Phishing Email Detection (MY Findings)

1. The Fake phishing Email:

Return-Path: <security-alert@novacloud-check.net>

Received: from mail.secureline-bh.net (mail.secureline-bh.net. [185.199.48.22])

by mx.google.com with ESMTPS id a9si2387123qkg.190.2025.11.14.07.33.10

for <arun.sharma@gmail.com>

(version=TLS1_2 cipher=ECDHE-RSA-AES256-GCM-SHA384);

Fri, 14 Nov 2025 07:33:10 +0530

Received-SPF: fail (google.com: domain of novacloud-check.net does not designate 185.199.48.22 as permitted sender) client-ip=185.199.48.22;

Authentication-Results: mx.google.com;

spf=fail (domain of novacloud-check.net does not allow this server)

dkim=none (message not signed)

dmarc=fail (p=reject) header.from=novacloud-check.net

Received: by mail.secureline-bh.net (Postfix, from userid 1002)

id 8HSJ5932; Fri, 14 Nov 2025 04:02:48 +0300 (AST)

Date: Fri, 14 Nov 2025 04:02:38 +0300

From: NovaCloud Security <security-alert@novacloud-check.net>

Reply-To: accounthelp@protonmail.com

To: arun.sharma@gmail.com.com

Message-ID: <20251114040238.GA59231@mail.secureline-bh.net>

Subject: ⚠️ Security Alert: New sign-in detected on your NovaCloud account

MIME-Version: 1.0

Content-Type: text/html; charset="UTF-8"

X-Originating-IP: 185.199.48.22

X-Mailer: PHPMailer 5.2.22

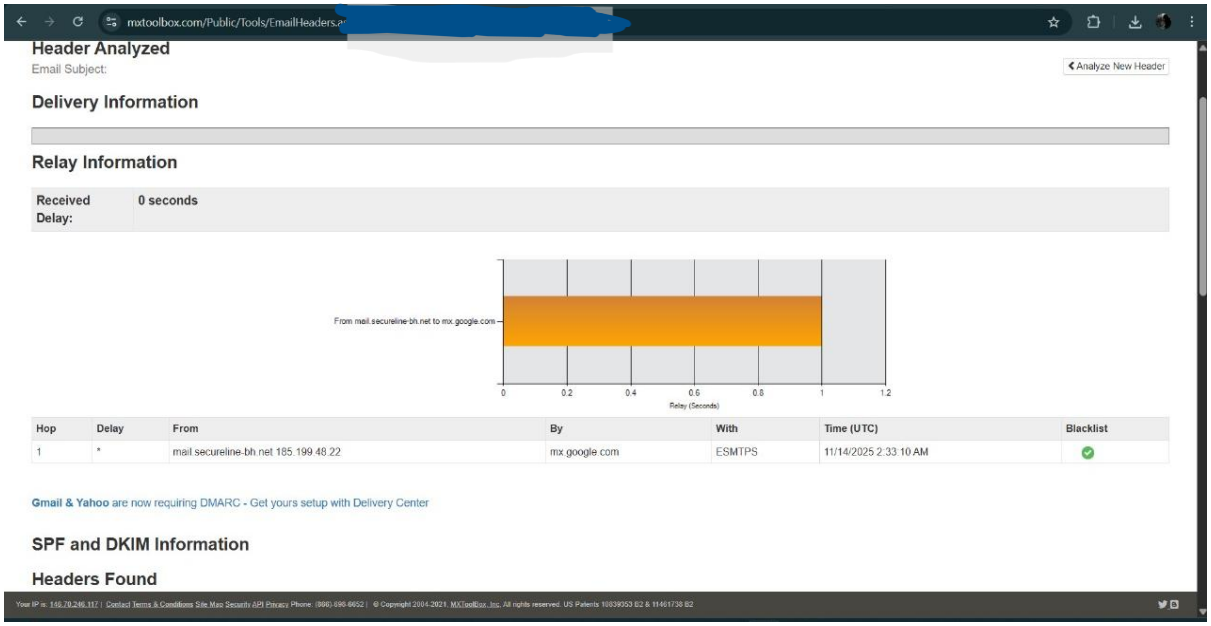

Fig.1 Results Using MX tool box

The Email Got Blacklisted and Now we try the same analysis with a legit email.

2. Legit Email:

GPTZero: Your monthly subscription limit is approaching

1 message

<team@optzero.

To: vaxxxxxxx@gmail.com

Hi x,

Wed, 5 Nov 2025 at 20:01

Thank you for being a supporter of GPTZero.

We would like to inform you that you've now exceeded 80% of your monthly words are currently on the Free plan, which allows you to analyze 10,000 words per month. Your plan and usage will renew on 02-Dec-2025.

upgrade avoie limit a e using GPTZero. You can reference the plan page: kisting upgrade options.

