From: all-nmsu-bounces@nmsu.edu [mailto:all-nmsu-bounces@nmsu.edu] **On Behalf Of** Norma Grijalva
Sent: Monday, August 25, 2014 9:55 AM
To: all-nmsu@nmsu.edu
Subject: Information Security Awareness Memo - Phishing Advisory

To: NMSU Community
From: Norma Grijalva, ICT
Date: August 25, 2014
Memo: Information Security Awareness Memo - Phishing Advisory

Email phishing activity ramps up across the country when classes begin and NMSU is no exception.

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 log on 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 a real threat 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 phishing scams is to do the following:

- Never click on any links in a suspicious e-mail message, just delete the message.
- 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. The root URL for NMSU is nmsu.edu as in the website my.nmsu.edu which displays a URL of https://my.nmsu.edu/web/mycampus/home . This pattern is true for all legitimate websites like Wellsfargo.com which might display a URL like https://www.wellsfargo.com/checking/ .
- Legitimate organizations such as ICT will never request your credentials via an email.
- Do not enter your NMSU Username and password or any other personally identifiable information via an email request.
- Do not reply to e-mails soliciting personal information.
- 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
CIO/AVP Information Technology
Email: norma@nmsu.edu
phone: 575-646-7767