

# Phishing Email Investigation Report

SOC L1 Analyst Practice Exercise

## 1. Incident Summary

|                      |                                                         |
|----------------------|---------------------------------------------------------|
| Report Date          | 14 July 2026                                            |
| Analyst Name         | Rabya Hassan (SOC L1 Trainee)                           |
| Reported By / Source | Inbox review / proactive check                          |
| Email Subject        | "Validate your AI investment strategy at AWS re:Invent" |
| Sender Display Name  | Amazon Web Services                                     |
| Sender Address       | aws-marketing-email-replies@amazon.com                  |
| Recipient            | hassanrabya90@gmail.com                                 |
| Date/Time Received   | Tue, 14 Jul 2026 00:56:26 +0000                         |
| Classification       | TRUE NEGATIVE — Legitimate Marketing Email              |
| Severity             | None — no action required                               |

## 2. Email as Received

The email presents itself as an AWS re:Invent marketing/promotional message. Sender name and unsubscribe link are visible in the client view, which is typical of a legitimate bulk marketing send.

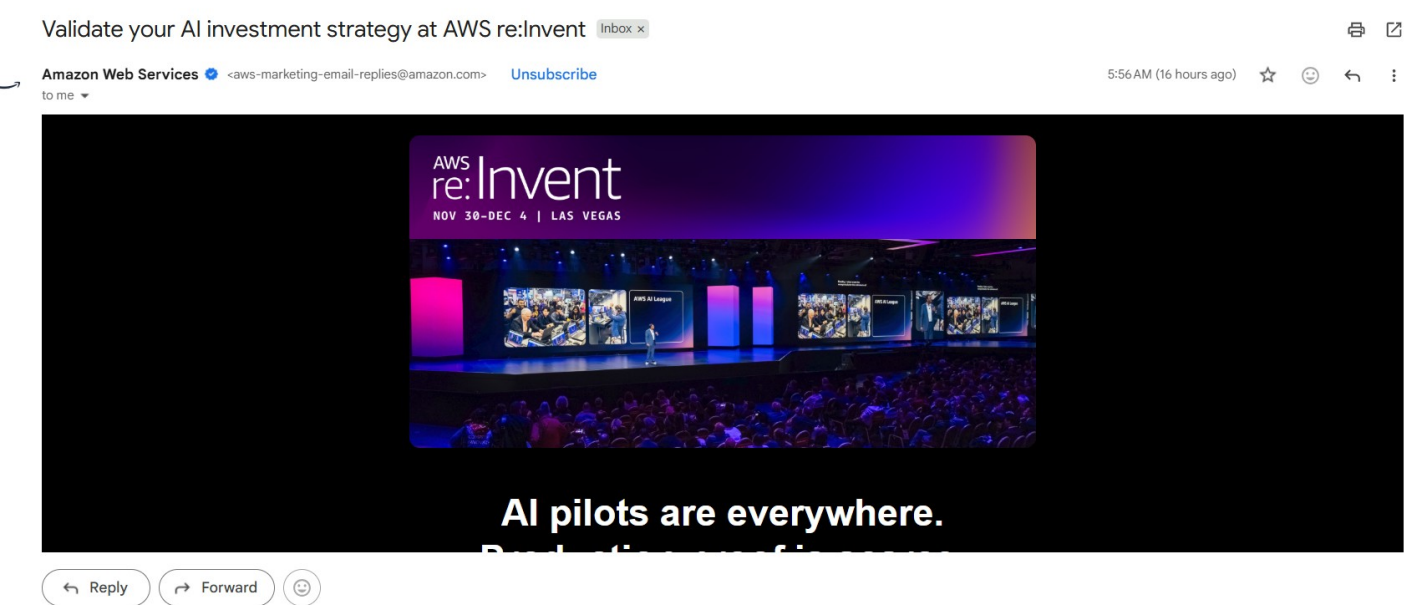


Fig 1 — Email as displayed in Gmail inbox

Headers were extracted and parsed using MXToolbox's Email Header Analyzer.

Fig 2 — Header analysis, part 1 (MXToolbox)

Received Header

Fig 3 — Header analysis, part 2 (MXToolbox)

|                   |                                                                                 |
|-------------------|---------------------------------------------------------------------------------|
| <b>SPF Result</b> | PASS — domain of ...@amazonses.com designates 54.240.48.139 as permitted sender |
|-------------------|---------------------------------------------------------------------------------|

|                     |                                                                               |
|---------------------|-------------------------------------------------------------------------------|
| <b>DKIM Result</b>  | PASS — two valid signatures: header.i=@amazon.com AND header.i=@amazonses.com |
| <b>DMARC Result</b> | PASS — p=QUARANTINE, header.from=amazon.com aligns                            |

Why this matters: all three checks passing together is the strongest technical signal of legitimacy available from headers alone. A spoofed "from amazon.com" email sent by an attacker's own infrastructure would almost always fail SPF and/or DKIM, because the attacker doesn't control Amazon's mail servers or Amazon's private DKIM signing key.

