Don't Get Phished

As part of their emphasis on cybersecurity, the campus Chief Information Security Officers remind all employees and students that phishing takes place regularly and that every employee must be vigilant to protect their personal information and their access to University resources.

Have you ever received emails and or instant messages with:

- Threats of account closures;
- Promises of money for little or no efforts; or
- Deals that are too good to be true?

If so, you may have been exposed to a possible phishing scam.

What is Phishing?

*Phishing* (fish'ing) is a fake email, website, instant message, or phone call attempting to gather your personal information for identity theft or fraud. Employees and students should also be aware that there’s more to phishing than trying to get a social security or bank account number. Stolen passwords can lead to trouble. Research is also subject to phishing.

Here are some clues to avoid taking the bait and getting phished:

- If you get an email, instant message, or phone call in which you are asked for financial or personal information, do not reply or click links within the message.
- Never provide sensitive personal or financial information through email.
- Do not click links in potentially fraudulent emails. A link that looks like it points to a valid website could be forged or cause your computer to download malware.
- Use caution when opening email attachments, even if they appear to be from someone you know.
- Does the “From” address refer to the sending entity? A phishing attempt that appears to come from the University should have.edu at the end of the “From.”
- Read the text of the message carefully for grammar and spelling errors.
- Without clicking any buttons, hover your mouse pointer over the URL and a box will show the real destination. Is it in another country?
- Always open a new browser window and type a website’s address in the URL field. Do not cut and paste the website address.
- Always try to talk to a real person if you are in doubt.
- Check your credit card and other financial statements regularly.
- Never call a phone number listed in a suspicious email. Check the listing in the phone book or in an online directory first.

**Multi-Factor Authentication**

Users can also take advantage of multi-factor authentication services available, e.g., Two-factor authentication for your Apple ID ([https://support.apple.com/en-us/HT204915](https://support.apple.com/en-us/HT204915)) or Google 2-Step Authentication ([http://www.google.com/landing/2step](http://www.google.com/landing/2step)).