[Bank Name]
[Department Name]
[Street Address]
[City, State, Zip Code]
[Date]

To our valued customers,

Subject: Official Notification regarding Cybersecurity Awareness and Phishing Protocols

In response to the increasing frequency of global cyber threats, [Bank Name] is writing to outline our official security protocols and provide guidance on protecting your financial information.

1. Our Communication Standards
To distinguish official bank communications from phishing attempts, please be advised that [Bank Name] will never:

- Ask for your full PIN, password, or security codes via email or SMS.
- Request remote access to your personal computer or mobile device.
- Ask you to move money to a "safe account" due to a security breach.
- Send links to login pages directly within an unsolicited email.

2. Identifying Phishing Incidents
Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity. Watch for these red flags:

- Urgent or threatening language demanding immediate action.
- Slightly altered email addresses or website URLs (e.g., [BankName]-secure.com).
- Generic greetings and poor grammar or spelling.

3. Mandatory Security Protocols
To ensure the safety of your accounts, we recommend the following actions:

- Enable Multi-Factor Authentication (MFA) on all digital banking profiles.
- Regularly update your banking application to the latest version.
- Monitor your account statements weekly for unauthorized transactions.

4. Reporting Procedure
If you suspect you have been a victim of a phishing attack or notice suspicious activity, please take the following steps immediately:

1. Contact our Fraud Department at [Phone Number].
2. Forward suspicious emails to [Email Address].
3. Change your online banking credentials through our official website.

Your security is our highest priority. Thank you for your continued vigilance.

Sincerely,

[Authorized Signature]
[Name of Officer]
[Title/Position]
[Bank Name]