Phishing scams most often take the form of fraudulent e-mail and text messages. Typically, these messages are designed to induce panic in the recipients through claims of loss of access to accounts (PayPal, e-mail or bank accounts, for example) or fraudulent activity on these accounts. These scams use such claims to trick recipients into immediately responding to the message or clicking on a link within the message. For example, a phishing scam message may warn you of fraudulent activity on your bank account and ask you to “click here” to verify your information. This often includes providing your account username and password. This is a phishing scam because a responsible banking company will not send you an e-mail regarding account activity. A responsible banking company also will not send an e-mail asking for account verification that requires your username and password.

Some ways to identify phishing e-mail include:

- Checking the sender’s e-mail address to see if the included domain (what comes after the “@” sign) matches the domain of the link in the body of the e-mail. You can do this by hovering over both the e-mail address and the link with your mouse cursor. If you aren’t sure about a link, send an e-mail to datasecurity@uab.edu to check BEFORE you click any links.
- Checking for misspellings or grammatical errors. Phishers often make mistakes somewhere in the subject line or the text of the e-mail.
- Being skeptical of messages that appear “too good to be true.” Use extra caution because it is likely a phishing scam.
- Being especially cautious when opening any e-mail messages retrieved from your e-mail spam or quarantine folder.

Remember, when you receive an e-mail that was unsolicited or unexpected, or is the least bit suspicious, please take the time to scrutinize it carefully. Most importantly, NEVER open attachments or click any links contained within suspicious e-mails.