
[Read](#)

### Recent Submissions

You can help! [Sign in or register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
<a href="#">9110771</a>	<a href="https://hijdevelopments.com.au/khgrd/chameleon/ind...">https://hijdevelopments.com.au/khgrd/chameleon/ind...</a>	<a href="#">laerm</a>
<a href="#">9110769</a>	<a href="https://scanned.page/682be7434901e">https://scanned.page/682be7434901e</a>	<a href="#">D3Lab</a>
<a href="#">9110767</a>	<a href="https://279685369873209763d09387h0.mymeriva.com/89...">https://279685369873209763d09387h0.mymeriva.com/89...</a>	<a href="#">D3Lab</a>
<a href="#">9110765</a>	<a href="https://onedeal.top/">https://onedeal.top/</a>	<a href="#">segasec</a>
<a href="#">9110764</a>	<a href="http://galixboy.site/">http://galixboy.site/</a>	<a href="#">segasec</a>
<a href="#">9110763</a>	<a href="https://healthcare.worldcastlive.com/wp-content/pl...">https://healthcare.worldcastlive.com/wp-content/pl...</a>	<a href="#">kkalmus</a>
<a href="#">9110762</a>	<a href="http://healthcare.worldcastlive.com/wp-content/plu...">http://healthcare.worldcastlive.com/wp-content/plu...</a>	<a href="#">kkalmus</a>
<a href="#">9110760</a>	<a href="https://tracker-livraison.com/">https://tracker-livraison.com/</a>	<a href="#">Josua33</a>
<a href="#">9110759</a>	<a href="https://tracker-livraison.com/as.php">https://tracker-livraison.com/as.php</a>	<a href="#">Josua33</a>
<a href="#">9110758</a>	<a href="https://tracker-livraison.com/step/z.php">https://tracker-livraison.com/step/z.php</a>	<a href="#">Josua33</a>

Click **is it a phish** option to identify the email phishing URL.

**6. Note any mismatched URLs (hover to see real link).**

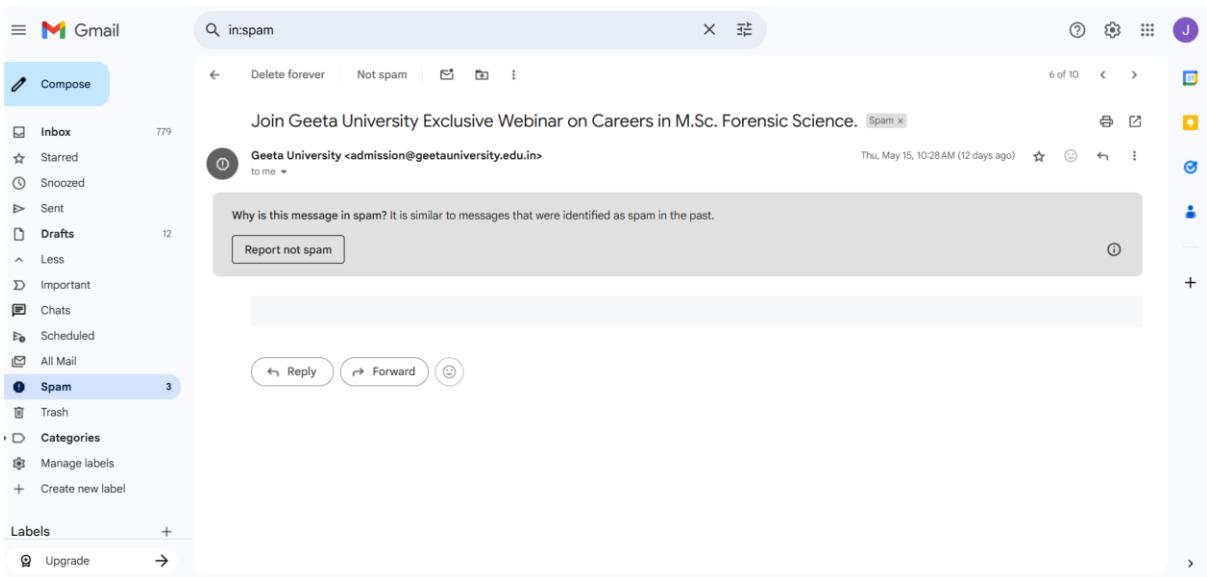
**7. Verify presence of spelling or grammar errors.**

Shown in Email	Real URL (on hover)	Suspicious?
<a href="https://gmail.com">https://gmail.com</a>	<a href="http://login-gmail.fake.ru/login.html">http://login-gmail.fake.ru/login.html</a>	<input checked="" type="checkbox"/> Yes

**A mismatched URL means:**

The **text you see** (like [www.bank.com](http://www.bank.com)) is different from the **actual destination** (like <http://malicious.ru/login>).

## 8. Summarize phishing traits found in the email



The email from Geeta University ([admissions@geetauniversity.edu.in](mailto:admissions@geetauniversity.edu.in)) found in your spam folder has some traits commonly associated with phishing or spam emails. Here are the whisking (spam/phishing-like) traits identified:

**1. Unsolicited Academic Offer:** The email promotes a webinar on M.Sc. Forensic Science without prior engagement, which is a common tactic in phishing to attract clicks.

**2. Generic Sender Address:** The sender email ([admission@geetauniversity.edu.in](mailto:admission@geetauniversity.edu.in)) may appear official but could be spoofed or mass-sent, leading Gmail to mark it as spam.

**3. Similarity to Past Spam:** Gmail specifically states that the message is "similar to messages that were identified as spam in the past."

**4. Marketing Style Subject:** The subject line (“Join Geeta University Exclusive Webinar...”) uses enticing words like “Exclusive” and “Careers,” which are often used in spam to lure users.

**5. No Personalization:** The message does not seem to be addressed personally, which is typical of mass-mail or phishing attempts.

**6. Spam Label by Gmail:** The presence in the Spam folder itself and the spam tag on the subject line strongly suggest it was flagged by Gmail’s automated filters.

THANK YOU