## 5. From / Reply-To / Return-Path Comparison

|                         |                                                                                                   |
|-------------------------|---------------------------------------------------------------------------------------------------|
| <b>From Address</b>     | aws-marketing-email-replies@amazon.com                                                            |
| <b>Reply-To Address</b> | aws-marketing-email-replies@amazon.com                                                            |
| <b>Return-Path</b>      | ...@amazonses.com (Amazon Simple Email Service — Amazon's own bulk mail infrastructure)           |
| <b>Do they match?</b>   | YES — all point back to Amazon-owned/operated domains, no third-party or lookalike domain present |

A phishing attempt impersonating AWS would typically show a Return-Path or Reply-To pointing to an unrelated free-mail address or a lookalike domain (e.g. amaz0n-support.com, aws-security-alert.net) — that mismatch is absent here.

## 6. Sending Infrastructure & Reputation

## 7. Embedded URL Analysis

The tracking/redirect link in the email body was extracted and submitted to VirusTotal rather than clicked directly.

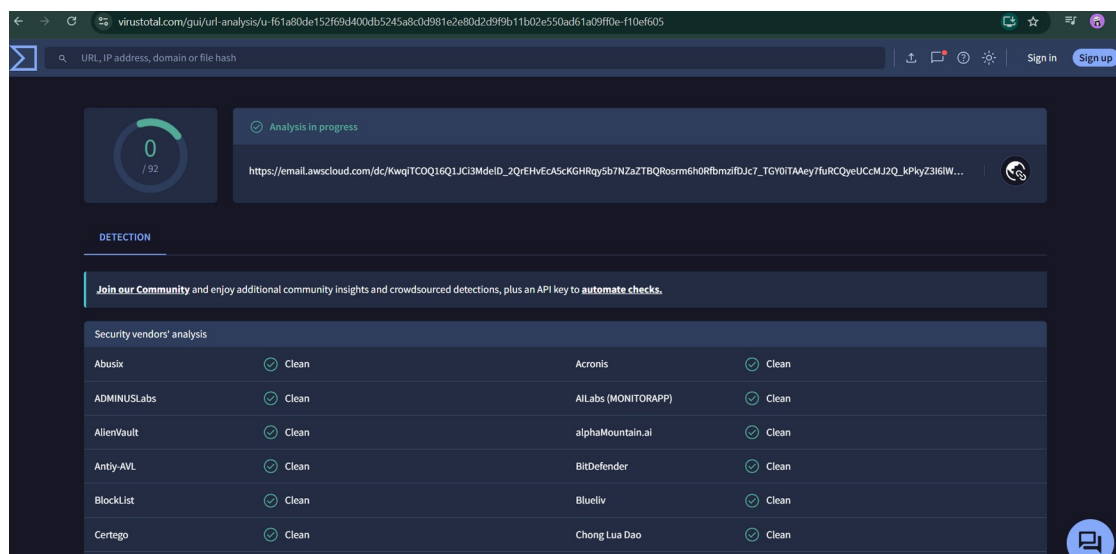


Fig 4 — VirusTotal URL scan result

|                           |                                                                                 |
|---------------------------|---------------------------------------------------------------------------------|
| <b>Scanned URL</b>        | https://email.awscloud.com/dc/KwqiTCOQ16Q1JCi3MdelD_...                         |
| <b>Hosting Domain</b>     | awscloud.com — an Amazon-owned/operated marketing-email domain, not a lookalike |
| <b>VirusTotal Verdict</b> | 0 / 92 security vendors flagged it — Clean                                      |

A malicious link disguised as an AWS notification would typically resolve to a domain with no relationship to amazon.com/awscloud.com, and would often show at least a handful of detections on VirusTotal, or be a freshly-registered domain.

## 8. Final Determination — Why This Is Legitimate

- ✓ SPF, DKIM, and DMARC all PASS and are aligned to amazon.com
- ✓ From, Reply-To, and Return-Path all resolve to Amazon-controlled infrastructure (amazon.com / amazonses.com)
- ✓ Sending IP belongs to Amazon SES, Amazon's own bulk-mail service
- ✓ Embedded link domain (awscloud.com) is Amazon-owned, not a lookalike/typosquat
- ✓ VirusTotal returned 0/92 detections on the link
- ✓ Standard, correctly-implemented List-Unsubscribe headers
- ✓ No urgency/threat language, no credential request, no attachment

**CONCLUSION:** This is a legitimate AWS re:Invent marketing email sent via Amazon's own SES infrastructure. No indicators of compromise, spoofing, or malicious content were found. No remediation action required — this can be classified as a false positive if it was flagged by any automated rule, or simply closed as benign if it was a proactive check.

