SPOTTING E-MAIL HOAXES AND SCAMS

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 methods for spotting e-mail hoaxes and scams.

Are you a Nigerian Government contracting millionaire or maybe you're an oil tycoon? Perhaps you are afraid to travel for fear of losing your kidney? These, like other e-mails, are hoaxes, scams and other urban legends. For many years, computer virus hoaxes have been circulating the Internet. In October of 1988, one of the first virus hoaxes publicized was the 2400 baud modem virus. Since that time, these expensive nuisances have flooded the Internet. It is the paranoia of getting a virus that often fuels virus hoaxes.

Internet hoaxes and chain letters are e-mail messages written with one purpose: to be sent to everyone you know. The messages they contain are usually untrue. Most of the hoax messages play on your need to be kind to others. Despite the abundance of them in your inbox, there is a way to identify if they are in fact hoaxes.

One example of a hoax that actually was sent to MCW employees was allegedly from numerous banks including M&I Bank. Some employees received an e-mail requesting their personal account information. These employees may or may not have had an account with the bank. M&I Bank did not send out an e-mail to their customers. The e-mail was a scam to obtain customer’s account information.

How to Recognize a Hoax
If it is too good to be true, it probably is. Most hoaxes come from mass mailers that are unknown and untraceable. Attempts to gain additional information about the offers may result in unknown websites, bogus companies and various other schemes. When phone numbers are present, they should never be called since you may connect to numbers that charge over 500 US dollars a minute.

There are several websites that list detailed information about e-mail hoaxes. There are three listed in our additional information section below. If you do not find the warning at the hoax website, it may just mean that this particular hoax has not yet been reported. If you cannot determine if a message is real or a hoax, you should consult your Desktop Technician, System Manager, or contact Information Services at 456-4357.

Preventing the Spread of E-mail Hoaxes
MCW users should never spread e-mail messages that are chain letters or hoaxes. Probably the biggest risk for hoax messages is their ability to multiply and potentially cause a denial of service on the Colleges’ e-mail servers. That is, the e-mail servers are so inundated with bogus e-mails, they literally “shut-down.” Many people knowingly or inadvertently send hoax messages to everyone in their address books.

Spammers (bulk mailers of unsolicited mailers) often harvest e-mail addresses from hoaxes and chain letters. In addition, spammers may deliberately start hoaxes and chain letters to gather email addresses.

In all cases, do not reply to the messages. Instead, delete them immediately. It is recommended that this type of mail be handled like Spam. Do not forward it. Do not respond to it. Delete it.

Computer Security Tip:
SPYWARE IS A GENERAL TERM USED FOR SOFTWARE THAT PERFORMS CERTAIN BEHAVIORS SUCH AS ADVERTISING, COLLECTING PERSONAL INFORMATION, OR CHANGING THE CONFIGURATION OF YOUR COMPUTER, GENERALLY WITHOUT YOUR KNOWLEDGE OR CONSENT.

You can reference additional information about e-mail hoaxes 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)