Introduction

This report analyses a suspicious email sample to identify potential phishing characteristics. Phishing is a cyberattack method where attackers impersonate legitimate entities to steal sensitive information such as login credentials, credit card details, or personal data. The goal of this analysis is to highlight the indicators of phishing in the email sample.

Phishing Indicators Identified

1. Sender's Email Address Spoofing

- The sender's email address appeared to mimic a legitimate organization (e.g., support@legit-company.com), but upon closer inspection, it contained subtle discrepancies (e.g., support@legit-companyy.com with an extra "y").
- The domain did not match the official domain of the claimed organization.

2. Email Header Discrepancies

- Analysis using an online email header analyzer revealed inconsistencies:
  - The "Return-Path" did not align with the "From" address.
  - The email originated from an IP address associated with a known suspicious location or hosting provider.

3. Suspicious Links

- The email contained hyperlinks with mismatched URLs. For example:
  - Display text: Click here to update your account
  - Actual URL: http://malicious-site.com/login (hovering revealed a non-legitimate domain).
- The links used HTTP instead of HTTPS, indicating a lack of encryption.

4. Urgent or Threatening Language

- The email body used alarming language to create a sense of urgency, such as:
  - "Your account will be suspended within 24 hours unless you verify your details."
  - "Immediate action required to avoid penalties."

5. Spelling and Grammar Errors

- The email contained noticeable spelling and grammatical mistakes, such as:
  - "Dear Costumer" instead of "Dear Customer."

    - "We detected an unusual activity" instead of "unusual activity."

6. Unusual Attachments

- The email included an unexpected attachment (e.g., an invoice or document) with a suspicious file extension (e.g., .exe, .zip).

7. Request for Sensitive Information

- The email asked for personal or sensitive information, such as passwords, Social Security numbers, or credit card details, which legitimate organizations typically do not request via email.

8. Generic Greetings

- The email used a generic greeting like "Dear User" or "Dear Valued Member" instead of addressing the recipient by name.

Summary of Phishing Traits

The email exhibited multiple red flags commonly associated with phishing attempts, including:

- Spoofed sender address.
- Mismatched or suspicious links.
- Urgent or threatening language.
- Poor spelling and grammar.
- Requests for sensitive information.

These traits indicate a high likelihood that the email was a phishing attempt designed to deceive the recipient into divulging personal information or downloading malicious content.

Tools Used

1. **Online Email Header Analyzer**: Used to inspect the email headers for inconsistencies.
2. **URL Inspection**: Hovered over links to reveal actual URLs.
3. **Manual Review**: Analyzed the email content for language, tone, and grammatical errors.

Recommendations

1. **Do Not Click Links or Download Attachments**: Avoid interacting with any links or attachments in suspicious emails.
2. **Verify the Sender**: Contact the organization directly using official contact details to confirm the email's legitimacy.
3. **Report Phishing Attempts**: Forward the email to your IT security team or the appropriate authority (e.g., Anti-Phishing Working Group).
4. **Educate Yourself and Others**: Stay informed about common phishing tactics to recognize and avoid future attempts.

Conclusion

Phishing emails often rely on social engineering tactics to exploit human psychology. By identifying the indicators outlined in this report, users can better protect themselves from falling victim to such attacks. Vigilance and skepticism are key when evaluating unsolicited or suspicious emails.