Date: [Insert Date]

Subject: URGENT: Protection Against Active Phishing Campaigns

Dear [Customer Name],

At [Bank Name], your account security is our top priority. We are writing to inform you of a recent increase in sophisticated phishing attempts targeting retail banking customers.

The Threat:
Cybercriminals are sending fraudulent emails and SMS messages (smishing) that appear to be from our bank. These messages often claim there is an "unauthorized transaction" or a "locked account" to trick you into clicking malicious links or disclosing your login credentials.

How to Protect Yourself:

- **Verify the Sender:** Check the email address carefully. We will only contact you from our official domain: [BankDomain.com].
- **Avoid Suspicious Links:** Do not click on links in unexpected emails. Always type our official website address directly into your browser.
- **Protect Your Credentials:** [Bank Name] will never ask for your password, PIN, or One-Time Password (OTP) over the phone or via email.
- **Enable Multi-Factor Authentication (MFA):** Ensure MFA is active on your mobile banking app for an extra layer of security.

What to do if you are targeted:
If you receive a suspicious message or believe you have shared your details on a fraudulent site, please contact our fraud department immediately at [Phone Number] or forward the suspicious email to [Abuse Email Address].

Thank you for your vigilance and for banking with [Bank Name].

Sincerely,

The Information Security Team
[Bank Name]