Phishing Email Analysis Report

Cyber Security Internship - Task 2

Analyst: Pranav Suryawanshi
Date: September 23, 2025

Objective:

The objective of this task was to identify phishing characteristics in a suspicious email sample to enhance awareness of phishing tactics and improve skills in email threat analysis.

Sample Email Overview:

The suspicious email was purportedly sent from "REV. MATT PATTERSON" under the domain mrcm.ru. The email subject was "LOAN," offering financial loan services at unusually low interest rates. The sender's email address and message content raised several red flags indicating potential phishing behavior (See Screenshot 1).

Phishing Indicators Identified:

1. Sender Spoofing

- The sender's email address ("v****v@mrcm.ru") looks suspicious as the domain "mrcm.ru" is uncommon and not related to any known legitimate financial institution.
- The use of a free email provider in the forwarded message signals possible spoofing (e.g., l**********7@gmail.com) indicating the email could be forwarded or manipulated (See Screenshot 3).

2. Suspicious Email Content

- The message contains poor grammar and awkward phrasing, often found in phishing attempts.
- The email uses urgent language enticing recipients to act quickly for refinancing their home with 2% interest, a suspiciously low offer that is uncommon (See Screenshot 1).

3. Email Header Discrepancies

- Analysis of the email headers using an online EML analyzer revealed suspicious domain activity:
- Links with suspicious Top-Level Domain (TLD) "mrcm.ru".
- Low reputation of sender's domain flagged.
- Message-ID and sender domain registrar inconsistencies hint at possible forgery.

- The header inspection confirms signs of Business Email Compromise (BEC) tactics such as reply thread hijacking (See Screenshot 2 and 3).

4. Threat Intelligence and VirusTotal Scan

- VirusTotal scan flagged the email file with an alert for HTML phishing.
- Although only 1 out of 63 security vendors flagged this, the specific detection was "Suspected of HTML Phishing" (See Screenshot 4).
- Multiple security vendors reported no detection, but caution recommends treating this mail as malicious.

Summary of Findings:

Attribute	**Observation**	**Conclusion**
Sender email domain	mrcm.ru (suspicious TLD and spoofed)	Suspicious
Content quality	Poor grammar and urgent language	Phishing characteristic
Header anomalies	Hijacked reply thread, suspicious domains	Indicative of phishing
VirusTotal and detection	1/63 flagged as "HTML Phishing"	Likely malicious

Conclusion:

The email analyzed displays multiple strong indicators of phishing, including sender spoofing, suspicious URLs, malicious attachments, phishing language, and header anomalies consistent with advanced email threats like Business Email Compromise. Receiver vigilance against such threats is critical.