MEMORANDUM

TO: All Employees

FROM: Information Security Department / [Your Name/Title]

DATE: [Insert Date]

SUBJECT: Urgent: Phishing Vulnerabilities and Cyber Threat Vigilance

---

Dear Team,

As we navigate an increasingly digital banking environment, our institution remains a primary target for cybercriminals. Recent security audits have highlighted a rise in sophisticated phishing campaigns designed to compromise banking credentials and sensitive client data.

To protect our assets and maintain client trust, all staff members are required to observe the following protocols:

- **Verify the Sender:** Always check the sender's full email address for subtle misspellings or unusual domains.
- **Do Not Click Unexpected Links:** Hover over links to preview the destination URL before clicking. If a request is urgent or unexpected, verify it through a secondary communication channel.
- **Protect Credentials:** No internal department or legitimate service provider will ever ask for your password or multi-factor authentication (MFA) codes via email.
- **Secure Attachments:** Never open attachments from unknown sources, especially those with .exe, .zip, or .scr extensions.

Reporting Procedures:

If you receive a suspicious email, do not delete it. Please use the [Report Phishing] button in your email client or forward the message as an attachment to [IT Security Email Address] immediately.

Cybersecurity is a shared responsibility. Your vigilance is our strongest defense against potential breaches.

Thank you for your cooperation.

Regards,

[Your Signature]
[Your Printed Name]
[Your Department]