INCIDENT REPORT – PHISHING ATTACK ANALYSIS

Incident Overview

Incident Type: Phishing / Social Engineering
Detection Source: Email Security (User-Reported)
Email Platform: Yahoo Mail (Delivered via Gmail infrastructure)
Severity: Medium (Escalates to High upon user interaction)
Status: Contained (No user interaction detected)

Executive Summary

A phishing email impersonating a legitimate organization was received by the user. The attacker used a real domain (`pbs.ac.th`) and Google mail infrastructure to increase trust and bypass basic email filtering. Although no malicious link or attachment was present initially, the email was designed to initiate conversation and later deliver malicious payloads or conduct financial fraud. The email was identified through manual inspection and raw header analysis before any user interaction occurred, preventing escalation.

Email Details

From Name:
Recipient Type: BCC (Undisclosed recipients)
Content Type: Plain text + HTML (Social engineering)
Subject: Good Morning
Recipient Type: BCC (Undisclosed recipients)
Content Type: Plain text + HTML (Social engineering)

Header & Authentication Analysis

Authentication Results

- **SPF:** None (Domain does not authorize sending IPs)
- **DKIM:** Pass (Signed using Google DKIM)
- **DMARC:** Unknown (No enforcement policy)

Finding:
DKIM pass alone does not confirm legitimacy. The absence of SPF and DMARC allows spoofed emails to be delivered.

Email Path Analysis

Source IP	Destination
209.85.219.66	Gmail Mail Server
Gmail	Yahoo Mail Server

Finding:

Email originated from Gmail infrastructure, commonly abused for phishing campaigns due to reputation trust.

Domain & Infrastructure Analysis

Domain WHOIS

- **Domain:** pbs.ac.th
- **Registered Since**: 2002
- **Status:** Active
- **Nameservers:** Cloudflare

Finding:
Legitimate domain likely compromised or misused via free email services.

IP Reputation Analysis

AbuseIPDB

- **Reports:** 737
- **Confidence of Abuse:** 73%
- **Categories:** Email Spam, Brute Force, Port Scan

VirusTotal

- **Community Score:** 0/95
- **Observation:** Known Google infrastructure; reputation varies based on usage

Finding:
Shared infrastructure means abuse must be correlated with behavior, not IP alone.

Attack Technique Mapping (MITRE ATT&CK)

Phishing	T1566
Social Engineering	T1204

Potential Attack Progression (If User Responded)

- Attacker builds trust through conversation
- Malicious attachment or phishing link delivered
- User executes payload
- Encoded PowerShell execution
- Possible malware deployment or credential theft

SOC Response Actions

- Email identified and analyzed
- User advised not to reply
- Sender blocked
- Indicators documented
- Awareness reinforced

Final Verdict

Conclusion:

This was a real-world phishing attempt leveraging trusted infrastructure and social engineering. Although technically authenticated (DKIM pass), the email exhibited multiple red flags including reply-to mismatch, missing SPF/DMARC, generic content, and mass targeting via BCC. Early detection prevented progression to malware delivery or financial fraud.