First Carolina Bank | BM Technologies, Inc.

February 18, 2026

# Phishing Reduction Best Practices

At BM Technologies, Inc., account security is our top priority, but it takes all of us to raise fraud awareness among our students. With fraud on the rise nationwide, knowing how to spot the signs is more important than ever.

## What you can do:

- Utilize materials on our storefront in student communication (we've added fraud-focused email, text/SMS, and social media templates)
- Work with your IT team to implement the below steps to help mitigate fraudulent communication before it ever reaches your students

## Recommend Email Filtering Configurations to Reduce Phishing Risk

The following configurations represent standard best practices for filtering phishing emails and improving email security posture across educational environments. These measures are designed to reduce risk, limit end-user exposure, and prevent compromise by quarantining suspicious messages before they reach inboxes.

1. **Enable Anti-Phishing Protection**
   Ensure that your email platform's anti-phishing policies are active and configured to automatically quarantine suspicious messages. Platforms like Microsoft 365 and Google Workspace offer these features by default but often require customization to be most effective.

2. **Block or Quarantine Suspicious Gmail Senders**
   We are currently observing a high number of phishing emails originating from personal @gmail.com accounts.

   ***Recommendation:*** *Block or quarantine inbound emails from @gmail.com domains at the gateway, especially if your institution has no expected correspondence from these addresses.*

3. **Flag and Quarantine Emails from External Sources with Risk Indicators**
   Configure rules to flag and quarantine emails with the following characteristics:

   - External origin (outside your domain)
   - Embedded links or file attachments
   - Display names mimicking internal users

   These messages should be quarantined as suspicious to prevent end-user exposure and reduce risk.

4. **Restrict Auto-Forwarding to External Addresses**
   Disable automatic forwarding to external domains unless explicitly required and logged. This limits the risk of data leakage through compromised accounts.

5. **Enable URL and Attachment Scanning with Quarantine Actions**
   Use advanced threat protection features to scan attachments and rewrite URLs in real time. Any email containing malicious or suspicious URLs or attachments should be quarantined automatically to prevent user engagement.

6. **Regularly Review Email Allow/Block Lists**
   Conduct periodic audits of domain and sender allow/block lists to avoid legacy entries that may expose your environment to known threats. Valid BankMobile-related domains are below:

   - @email.bankmobiledisbursements.com
   - @email.bankmobilevibe.com
   - @bankmobilewebemail.com
   - @storefront.bankmobiledisbursements.com
   - @bankmobiledisbursements.com
   - @bankmobile.com
   - @mailpc.custhelp.com
   - @e.bmtechnologiesinc.com
   - @mailman.bankmobilewebemail.com
   - @mailman.bmtx.com