Phishing Email Analysis Report

Objective:

To identify phishing characteristics in a suspicious email sample using email headers, body content, and embedded elements.

Sample Email (Text Format):

From: PayPal
To: uday.bhale@example.com
Subject: Urgent: Your Account Has Been Suspended

Dear Customer,

We have noticed suspicious activity on your PayPal account. For your security, we have temporarily suspended your account.

To restore access, please verify your account immediately by clicking the link below:
https://paypal-verification.secure-update-login.com

Failure to act within 24 hours will result in permanent suspension of your PayPal account.

Thank you,
PayPal Security Team

Attachment: AccountVerificationForm.exe

Header Analysis:

Indicator	Evidence
Spoofed Email Address	support@paypalsecure.com (not from paypal.com)
Failed SPF/DKIM	Email failed authentication checks
Return Path/IP	Return-Path: suspiciousmail.ru (not PayPal)

Body Content Analysis:

• Uses urgency and threat: 'Failure to act within 24 hours...'
• Emotional manipulation to prompt immediate action
• Generic salutation: 'Dear Customer' instead of the user's name

Link Inspection:

URL shown: https://paypal-verification.secure-update-login.com
URL is not owned by PayPal, uses deceptive subdomains.

Attachment Check:

Attachment: AccountVerificationForm.exe
.exe file can execute malicious code. No real company asks for verification via executables.

Summary of Phishing Traits Found:

Trait	Evidence
Spoofed Email Address	Fake domain: paypalsecure.com
Failed SPF/DKIM	Header analysis failure
Deceptive URL	Does not belong to PayPal
Urgency/Threat Language	Pressure to act within 24 hours
Generic Greeting	No personalization
Malicious Attachment	.exe file present
Grammar Issues	Minor formatting/language problems

Conclusion:

This email is a clear phishing attempt intended to steal credentials or install malware. Do not click any links or open the attachment.

Recommended Actions:

• Report the email to your email provider and PayPal (phishing@paypal.com).
• Do not click any links or open any attachments.
• Educate others on how to spot phishing emails.