From: All-nmsu <all-nmsu-bounces@nmsu.edu> **On Behalf Of** Norma Grijalva
Sent: Thursday, August 23, 2018 10:21 AM
To: all-nmsu <all-nmsu@nmsu.edu>
Subject: Information Security Awareness Memo - Phishing Advisory

To: NMSU Community
From: Norma Grijalva, ICT
Date: August 23, 2018
Memo: Information Security Awareness Memo - Phishing Advisory

Welcome back Aggies!

NMSU values your security and privacy, unfortunately the start of the semester brings with it numerous email phishing scams.

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 login credentials, banking information, credit card information, or other sensitive information. If you supply this information, it will be 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 9 and 13 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, however some still get through.

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

1) Do not click on any links in a suspicious 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 or a popup bubble in your email client.
3) Do not enter your NMSU Username and passphrase … ICT will never request your credentials via an email.
4) Do not reply to e-mails soliciting personal, banking, credit card, NMSU, or other login information
5) Report suspicious emails to abuse@nmsu.edu.

If you believe you may have inadvertently clicked on the link in a phishing scam email or provided sensitive information, please go to My.NMSU.edu and immediately change your passphrase.

Additional Security Tips:

1) If you use a public computer including NMSU lab computers, please be sure to close your browser and logout every time.
2) Do not share your NMSU account passphrase with anyone.
3) Phishers are also using other methods to contact people such as phone calls or pop computer warning screens. Do not provide any personal information or allow access to your systems.
4) Instead of clicking on a link, type the link address into your browser.

For more security information go to http://infosec.nmsu.edu/.

We appreciate your vigilance 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.

--
Norma Grijalva, PhD
CIO/AVP Information Technology
Email: norma@nmsu.edu
phone: 575-646-7767