This newsletter is one in a series that provides general information on key components of the HIPAA Security Regulation. More detailed information and policies are available on the MCW HIPAA website. In this newsletter we’ll cover some important information for you regarding spoofing and phishing.

Spoofing
Email spoofing may occur in different forms, but all have a similar result: a user receives e-mail that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Examples of spoofed e-mail that could affect the security of your information include:

- An e-mail claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this.
- An e-mail claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

Phishing
Phishing attacks use both social engineering and technical maneuvers to steal consumers’ personal identity data and financial account credentials. Social-engineering schemes use ‘spoofed’ e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical maneuvers plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through denial of service (DNS) hijacking.

How to Avoid Phishing Scams
The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any e-mail with urgent requests for personal financial information.
  - Unless the e-mail is digitally signed, you can't be sure it wasn't forged or ‘spoofed’.
  - Phishers typically include upsetting or exciting (but false) statements in their e-mails to get people to react immediately.
  - They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
  - Phisher e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are.

- Don't use the telephone numbers or links provided in an e-mail to get to any web page if you suspect the message might not be authentic. Instead call the company on the telephone by using publicly advertised numbers, or log onto the website directly by typing in the Web address in your browser.

- Avoid filling out forms in e-mail messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browser’s address bar - it should be "https:" rather than just "http://".

- Regularly log into your online accounts. Don't let over a month go by before you check each account.

If you suspect you have experienced any phishing attacks at the College, notify your Desktop Technician, System Manager, or contact Information Services at 456-4357.

**COMPUTER SECURITY TIP:**

**SOCIAL ENGINEERING, OFTEN REFERRED TO AS “PEOPLE HACKING” IS AN OUTSIDE HACKER’S USE OF PSYCHOLOGICAL TRICKS ON LEGITIMATE USERS OF A COMPUTER SYSTEM TO OBTAIN INFORMATION (USERNAMES, PASSWORDS, ETC.) NEEDED TO GAIN ACCESS TO THEIR SYSTEMS.**

You can reference additional information on computer security at:

The MCW HIPAA website: [http://infoscope.mcw.edu/display/router.asp?docid=8598](http://infoscope.mcw.edu/display/router.asp?docid=8598)
The MCW Information Services website: [http://infoscope.mcw.edu/display/router.asp?docid=7798](http://infoscope.mcw.edu/display/router.asp?docid=7798)