Phishing is a form of social engineering that attempts to ‘con’ users into giving up sensitive information, for example personally identifiable or financial information.

Communications that seem to be from popular social web sites, financial institutions, well-known companies, IT support staff, etc. are used to lure people into giving up information which could then be used to impersonate the individual for financial gain or some other reason.

Phishing is typically carried out through e-mail spoofing or instant messaging and it characteristically directs users to enter information at a fake website that looks very much like the legitimate website.

Some quick tips to stay safe:

- Be suspicious of attachments and unexpected e-mail messages.
- Never reveal personal or financial information in e-mail, and never respond to e-mail requests for this information.
  - Legitimate organizations will never ask for this type of information in an e-mail.
- Pay attention to the ‘make up’ of the message. It may look authentic, i.e. logos, urls, etc., but there are typically mistakes, for example with grammar.
- Never click on a link in a suspicious message; it could be used to spread malicious software. The domain name may appear to be the real domain name but it may have been altered. If you have reason to believe that the message is real, call the organization or go out to a web browser and enter the web address but don’t click on any links in the message.
- Ensure that your antivirus is up to date and running in real time scan mode.
- Take note if the message contains threats or a sense of urgency.
  - Cybercriminals often use threats to get what they want. The threat could make you let your guard down and cause you to respond quickly without thinking.

Remember, you can usually trust your instincts; if you think the message is suspicious it probably is, just delete it. If you continually have an issue with phishing, please contact the PMACS Service Desk or Information Security for assistance.

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo: David.Wargo@uphs.upenn.edu
For more security related information, visit the PMACS Information Security web page:
http://www.med.upenn.edu/pmacs/