## 9. For Comparison — What Would Make This a Phishing Email Instead?

Since the goal is learning to tell the two apart, here is what specific red flags in each of the same checks above would have flipped this to a TRUE POSITIVE phishing verdict:

### Authentication headers

- ✗ SPF = fail or softfail, especially while the From address still claims @amazon.com
- ✗ DKIM = fail, or a DKIM domain that doesn't match the From domain at all (e.g., signed by some unrelated domain)
- ✗ DMARC = fail — this is the strongest single red flag, since DMARC exists specifically to catch spoofed From addresses

### Sender / Reply-To / Return-Path

- ✗ Reply-To or Return-Path pointing to a free webmail address (Gmail, Yahoo) instead of a corporate domain
- ✗ A lookalike/typosquat domain: amaz0n.com, amazon-security.net, aws-billing-support.info, extra hyphens or added words
- ✗ Display name says "Amazon Web Services" but the actual email address is completely unrelated

## Sending infrastructure

✗ Sending IP has a poor reputation on AbuseIPDB, or belongs to a generic VPS/hosting provider instead of a known corporate mail service

## Links and attachments

✗ Embedded link resolves to a domain unrelated to the claimed sender (e.g., "AWS" email linking to a .ru or .xyz domain)

✗ VirusTotal shows any nonzero detections, or the domain was registered very recently (check via WHOIS)

✗ Unexpected attachment, especially macro-enabled Office files or password-protected zips

✗ URL uses a shortener (bit.ly, tinyurl) to hide the real destination

## Content / social engineering signals

✗ Urgency or threats: "your account will be suspended," "act within 24 hours"

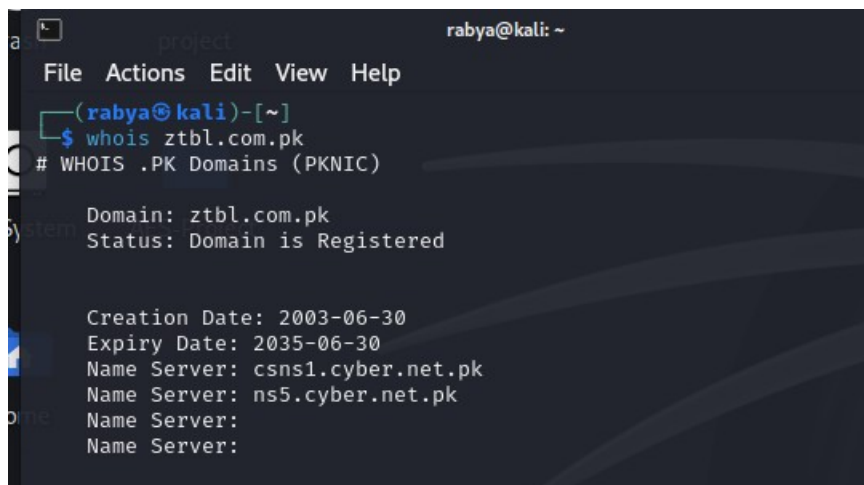
✗ Direct request for credentials, payment details, or MFA codes

✗ Generic greeting ("Dear Customer") instead of your actual name, on an email that should be personalized

✗ Grammar/spelling errors inconsistent with a professional organization's usual communications

## Rule of thumb for L1 triage

No single indicator alone is 100% proof either way — judge the totality. A passing SPF/DKIM/DMARC set is strong evidence of legitimacy, but a compromised legitimate account can still pass all three while sending a malicious link, so the URL/attachment checks in Steps 6–7 remain necessary even when authentication passes. Conversely, a single failed check isn't automatically malicious — some legitimate senders have misconfigured SPF — so always corroborate with at least 2–3 indicators before making a final call.

