Beware of Phishing Attempts

Phishing emails are an attempt to gather information by masquerading as a trustworthy source. Users are asked to provide sensitive information such as usernames and passwords, credit card data, social security numbers, bank account information or other personally identifiable information. The phishing communications often come from email spoofing (bogus or stolen email accounts), or instant messaging. Phishing emails that contain website links not only attempt to gather sensitive user information, but may also attempt to exploit vulnerabilities in the users’ browser or operating system, and infect their machine with malicious code. Always remember, the University will never ask you for your ID and Password in an email. Ask yourself if the quality and/or content of the message is questionable?

(over...)
Beware of Phishing Attempts

What do I look for?

1. Does the “From:” address refer to the sending entity? A phishing attempt that appears to come from the University should have ua.edu at the end of the “From:” address.

2. Read the text of the message carefully for grammar and spelling errors. Many phishing attempts have poor grammar and/or spelling.

3. Contact information – usually University email will provide contact information (e.g. “Please contact the University Service Desk at 348-5555”), but not all the time.

4. Web Links – mouse hover trick – Without clicking any buttons, hover your mouse pointer over the URL and a box will show the real destination. Does the link refer to the sending entity? Occasionally, the University will use an outside entity to post videos, etc.