Online Fraud

Hancock Bank and Trust Company wants to inform you of the most common types of Online Fraud which are *Phishing and Spoofing.* These types of fraud usually come in the form of e-mails that appear to be sent from legitimate sources. These e-mails ask customer to verify personal information (phishing) or to link to counterfeit (spoofed) websites that seem real.

To better protect yourself, watch for e-mails that:

- Urge you to act quickly because your account may be suspended or closed, or to update personal information
- Don't address you by name, but instead use a more generic greeting such as " Dear Valued Customer."
- Ask for account numbers, passwords, Access IDs, or other personal information.

Hancock Bank and Trust Company will never ask for sensitive data such as account numbers or your Access ID, or passwords in an e-mail.

Other Common Forms of Fraud

Fraudsters may also use other contact methods to obtain your private information. These include but are not limited to text messages (smishing) and through phone calls (voice phishing or vishing). You might receive a text message, phone call, or voice mail warning that your account may be suspended, frozen, or compromised unless you visit a particular website or call a designated phone number where you will then be asked for personal information. These "scare" tactics are designed to convince you to provide your information or face negative consequences.

Hancock Bank and Trust Company will never ask for sensitive data such as account numbers or your Access ID, or passwords in an e-mail.