A terminal window on a Kali Linux system. The prompt is 'rabya@kali: ~'. The user has entered the command 'whois ztbl.com.pk'. The output shows WHOIS information for the domain ztbl.com.pk, including its creation and expiry dates and name servers.

```
File Actions Edit View Help
(rabya@kali)-[~]
$ whois ztbl.com.pk
# WHOIS .PK Domains (PKNIC)

Domain: ztbl.com.pk
Status: Domain is Registered

Creation Date: 2003-06-30
Expiry Date: 2035-06-30
Name Server: csns1.cyber.net.pk
Name Server: ns5.cyber.net.pk
Name Server:
Name Server:
```

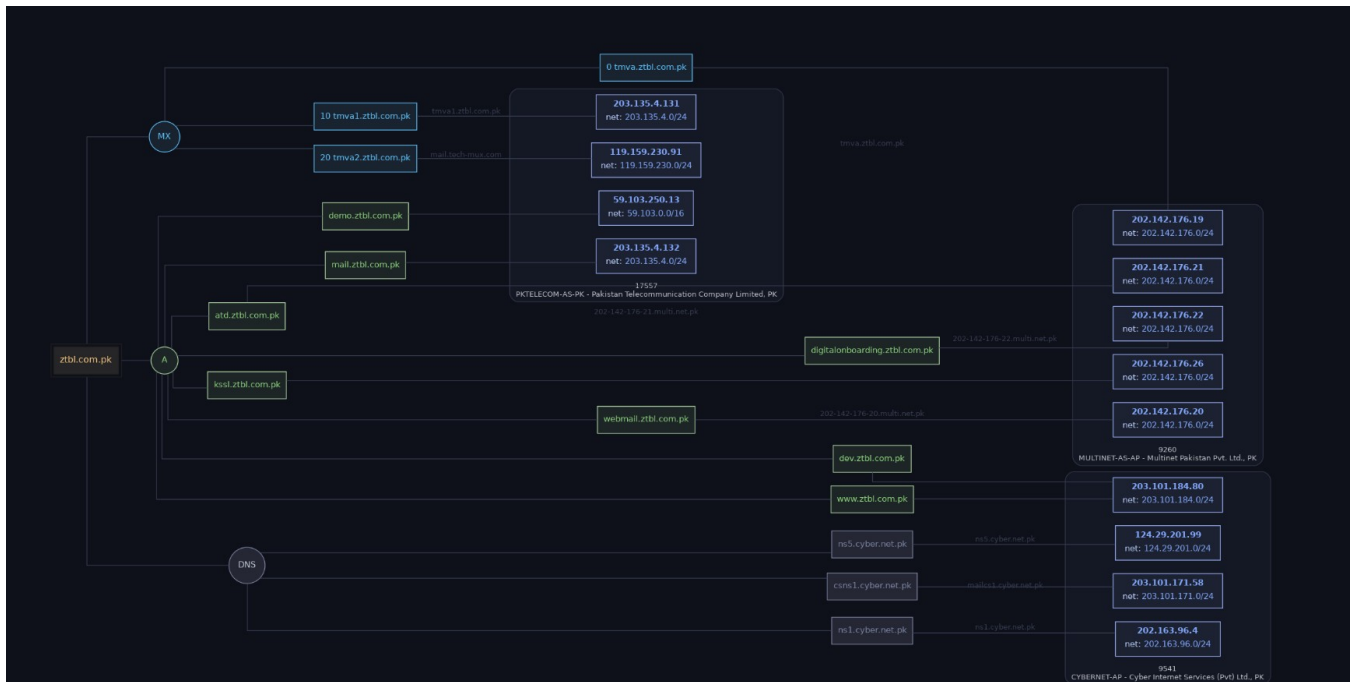
# ztbl.com.pk

Updated 1 day ago ↻



## Domain Information

|                |                                        |
|----------------|----------------------------------------|
| Domain:        | ztbl.com.pk                            |
| Registered On: | 2003-06-30                             |
| Expires On:    | 2035-06-30                             |
| Status:        | Domain is Registered                   |
| Name Servers:  | csns1.cyber.net.pk<br>ns5.cyber.net.pk |



| Pref   | Hostname                  | IP Address                                                                          | TTL          |                         |      |
|--------|---------------------------|-------------------------------------------------------------------------------------|--------------|-------------------------|------|
| Pref0  | Hostnametmva.ztbl.com.pk  | IP Address202.142.176.19<br>Multinet Broadband (AS9260)                             | TTL10<br>min | Blacklist Check<br>Test | SMTP |
| Pref10 | Hostnametmva1.ztbl.com.pk | IP Address203.135.4.131<br>Pakistan Telecommunication company limited<br>(AS17557)  | TTL10<br>min | Blacklist Check<br>Test | SMTP |
| Pref20 | Hostnametmva2.ztbl.com.pk | IP Address119.159.230.91<br>Pakistan Telecommunication company limited<br>(AS17557) | TTL10<br>min | Blacklist Check<br>Test | SMTP |

|                                                                                             | Test                     | Result                   |
|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
| Status<br> | NameDNS Record Published | ResponseDNS Record found |

|                                                                                               | Related Tests                | Result                                         |                                                                                               |
|-----------------------------------------------------------------------------------------------|------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Status<br>   | NameBIMI Record Published    | ResponseBrand Logo not appearing in inboxes    |  More Info |
| Status<br>   | NameDMARC Record Published   | ResponseDMARC Record found                     |                                                                                               |
| Status<br> | NameDMARC Policy Not Enabled | ResponseDMARC Quarantine/Reject policy enabled |                                                                                               |

