Phishing is a form of social engineering that attempts to ‘con’ users into giving up sensitive information, e.g. 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 this 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.

**Signs That Someone Has Gone Phishing** –

The message contains misspelled words and/or poor grammar is used.

- Cybercriminals may get pictures, logos, URLs, and other graphics to look authentic but they don’t seem to be able to do a very good job with editing their communications.

The message is asking for personally identifiable information, such as credit card numbers, passwords, PINs or Social Security Numbers.

- A legitimate organization, e.g. bank, credit card company, IRS, IT support will never ask you for this type of information in an e-mail.

The message instructs you to “Click here”.

- Never click 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 the link in the message.

The message contains "threats" or statements that create a sense of urgency. For example: "Your account will be locked until you reply" or "We have noticed activity on your account from an unusual location."

- 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.