To: All Branch Managers

From: IT Security Department

Date: [Insert Date]

Subject: SECURITY DIRECTIVE: Phishing Prevention and Cybersecurity Awareness

Dear Branch Manager,

This directive outlines mandatory security protocols to protect our branch network against increasing phishing threats and cyber-attacks. As Branch Manager, you are responsible for ensuring your team strictly adheres to the following instructions:

1. Email Vigilance

- Verify all "External" email tags before clicking links or downloading attachments.
- Inspect sender email addresses for subtle misspellings or unusual domains.
- Treat all urgent requests for password changes or wire transfers as high-risk.

2. Reporting Procedures

- Staff must immediately report suspicious emails using the "Report Phishing" button.
- If a staff member clicks a suspicious link, the computer must be disconnected from the network and reported to IT Support immediately.

3. Credential Protection

- Multi-Factor Authentication (MFA) must remain enabled on all accounts.
- Passwords must never be shared, written down in public view, or reused across personal accounts.

4. Branch Compliance

- All branch staff must complete the monthly Cybersecurity Awareness Training by the [Insert Day] of each month.
- Ensure no unauthorized devices (USB drives, personal laptops) are connected to the branch network.

Non-compliance with these security measures increases the risk of data breaches and financial loss. Please confirm receipt of this directive and brief your team during your next staff meeting.

Regards,

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