


# Phishing Email Header Analysis Report

This report contains screenshots of a phishing email's header analysis using Google Admin Toolbox. The analysis helps detect spoofed sender information and failed authentication checks such as SPF, DKIM, and DMARC.

# Screenshot 1: Raw Email Header Input



Google Admin Toolbox Messageheader

Return-Path: <support@amz-check.com>  
Received: from unknown (HELO smtp.randommailserver.com) (192.168.1.22)  
by mail.example.com with SMTP; Wed, 06 Aug 2025 14:35:21 +0000  
Received-SPF: Fail (mail.example.com: domain of amz-check.com does not designate 192.168.1.22 as permitted sender)  
Authentication-Results: mail.example.com;  
spf=fail (sender IP is 192.168.1.22) smtp.mailfrom=support@amz-check.com;  
dkim=none header.d=amz-check.com;  
dmarc=fail action=quarantine header.from=amz-check.com  
From: Amazon Support <support@amz-check.com>  
Subject: Important: Your Account Has Been Suspended  
To: victim@example.com  
Date: Wed, 06 Aug 2025 14:35:20 +0000  
Message-ID: <fake-id@amz-check.com>  
MIME-Version: 1.0

ANALYZE THE HEADER ABOVE

## Screenshot 2: Header Analysis Results

MessageId	fake-id@amz-check.com
Created at:	8/6/2025, 8:05:20 PM GMT+5:30 ( Delivered after 1 sec )
From:	Amazon Support <support@amz-check.com>
To:	victim@example.com
Subject:	Important: Your Account Has Been Suspended
SPF:	fail with IP Unknown! <a href="#">Learn more</a>
DKIM:	none <a href="#">Learn more</a>
DMARC:	fail <a href="#">Learn more</a>

#	Delay	From *	To *	Protocol	Time received
0	1 sec	unknown	→ mail.example.com	<a href="#">SMTP</a>	8/6/2025, 8:05:21 PM GMT+5:30

ANALYZE ANOTHER HEADER