[dns lookup](#)
[dns check](#)
[dmarc lookup](#)
[spf lookup](#)
[dns propagation](#)

Reported by **csns1.cyber.net.pk** on 7/15/2026 at **12:37:43 PM (UTC -5)**, [just for you](#). [Transcript](#)

Shodan

Maps

Images

Monitor

Developer

More...

☰

 SHODAN

hostname:ztbl.com.pk

🔍

TOTAL RESULTS

5

TOP PORTS

25

2

143

1

443

1

995

1

TOP ORGANIZATIONS

Multinet

Pakistan Pvt. Ltd.

4

Premium DSL on ISB Huawei BRAS-1

🏠 View Report

📖 View on Map

🔍 Advanced Search

Product Spotlight: A native desktop app to access Shodan using your API key. Fast and optimized for power users. Check out [Shodan Terminal](#)

203.135.4.131

2026-07-15T05:36:28.540771

tmva1.ztbl.com.pk

Premium DSL on ISB Huawei BRAS-1

🇵🇰 Pakistan, Rawalpindi

starttls

🔒 SSL Certificate

Issued By:

|- Common Name:

Go Daddy Secure Certificate Authority - G2

|- Organization:

GoDaddy.com, Inc.

Issued To:

|- Common Name:

\*.ztbl.com.pk

220 L1TMDDEI01.ztbl.com.pk

250-l1tmddei01.ztbl.com.pk

250-PIPELINING

250-SIZE 31457280

250-ETRN

250-STARTTLS

250-ENHANCEDSTATUSCODES

250-8BITMIME

250-DSN

250 CHUNKING

on ISB  
Huawei  
BRAS-1  
1

250-DSN  
250 CHUNKING

**202.142.176.19**

tmva.ztbl.com.pk  
Multinet Pakistan Pvt. Ltd.  
🇵🇰 Pakistan, Wah Cantt

starttls

2026-07-14T17:16:27.911866

 **SSL Certificate**

Issued By:  
|- Common Name:  
Go Daddy Secure Certificate Authority - G2  
  
|- Organization:  
GoDaddy.com, Inc.

Issued To:  
|- Common Name:  
\*.ztbl.com.pk

220 L1TMDDEI01.ztbl.com.pk  
250-l1tmddei01.ztbl.com.pk  
250-PIPELINING  
250-SIZE 31457280  
250-ETRN  
250-STARTTLS  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250-DSN  
250 CHUNKING

**202.142.176.20**

202-142-176-20.multi.net.pk  
ztbl.com.pk  
Multinet Pakistan Pvt. Ltd.  
🇵🇰 Pakistan, Wah Cantt

2026-06-26T03:55:23.794290

 **SSL Certificate**

Issued By:  
|- Common Name:  
Go Daddy Secure Certificate Authority - G2  
  
|- Organization:  
GoDaddy.com, Inc.

Issued To:  
|- Common Name:  
\*.ztbl.com.pk

TECHNOLOGIES

MORE INFO

↓ Export

CMS

 [WordPress](#)

Analytics

 [Google Analytics](#) GA4

Blogs

 [WordPress](#)

Video players

 [Vimeo](#)

Security

 [reCAPTCHA](#)

Font scripts

CDN

 [Cloudflare](#)

 [Unpkg](#)

 [jsDelivr](#)

 [cdnjs](#)

Databases

 [MySQL](#)

Tag managers

 [Google Tag Manager](#)

JavaScript libraries

 [Select2](#)



[reCAPTCHA](#)

#### Font scripts



[Font Awesome](#) 6.5.2

#### Web servers



[Apache HTTP Server](#)

#### Programming languages



[PHP](#)

#### JavaScript libraries



[Select2](#)



[lit-html](#) 3.3.2



[lit-element](#) 4.2.2



[jQuery](#) 3.6.1



[DataTables](#) 1.10.23



[AOS](#)

#### UI frameworks



[Bootstrap](#) 3.3.7

#### Performance



[Priority Hints](#)

[Something wrong or missing?](#)

**See website technologies in your CRM**



Add website technology data to HubSpot, Salesforce, or