Phishing Email Analysis Report

1. Sample Phishing Email

Subject: Urgent: Your Account Has Been Suspended
From: support@paypall.com
To: you@example.com
Body:
Dear Customer,
We detected unusual activity on your PayPal account.
Please verify your account immediately by clicking the link below, or your account will be permanently suspended.
Verify Now
Failure to do so will result in permanent loss of access.
Thank you,
PayPal Security Team
Attachment: AccountVerificationForm.exe

2. Sender Spoofing

The sender email 'support@paypall.com' mimics a legitimate address but contains a typo (extra 'l').

3. Email Header Check

Headers show the email was sent from an untrusted server (e.g., smtp-random.ru), and SPF/DKIM failed.

4. Suspicious Links/Attachments

The link uses a Bit.ly shortener to disguise its true destination. Attachment is a '.exe' file, which is highly risky.

5. Urgent Language

Phrases like 'immediately' and 'permanently suspended' are used to scare the user into action.

6. Mismatched URLs

Hovering over the 'Verify Now' link shows a different destination than what is displayed.

7. Grammar/Spelling Errors

The email contains typos such as 'PayPall' and has awkward phrasing, which is unprofessional.

8. Summary of Phishing Traits

Trait	Description
Spoofed Email Address	support@paypall.com mimics a real domain
Header Discrepancies	Sent from suspicious mail server, SPF/DKIM failed

Suspicious Links	Bit.ly used to mask destination
Executable Attachment	.exe file likely carries malware
Urgent Language	Uses scare tactics like account suspension
Mismatched URLs	Hover shows different URL than displayed
Grammar Errors	Multiple language and formatting issues