**Cyber Awareness Training**

**Purpose of Training**

This training is meant to educate students, faculty, and staff on the best practices within cybersecurity with the mission of ensuring that the universities systems remain secure with the increase in cyber-attacks across the country. It will provide valuable information to all users and keeps all users in compliance with university rules.

**Training Requirements**

This training will be required for all individuals affiliated with the university annually to keep everyone informed with steps that you should be taking to protect yourself and the university. This training will be due by the end of the first week of the semester of each academic year. If a student or staff starts mid-academic year, then they will be required to complete the initial training within one week of starting. Failure to complete the training within the required period will result in the user account to be locked.

**Topics Covered:**

1. Password Security
   1. Strong Passwords
   2. Password Reuse
   3. Forced Password Change
   4. Multi-Factor Authentication
2. Wifi Security
   1. Public Wifi
3. Removable Media
   1. USB Drives
4. Social Media Use
   1. Information Posted
   2. Friends
   3. Quizzes
5. Shoulder Surfing
   1. Dangers
   2. Prevention
6. Email Security
   1. Attachments
   2. Phishing
7. Social Engineering
8. Internet Security
9. Physical Security
   1. Protecting your Devices
   2. Desk Areas
10. Mobile Security
11. Cybersecurity Policies
    1. Acceptable Use Policy
12. Common Scams

The quizzes for each section of the training are to help ensure that you are learning the materials and help prepare you for the final test, which is required to get credit for completing the exam. The final test will consist of 25 multiple choice and true and false questions. To pass the cyber awareness training, you are required to get an 80% on the final exam.