Best regards,

The GPTZero Team

Since its legit I cannot disclose the email header…

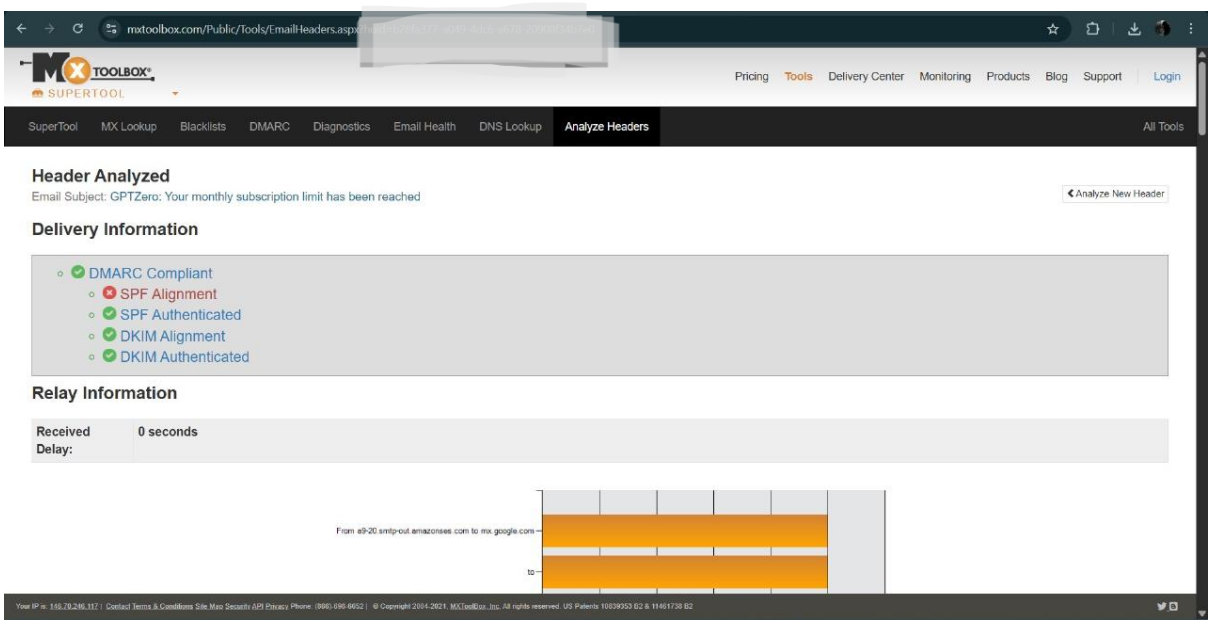

Fig 2.1 Legit email Results

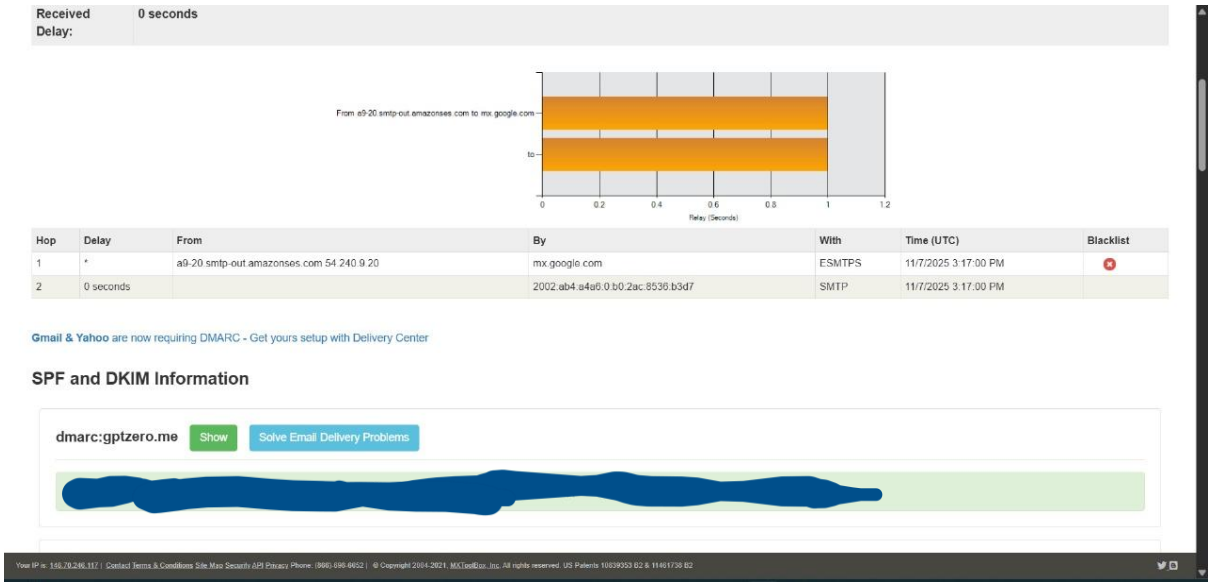

Fig 2.2 Legit Email Results

3. Table Of the Results

Feature	**Real Email**	**Fake Email**
Sender Server	Amazon SES	Unknown VPS
SPF	Pass	Fail / Missing
DKIM	Pass	None
DMARC	Configured	Missing / fail
Blacklist	Possibly flagged but trusted	Actively blacklisted

Feature	Real Email	Fake Email
Routing	Clean, legitimate	Suspicious, direct server
Domain Trust	High	Very low

4. Summary:

This project involved comparing a fraudulent email against a legitimate baseline, using an 8-step analysis workflow to identify technical and social engineering flaws.

- **Tools Used:** Online Header Analyzer (e.g., MXToolbox) and manual content review.
- **Key Finding:** The phishing email failed all technical security checks.
- **Analysis:**
    - **Technical:** The email **failed SPF, DKIM, and DMARC** authentication protocols, confirming it was spoofed and unauthorized. The sender IP was verified to be on a **Blacklist**.
    - **Social Engineering:** The email used **high-urgency language** ("Immediate Action Required") and contained **mismatched, fraudulent URLs** and poor grammar (Tasks 5, 6, 7).
- **Conclusion:** The email was definitively identified as a **malicious phishing attempt** due to the complete failure of email authentication combined with clear social engineering tactics.
- **Documentation:** The final findings, including a detailed comparison table of authentication results, were prepared.