From: all-nmsu-bounces@nmsu.edu [mailto:all-nmsu-bounces@nmsu.edu] **On Behalf Of** Norma Grijalva
Sent: Wednesday, October 07, 2015 5:46 PM
To: all-nmsu@nmsu.edu
Subject: NMSU participates in National Cyber Security Awareness Month

To: NMSU Community
From: Norma Grijalva, ICT
Date: October 7, 2015
Subject: NMSU participates in National Cyber Security Awareness Month

National Cyber Security Awareness Month (NCSAM) is celebrated every October and was created as a collaborative effort between government, education, and industry to ensure every American has the resources they need to be more secure online.

Multiple events are planned for October. We invite you to the kickoff Cyber Security Awareness event on **Thursday October 8, at 8:30 AM in Corbett Center Senate Chambers.** You may also view the webcast at: http://panopto.nmsu.edu/Panopto/Pages/Viewer.aspx?id=7229aaa3-4ecf-42ea-ab31-eb2598cee592 . To ensure that all of the NMSU community gets the message about cyber security, we will be visiting the NMSU community colleges and have other events. ICT will provide more details in the near future.

NMSU participates in this effort by making the NMSU community aware of cyber security threats including but not limited to phishing, malware, viruses, social engineering and social media threats. For more information on how to stay safe online we invite you to visit NMSU's Information Security website at infosec.nmsu.edu for tips and resources on safe computing practices.

Some Information Security Best Practices:

- Any computing/communication device that is connected to the Internet is vulnerable to viruses. Please be sure you have an up-to-date anti-virus and malware software installed on your computers. NMSU provides the Sophos anti-virus/malware software free of charge to the NMSU community and it can be downloaded at http://software.nmsu.edu/.
- Any computing/communication device that is connected to the Internet must have its operating system and applications up to date! Security patches and updates are released weekly.
- Use complex passwords that combine numbers, letters, capitalization, and symbols with minimum length of 8 and ideally longer. Create unique passwords for different accounts, so if one account is hacked the others are not affected. An example of a good password: TheAggiesaregoing2win!
- Do not click links in emails unless you are expecting them or you have verified they are from a trusted source. Even when visiting reputable websites avoid clicking on ads. As many as one-third of all ads contain malware.
- When using a public Wi-Fi for sensitive business use a Virtual Private Network (VPN). More information about NMSU's VPN service is available at http://ictvpn.nmsu.edu/.
- If you are on campus using wireless for sensitive work be sure to use the AggieAir-WPA2. For instructions on how to use this service go to http://helpdesk-kb.nmsu.edu/DOCS/WPA2_Windows.html .
- Be a good network citizen, if you see an email or website that is suspicious report it to abuse@nmsu.edu . ICT relies on your help to increase our threat intelligence.

For more information about information security visit infosec.nmsu.edu . Cyber security is everyone's responsibility. If you have any questions or comments regarding this memo, do not hesitate to contact me via email at norma@nmsu.edu.

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