To: All Bank Employees

From: Information Security Department

Date: [Insert Date]

Subject: Urgent: Cybersecurity Threat Awareness and Phishing Protocols

Dear Team,

As part of our ongoing commitment to protecting bank assets and customer data, this letter serves as a formal reminder regarding our cybersecurity protocols and the increasing threat of phishing attacks.

Current Threat Landscape
Cybercriminals are frequently using sophisticated phishing emails to gain unauthorized access to internal systems. These emails often appear to be from trusted sources, such as senior management, vendors, or IT support.

Mandatory Phishing Protocols:

- **Verify the Sender:** Always check the actual email address, not just the display name.
- **Do Not Click:** Never click on suspicious links or download attachments from unsolicited emails.
- **Protect Credentials:** The IT department will never ask for your password via email.
- **Report Immediately:** If you receive a suspicious email, use the "Report Phishing" button or contact the Security Operations Center (SOC) at [Insert Extension].

In Case of a Potential Breach:
If you believe you have accidentally clicked a malicious link or entered your credentials on a suspect site, disconnect your workstation from the network immediately and call the IT Emergency Line at [Insert Number].

Your vigilance is our strongest defense. Thank you for your cooperation in keeping our institution secure.

Best regards,

[Your Name/Signature]
Chief Information Security Officer
[Bank Name]