Phishing Email Analysis Report

This report analyzes a sample phishing email and highlights key indicators such as spoofed sender address, header mismatches, malicious links, and social engineering content.

1. Sample Email Summary

A suspicious email pretending to be from PayPal was analyzed. The sender address contained a spoofed domain, and the email attempted to create urgency.

2. Header Analysis Findings

SPF = FAIL DKIM = FAIL Return-Path mismatch IP does not belong to PayPal. These are strong indicators of spoofing.

3. Link Analysis

Visible link: https://paypal.com/login Actual redirect: http://malicious-site.ru/paypal-login This confirms malicious intent.

4. Content Red Flags

Urgent language, grammar errors, threats of account suspension, and a fake login button were observed.

5. Conclusion

This email is confirmed phishing. It uses spoofing, social engineering, and malicious links to steal user credentials.