NM STATE UNIVERSITY

Garrey Carruthers, Ph.D.
Chancellor
New Mexico State University System
MSC 3Z
P.O. Box 30001
Las Cruces, NM 88003-8001
575-646-2035, fax: 575-646-6334
president@nmsu.edu

DATE: March 27, 2017

TO: All NMSU employees

FROM: Garrey Carruthers, Chancellor

SUBJECT: Your Responsibility -- Keeping Personal Data Secure

Last month, several individuals had their direct deposit payments stolen by hackers. We believe the hack occurred after these individuals clicked on a link inside a scam email, also known as a phishing email. That money is now unrecoverable.

NMSU and its staff and students, as with those at other large organizations, are under continual attack from hackers trying to steal your private data. While NMSU continually improves security measures, there is no way to completely prevent exposure to these types of attacks. **You must protect yourself from these common threats.**

The purpose of this message is to alert you to the fact that <u>you are responsible for any personal loss resulting from providing your private information</u> in a phishing scam. Each individual must protect their own private data and be alert and knowledgeable of threats posed by scam emails.

Your NMSU password, bank account number and social security number, to name a few, are all your private information. In the wrong hands, this data can be used to steal from you and places the personal information of others at risk. Scam emails typically masquerade as emails from sources you trust – like your bank or the NMSU payroll department. The MOST important protection you have is to remember that "NMSU will **never** ask you to provide your NMSU ID/password, bank account information or any other private data via an email web link."

You are personally responsible for developing the skills to identify these threats. You can fulfill this responsibility by educating yourself and using a healthy measure of skepticism and a critical eye when **any** unsolicited email, phone call, screen pop-up or individual asks you for your private information. For these reasons, NMSU requires all employees to complete the Computer and Data security training on a yearly basis to help you develop essential security skills.

When you receive a phishing email or any suspicious solicitation, please forward it to our security folks at abuse@nmsu.edu. ICT does not reply to all submissions but you can be assured that countermeasures will be adopted for any scam emails.

To learn more about security, I want everyone to go to http://infosec.nmsu.edu/cyber-security-tips/ and take time to read at least a couple of the articles. By learning these tips and other simple skills, you can protect yourself and NMSU from these attacks. Let's all take ownership of security, zealously guard our private data, and send these criminals packing.