Phishing Email Header Analysis Report

Date: 25 June 2025

Analyst: Suyash Nalawade

Tool Used: MXToolbox Email Header Analyzer

Objective

To analyze the header of a potentially suspicious email to identify phishing indicators based on SPF, DKIM, DMARC checks, sender IP, and domain information.

Email Header Analysis Summary

The following results were obtained from the MXToolbox header analysis tool:

Parameter	Result
SPF (spf1.pd.sender-elb.com)	❌ FAIL
SPF (spfreceiver.pd.sender)	❌ FAIL
DMARC	✅ PASS – Policy: quarantine
DKIM (getresponse.frmail)	✅ PASS (signature failed in one case)
Sender IP	77.32.148.62 (not blacklisted)
Return-Path	bounce@getresponse.frmail.it
Delivered-To	audxxxxxx@gmail.com

Conclusion

The email failed SPF checks, indicating it may have been sent from a server not authorized by the domain. Although DKIM and DMARC passed, the mixed authentication results suggest caution. Further analysis of the email content is necessary to verify phishing intent.