To: All Banking Staff

From: IT Security Department / Management

Date: [Insert Date]

Subject: Letter of Instruction: Phishing Identification and Cyber Threat Reporting

Dear Team,

To ensure the security of our financial assets and client data, all staff members are required to adhere to the following instructions regarding email security and threat reporting.

1. Identification of Phishing Attempts

Before interacting with any email, verify the following indicators of a phishing attempt:

- **Sender Address:** Check for misspellings or domains that do not match official company records.
- **Urgent Language:** Be wary of emails creating a false sense of urgency or threatening account suspension.
- **Suspicious Links:** Hover over links to view the actual destination URL before clicking.
- **Unexpected Attachments:** Do not open attachments from unknown sources, especially .zip or .exe files.
- **Requests for Credentials:** The bank will never ask for your password or multi-factor authentication (MFA) codes via email.

2. Mandatory Reporting Procedures

If you identify a suspicious email or believe you have encountered a cyber threat, you must take the following steps immediately:

- **Do Not Engage:** Do not click links, download attachments, or reply to the sender.
- **Use the Report Button:** Click the "Report Phishing" button in your email client toolbar.
- **Notify the Help Desk:** Contact the IT Security Help Desk at [Insert Phone Number] or [Insert Email Address].
- **Isolate the Device:** If you have already clicked a link or downloaded a file, disconnect your computer from the network (unplug the ethernet cable or turn off Wi-Fi) and wait for IT instructions.

3. Compliance

Failure to report known threats or gross negligence regarding security protocols may result in a review of security access privileges. Protecting our banking infrastructure is a collective responsibility.

Thank you for your vigilance.

Sincerely,

[Your Name/Signature]
[Your Title]
[Bank Name]