Cybersecurity Case Report

Email Legitimacy & Infrastructure Validation Investigation

Analyst: Zuri

Date Investigated: February 22, 2026

---

1. Executive Summary

A benefits open enrollment email was flagged as potentially malicious due to sender formatting and embedded HTTP links. A structured multi-layer investigation was conducted including WHOIS analysis, DNS resolution, TLS certificate validation, HTTP header inspection, and SPF/DKIM/DMARC authentication review.

Final Determination: The email and associated domain were authenticated and legitimate. No indicators of phishing, spoofing, or malicious infrastructure were identified.

2. Initial Indicators of Suspicion

- Campaign-style sender address format
- Embedded HTTP link
- Marketing-style bulk distribution appearance
- Branding mismatch concerns

3. Investigation Methodology & Findings

WHOIS Analysis

Domain created December 13, 2004. Registered via GoDaddy. Active registration through 2028. Long-standing domain history reduces likelihood of phishing throwaway domain.

DNS Resolution

Domain resolved to Cloudflare IP addresses (104.18.x.x range). Stable DNS resolution with no fast-flux behavior.

HTTP Header Inspection

301 redirect from HTTP to HTTPS. Secure and HttpOnly cookies present. No malicious redirect chains observed.

TLS Certificate Validation

Valid Let's Encrypt certificate. Modern ECC cryptography (SHA384). SAN includes wildcard and base domain. No certificate anomalies detected.

Email Authentication (SPF/DKIM/DMARC)

SPF: PASS. DKIM: PASS. DMARC: PASS. Sending IP authorized. Message integrity verified. No spoofing indicators identified.

4. Risk Reclassification

- Initial Assessment: Medium–High Risk
- Post-WHOIS & DNS Analysis: Medium Risk
- Post-TLS Validation: Low Risk
- Post-SPF/DKIM/DMARC Validation: Very Low Risk
- Final Determination: Legitimate Enrollment Communication

5. Skills Demonstrated

- Domain OSINT analysis
- DNS and IP infrastructure investigation
- CDN identification and HTTP header inspection
- TLS certificate validation and cryptographic review
- SPF/DKIM/DMARC authentication analysis
- Risk classification and incident documentation

Prepared as part of Zuri's Cybersecurity Portfolio – 2026