Phishing Email Analysis Report

Email Subject: Urgent: Suspicious Activity Detected On Your Account
From: PayPal Support <support@security-paypa1.com>
Date Received: August 5, 2025

Phishing Indicators Found:

Indicator	Description
Spoofed Email Address	Uses paypa1.com instead of legitimate paypal.com
Urgent and Threatening Language	Pressure to act within 24 hours
Suspicious Link	https://paypal-security-check.tk/verify not related to PayPal
Generic Greeting	‘Dear Customer’ is not personalized
Header Discrepancies	SPF and DKIM failed; IP mismatch
Free Domain Usage	Uses .tk which is common in scams
No Account Info	No specific account or personal details given

Conclusion:
This is a phishing email attempting to steal user credentials by imitating PayPal. It uses urgency, a spoofed email, fake links, and vague language. The sender's domain is suspicious, the URL does not match PayPal’s domain, and the headers show failed authentication. This email should be reported and deleted immediately.

Tools Used:
- Sample phishing email (hand-crafted)
- MXToolbox Header Analyzer
- Manual inspection for URLs and language