## Phishing Awareness Checklist

#### Stay on alert and use this checklist to quickly determine if a strange message could be a phishing attack.

#### 4 Ways to Spot A Phish

1. **Check the Header**
* Have I given my email address to this company before?
* Do I have an account with this company?
* Does the sender identity match the purpose of email?
* Is my email listed as the From: address?
* Is the To: address to undisclosed-recipients or to a large number of recipients you are not familiar with?
1. **Check the Content**
* Do links provided in the body of the email look valid?
* Are there misspelling and typos? How is the grammar and is the tone appropriate?
* Am I being promised a lot of money for little or no effort on my part?
* Am I asked to provide money up front for questionable activities, a processing fee, or to pay the cost
of expediting the process?
* Is someone asking me for my bank account number, other personal financial information or passwords?
(“Verify your account.” or “Click the link below to gain access to your account.” are common)
1. **Consider the purpose of the email**
* Is the issue really as urgent as the sender makes it to be?
	+ “If you don’t respond within 48 hours, your account will be closed.”
	+ “Failure to do this may automatically render your account deactivated.”
* Why does the sender request confidentiality? How can I tell if the proposed activity is legitimate and authentic?
1. **Be cautious with attachments**
* Do not open unexpected attachments.
* Do not open attachments from strangers. Always be absolutely certain you know the sender first.
* Do not open unusual attachments.
* Don’t open attachments that come with strange-looking messages.