The RED FLAGS of Phishing Emails

1. **Suspicious or Unusual Email Address:** Does that look like an email address your bank would use? Be wary of unexpected emails from addresses that aren't like the ones your bank typically employs.
2. **Typos/Misspelled Words, Unusual Grammar:** If you see misspelled words or odd grammar, they are all clear signs of an impersonator. Real banks use spell check.
3. **Scare Tactics or Urgent Language:** Don't panic. If an email uses scare tactics, such as urgent warnings of account closure or security breaches, you can safely assume it's a scam.
4. **Suspicious URLs or Hyperlinks:** Never click on them. Banks will never ask you to log in via email. Phishing emails use deceptive URLs to take you to malicious websites. Never click links that you weren't expecting.
5. **Unexpected Attachments:** Banks will never send an email attachment — especially when you didn't ask for it. Attachments can contain malware that can compromise your computer or personal information. Never click on attachments from emails supposedly from your bank.