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 important information for you regarding e-mail spam.

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender. Spam prevents you from focusing on the important things you need to do every day at the College. Spam clogs up the College’s servers and storage systems with unwanted and unnecessary e-mails, and in the worst case can be a “denial of service attack.”

These types of unsolicited e-mails include: chain letters, pyramid schemes, and requests for financial support. A common technique is to tell you that “your financial information is out of date” and that in order to correct the information you are requested to provide updates at the “bank’s website.” If requested by way of e-mail, never go to a website and enter your personal or financial information!

Here are some of the most common scam offers likely to arrive by e-mail:

- Updating Financial Information at a Bank
- Chain Letters
- Work at Home Schemes
- Weight Loss Claims
- Credit Report Offers
- Advance Fee Loan Scams

You should never reply to e-mail Spam, even if it is to send a "remove" request. You should simply delete unwanted e-mail traffic. Most e-mail Spammers ignore your response, or worse, they add you to their validated e-mail address lists. Some Spammers are known to sell or share their validated e-mail lists for others to use.

There are numerous ways to reduce the amount of spam that you receive. Try not to display your email address in public. That includes newsgroup postings, chat rooms, websites or in an online service's membership directory.

Check the privacy policy when you submit your address to a website. See if it allows the company to sell your e-mail address. You may want to opt out of this provision, if possible, or not submit your e-mail address at all to websites that won't protect it.

As previously discussed, your best defense is not to respond to unsolicited e-mail Spam, but simply delete these messages.

Information Services or your System Manager are continually implementing methods of screening out unwanted spam on College e-mail accounts. If you believe you are receiving a mass amount of spam e-mails, notify your Desktop Technician, System Manager, or contact Information Services at 456-4357.

**COMPUTER SECURITY TIP:**

MAKE SURE TO INSTALL VIRUS SCANNING SOFTWARE ON YOUR LAPTOP AND HOME COMPUTER AND KEEP VIRUS SCANNING DEFINITION FILES UP TO DATE.

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)