September 3, 2015

TO: Faculty and Staff
FROM: Midhat Asghar
       Assistant Vice President for Information Resource Management
RE: Phishing Attempt Threat Advisory

Dear Faculty & Staff,

Phishing is a fraudulent process used by email spammers to acquire sensitive information from users such as usernames, passwords, and credit card details. Email recipients are often deceived by phishing attempts since messages appear to be sent by legitimate and trustworthy sources.

Recently, we have experienced continues targeted phishing attempts.

Our email traffic is filtered, which provides you with protection against dangerous viruses and spam. However, some may occasionally get through to your inbox, so please use caution. If you happen to receive a message that appears to be spam, close the message immediately and report it.

Here is an example of what a phishing scam in an email message might look like.

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form.

http://www.facebook.com/application_form

Note: If you don't fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

- **Spelling and bad grammar**: Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not
allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.

| https://www.woodgrovebank.com/loginscript/user2.jsp |

Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised.

- **Spoofing popular websites or companies.** Scammers use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

Information Technology Services, Office of Information Resources, Office of Distance Learning or any other PVAMU unit will **NEVER** ask for username and password to be submitted by an email or click on links to update mailbox.

If you have clicked on the link, or replied to this email, or think that your password has been compromised, please do the following immediately,

- **Change your password at** www.pvamu.edu/passwordreset
- **Contact Information Technology Services at** 936-261-2525
- **Notify Mr. Midhat Asghar at** miasghar@pvamu.edu
- **Disconnect the computer from network (unplug network cable)**

Below is sample of a recent phishing attempt.

**From:** "Harris, Jennifer D"
**Date:** September 3, 2015 at 12:43:38 PM CDT
**To:** "Harris, Jennifer D"
**Subject: Your mailbox has been compromised**

Your mailbox has been compromised, Kindly Authenticate your Outlook Account to prevent a permanent closure of this email address/Outlook web-mail account Click Here http://workfadministrator.hol.es/ to Authenticate.

If Unable to Access the Above link, Kindly Click on Employee, Faculty, Staff Members Access Page to confirm that your email account Has been Authenticated by filling the Link provided with the institution requirement.

ITS help desk
ADMIN TEAM