Phishing Email Analysis Report

Internship Task 2 - Cybersecurity

Objective

To analyze a sample phishing email and identify characteristics that indicate it is a phishing attempt. This task enhances awareness of phishing tactics and email threat analysis skills.

Sample Phishing Email

```
From: PayPal Support <support@secure-paypal.com>
Subject: Urgent Action Required - Account Suspended

Dear Customer,

We noticed suspicious activity in your PayPal account. As a precautionary measure, we have temporarily suspended your account access.

To restore your access, please verify your identity by clicking the link below:

[Verify Now](http://secure-paypal-login.com/verify)

Failure to verify within 24 hours will result in permanent account suspension.

Thank you for your attention,
PayPal Support Team

Attachment: PayPal_Statement.pdf.exe
```

Phishing Indicators & Flaws Identified

1. Spoofed Sender Email

- Email Used: support@secure-paypal.com

- Legitimate Domain: @paypal.com

- Explanation: Attackers often use similar-looking domains to trick users. secure-paypal.com is not an official PayPal domain.

2. Urgent and Threatening Language

- Phrase Used: ?Failure to verify within 24 hours will result in permanent account suspension.?

- Explanation: Phishing emails use urgency or fear to prompt quick, irrational action.

3. Suspicious Link

- Displayed Text: Verify Now

- Actual URL: http://secure-paypal-login.com/verify

- Legitimate URL: Should be https://www.paypal.com

- Explanation: Hovering over the link reveals a malicious domain, a common phishing trick.

4. Dangerous Attachment

- Filename: PayPal_Statement.pdf.exe

- Explanation: File appears to be a PDF but is actually an executable file. This can install malware if opened.

5. Generic Greeting

- Used Greeting: ?Dear Customer?

- Explanation: Legitimate companies usually personalize emails with your name. Generic greetings are common in mass phishing emails.

6. Poor Grammar or Spelling

- Errors Found: None in this example, but this is a frequent indicator in other phishing attempts.

Header Analysis (Optional - For Advanced Detection)

Using tools like MxToolbox Email Header Analyzer, you can inspect:

- Return path mismatch

- SPF/DKIM/DMARC failures

- IP address origin and geolocation

Conclusion

This phishing email contains multiple red flags:

- Suspicious sender domain

- Urgent tone

- Malicious links and attachments

- Lack of personalization

Recognizing these characteristics can help users avoid falling victim to phishing attacks.

Recommendations

- Never click on links or download attachments from unknown sources.

- Always check sender domains and URLs carefully.

- Enable multi-factor authentication (MFA) for additional protection.

- Report suspected phishing emails to your IT or security team.