To: All Employees and Stakeholders

From: IT Security/Compliance Department

Date: [Insert Date]

Subject: Compliance Notification: Cybersecurity Threat Awareness and Phishing Defense

Dear Team,

This letter serves as a formal notice regarding our mandatory cybersecurity compliance requirements. To ensure the protection of company data and maintaining regulatory standards, all personnel must adhere to the following threat awareness and phishing defense strategies.

1. Identification of Phishing Threats

Employees are required to scrutinize all incoming emails for the following red flags:

- Generic greetings and urgent, threatening language.
- Discrepancies between the sender's display name and the actual email address.
- Unusual requests for sensitive information or financial transactions.
- Suspicious attachments or links that do not match the destination URL when hovered over.

2. Defense and Prevention Protocols

To mitigate risks, the following protocols are now in effect:

- **Verification:** Use an alternative communication channel (phone call or chat) to verify any internal request for sensitive data or wire transfers.
- **Multi-Factor Authentication (MFA):** MFA must be enabled on all company-related accounts without exception.
- **Reporting:** Any suspicious email must be reported immediately using the "Report Phishing" button or by forwarding it to [Insert Security Email Address].

3. Compliance Training Requirements

Completion of the quarterly Security Awareness Training module is mandatory. Failure to complete the training by [Insert Deadline] will result in a notification to management and temporary suspension of network access until the requirement is met.

Maintaining a secure environment is a collective responsibility. By following these strategies, we protect our clients, our colleagues, and our organization from evolving cyber threats.

Regards,

[Insert Name/Signature]
[Insert Title]
[Insert Company Name]