



PRAIRIE VIEW A&M UNIVERSITY


A Member of the Texas A&M University System

March 25, 2021

OFFICE OF BUSINESS AFFAIRS MEMORANDUM No. FY21-28

Distributed via Campus Email

To: PVAMU Faculty and Staff

From: Cynthia A. Carter-Horn 
Senior Vice President for Business Affairs

James M. Palmer 
Provost & Senior Vice President for Academic Affairs

Re: Cybersecurity Event and Personal Safeguards

On February 4, 2021, Prairie View A&M University experienced a major cybersecurity event that immobilized all major network systems, impacting our ability to access critical day-to-day operational systems. The Cyber Response Team from The Texas A&M University System worked continuously with our IT staff and others to restore systems, turning the continued restorations over to our IT staff on February 21, 2021. Our IT staff are still working to restore systems.

Unfortunately, we have recently determined that the threat actors who hacked into our systems were able to access some of Prairie View A&M University's information on our network shared drives. We have identified the compromised data and are in the process of making the appropriate notifications, including identifying those impacted individuals via U.S. mail and, out of an abundance of caution, providing them with instructions to sign up for free credit monitoring services.

As we continue to restore systems and transition applications and services on premise to cloud-based for the most optimum levels of security and safeguarding of data, we provide the following suggestions.

- Work files should be saved to cloud-based applications like Microsoft OneDrive or Syncplicity instead of on your computer's hard drive or network drive.
- Do not use your work email or work-related systems for personal use.
- Limit the sharing of work files that contain personal identifiable information. When you save those files, they should be encrypted. If you do have to share the drives, please do so via secure means (i.e., email encryption or by assigning a password and notifying the recipient of the password under a separate communication).
- Most, if not all, PVAMU or Texas A&M System applications require multi-factor authentication. Be aware of logins to your accounts. If you did not login yet and receive a request to authenticate to your designated device, immediately decline, change your password and notify the IT Helpdesk.

xc: Ruth J. Simmons