CYBERSECURITY (CYB)

Courses and Descriptions

CYB 105 Introduction to Cybersecurity 3 Credits
Introduction to Cybersecurity introduces students to this interdisciplinary field by exploring the technology, policies, and processes that enable assured computer operations. Students will be introduced to recent developments in cybercrime such as phishing, ransomware, viruses, and worms. Students will also learn about the policy and legislation regarding privacy, terrorism, hacktivism, and the dark web. Students will also be introduced to programming and networking concepts.

CYB 110 Cybercrime and Cyberterrorism 3 Credits
This course explores the world of cybercrime and cyber terrorism. Students will learn about the social and legal aspects of cybercrime and the technical tools that enable the investigation of these acts. They will discuss and review several definitions and types of cybercrime, and the roles of private sectors and law enforcement in detecting, investigating and preventing these acts.

CYB 130 IT Fundamentals 3 Credits
IT Fundamentals is designed to immerse students in the essentials of computer hardware and software. The IT Fundamentals course provides students with principles of data and technology that frame and define cybersecurity and insight into the importance of cybersecurity and the integral role of cybersecurity professionals. Students will explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

CYB 200 Operating Systems & Cybersecurity 3 Credits
This course focuses on the fundamental properties of three major operating systems (Linux, MacOS, and Windows). The course covers file systems, command line interfaces, and shell scripting. Students will learn how to manage user groups while focusing on security. They will also be introduced to SQL database architecture.
Prerequisite(s): CYB 130.

CYB 240 Ethical Hacking and Penetration Testing 3 Credits
This course introduces students to the methods of penetration testing and hacking as method of locating and successfully exploiting computer systems for the purpose of making computer systems more secure. This process includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real and generating specific and effective recommendations for addressing and fixing security issues discovered vulnerability assessments and penetration.
Prerequisite(s): (CYB 200 with a minimum grade of D or CSC 240 with a minimum grade of D) and CSC 260 with a minimum grade of D.

CYB 260 Network Defenses and Countermeasures 3 Credits
This course in network defenses and countermeasures prepares students to defend networks against attacks by implementing proactive protection measures and by responding to active and potential threats. It covers multiple techniques for network defense, including firewalls, intrusion-detection systems, VPNs, encryption, and system hardening.
Prerequisite(s): CYB 240.

CYB 300 Developing & Deploying Cybersecurity Programs 3 Credits
In Developing and Deploying Cybersecurity Programs, students will learn how to create cybersecurity policies, standards, guidelines and plans, and the differences between them. Students will learn how threats develop, and how threat actors launch attacks on their targets. The material in this course conforms to the NIST Cybersecurity Framework and the ISO/IEC 27000-series standards.
Prerequisite(s): CSC 260 with a minimum grade of D.

CYB 320 Cyber Forensics 3 Credits
This course covers the technical and legal aspects of cyber forensics, including general forensic procedures, electronic discovery, imaging, hashing, file recovery, mismatched file types, and preserving the chain of evidence. Students will perform detailed cyber forensic analyses on compromised system images, using both open-source and court-approved digital forensic software tools to conduct forensic examinations, write analytical reports, and practice mock courtroom presentations.
Prerequisite(s): CYB 200.

CYB 490 Cybersecurity Independent Study and Research 3 Credits
Immerses the student in guided research. The student learns to organize material, use the literature, obtain reproducible data, and synthesize the results of the study. If possible, the student will publish the results or present them at a scientific meeting.

CYB 491 Internship in Cybersecurity 1-4 Credits
A supervised research experience in an approved organization where qualified students gain real-world knowledge and utilize their academic training in a professional environment. Placement may be in private, public, non-profit, or governmental organizations under the guidance of a mentor. The mentor and student will have regular consultation with the departmental internship coordinator to assess the student's progress. Normally, 40 hours of internship per credit is required. The grade for the course will be determined by the student's overall performance in their research work, a research paper documenting their work with their internship mentor and an oral or poster presentation at the end of the semester. Available for juniors and seniors.
Prerequisite(s): 2.5 GPA and Permission of Dept. Chair/Program Director.