Email Scams:
Phishing

How can I spot a phishing scam?

Look for these warning signs:

- **Language and tone.** The message you receive may urge you to act quickly by suggesting that your account is threatened. It may say that if you fail to update, verify or confirm your personal or account information, access to your accounts will be suspended. The wording may also be sloppy and contain misspellings.

- **Requests for personal information.** Scam e-mails typically ask for personal or account information such as:
  - Account numbers
  - Credit and check card numbers
  - Social Security numbers
  - Online banking user IDs and passwords
  - Mother's maiden name
  - Date of birth
  - Other confidential information

- **E-mailed instructions to download software.** All your online banking should be done through our secure Web site, and we will not send you e-mail instructions to download any banking software to your computer. Do not install software downloads directly from e-mail messages, or from companies or Web sites you do not recognize. When in doubt, contact customer service at 888-567-2101.

- **Non-secure Web pages.** Clever thieves can build a fake Web site that looks nearly identical to an authentic one. They can even alter the URL (the Web address) that appears in your browser window. Watch out for non-secure Web pages that ask for sensitive information (secure sites will typically display a lock in the status bar at the bottom of your browser window).

If you receive an email requesting such personal information, please call us immediately.
Toll free – 1-888-567-2101