The RED FLAGS of Phishing Texts

1. **Unusual phone numbers:** Is that the number your bank usually uses to send text messages? Legitimate text message updates come from "short codes," official 4–5-digit numbers used by your bank.
2. **Hyperlinks/Requests:** Your bank will never ask you to log into your account by texting a link. If a text message requests you to login - or requests any personal or sensitive information, such as account numbers, PINs, passwords, or social security numbers, you can assume it's a scam.
3. **Odd grammar:** If you see misspelled words or odd grammar they are clear signs of an impersonator. Real banks use spell check.
4. **Scare tactics and urgent language:** Phishing texts try to create a sense of panic, such as threatening to suspend your account or urging you to log in to verify. Real bank texts won't.
5. **Texts asking you to open a link:** Banks rarely — if ever — send links via text. Don't click them. Instead, verify the message by visiting your bank's official website, or calling the number on the back of your card.