From: Norma Grijalva [mailto:norma@nmsu.edu]
Sent: Thursday, December 05, 2013 9:20 AM
To: all-nmsu@nmsu.edu
Subject: Security Awareness Memo - Phishing Advisory-NMSU Email Verify

To: NMSU Community
From: Norma Grijalva, ICT
Date: December 5, 2013
Memo: Security Awareness Memo - Phishing Advisory - NMSU Email Verify

An email phishing scam made it past our email filters today. The subject of the email was **NMSU Email Verify. If you inadvertently clicked on the link contained in this email, please go to My.NMSU.edu and immediately change your password.**

Phishing (pronounced "fishing") is an attack by the computer hacking and fraud community to lure you to fraudulent, but official-looking websites. They do this by creating e-mails that look very much like they are being sent from legitimate organizations. However, when you click on a link in the e-mail it takes you to a mock-up of the legitimate organization's website where you are asked for your logon credentials, credit card information or other sensitive information. When you supply this information, it is used by hackers/fraudsters to commit illegal acts. Phishing is a significant problem; even large security-savvy organizations are successfully targeted. Phishing is real and will be with us for the foreseeable future. Understanding this threat has never been more important.

NMSU receives and processes between 8 and 11 million email messages per day. Approximately 98% of those messages are identified by our email filtering appliances as junk, phishing, malware or spam and are quarantined or discarded. For more security information go to http://infosec.nmsu.edu/.

The simplest way to protect yourself from phishers is to do the following:

1. Do not click on any suspicious links in an e-mail message, just delete the message.
2. To check the authenticity of a link, place your cursor over the link but do not click (hover). You should see the real link destination in the bottom left portion of the window of your email client. If it does not end with nmsu.edu it is likely fraudulent.
3. Do not enter your NMSU Username and password....ICT will never request your credentials via an email.
4. Do not reply to e-mails soliciting personal information.
5. Report suspicious emails to abuse@nmsu.edu.

We appreciate your patience as we continue to work together to battle those who are attempting to circumvent our security measures. If you need help, please contact the ICT help desk at helpdesk@nmsu.edu or (575) 646-1840. As always you are welcome to email me directly at norma@nmsu.edu with any questions or concerns.

Thank you and stay vigilant.

--
Norma Grijalva, PhD
Interim CIO
Email: norma@nmsu.edu
phone: 575-646-7767