

# CYBERSECURITY - CYB

<p><b>CYB 500 Cybersecurity Principles</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>This course examines the landscape and the broad areas of cybersecurity which includes topics such as: Symmetric &amp; Public-Key Encryption, Access Control, Database Security, Malware, DoS (Denial-of-Service) Attacks, Intrusion Detection &amp; Firewalls, Software Security, Security Management &amp; Policies, Internet Security, and Legal &amp; Ethical Aspects of Cybercrime. Students will also complete hands-on labs and exercises to reinforce their working knowledge of computer, network and information security topics. <b>Prerequisite:</b> (CSC 310 and CSC 310L) or (CSC 610 and CSC 610L) may be taken concurrently, and (CSC 112 and CSC 112L) or (CSC 512 and CSC 512L). <b>Corequisite:</b> CYB 500L. <b>Offered:</b> every fall &amp; spring.</p>	<p><b>CYB 520 Ethical Hacking and Penetration Testing</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>This course provides an in-depth understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Students will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. <b>Prerequisite:</b> CYB 500 and CYB 500L; may be taken concurrently. <b>Corequisite:</b> CYB 520L. <b>Offered:</b> every spring.</p>
<p><b>CYB 500L Cybersecurity Principles Lab</b> <span style="float: right;"><b>0 Credits</b></span></p> <p>Required lab for CYB 500. <b>Corequisite:</b> CYB 500. <b>Offered:</b> every fall &amp; spring.</p>	<p><b>CYB 520L Ethical Hacking and Penetration Testing Lab</b> <span style="float: right;"><b>0 Credits</b></span></p> <p>Required Lab for CYB 520 <b>Prerequisite:</b> CYB 500 and CYB 500L. <b>Offered:</b> every spring.</p>
<p><b>CYB 501 Cybersecurity Principles for Business</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>This course examines the landscape and the broad areas of cybersecurity which includes topics such as: Symmetric &amp; Public-Key Encryption, Access Control, Database Security, Malware, DoS (Denial-of-Service) Attacks, Intrusion Detection &amp; Firewalls, Software Security, Security Management &amp; Policies, Internet Security, and Legal &amp; Ethical Aspects of Cybercrime. <b>Offered:</b> every fall &amp; spring.</p>	<p><b>CYB 540 Network and Internet Security</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>The purpose of this course is to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (especially Internet standards) that have been widely deployed. The first part of the course will cover a concise survey of the cryptographic algorithms and protocols underlying network security applications, including encryption, hash functions, message authentication, and digital signatures. The second part of the course will cover important network security tools and applications, including key distribution, Kerberos, X.509v3 certificates, Extensible Authentication Protocol, S/MIME, IP Security, SSL/TLS, IEEE 802.11i WiFi security, and cloud security. Finally, we will look at system-level security issues, including the threat of and countermeasures for malicious software and intruders, and the use of firewalls. <b>Prerequisites:</b> CYB 500 (can be taken concurrently), and ((CSC 310 and CSC 310L) or (CSC 610 and CSC 610L)). <b>Corequisite:</b> CYB 540L. <b>Offered:</b> every fall.</p>
<p><b>CYB 505 Capture the Flag &amp; Cybersecurity</b> <span style="float: right;"><b>1.5 Credits</b></span></p> <p>CTF stands for Capture The Flag. It's a competition where contestants solve challenges related to cybersecurity. These challenges can range from basic programming exercises to more complex tasks like hacking into servers to retrieve hidden data. The ultimate goal is to find a specific piece of text called the flag. Students will participate in weekly meetings and at least two CTF events in the semester. <b>Offered:</b> every fall &amp; spring.</p>	<p><b>CYB 540L Network and Internet Security Lab</b> <span style="float: right;"><b>0 Credits</b></span></p> <p>Required lab for CYB 540 <b>Corequisite:</b> CYB 540. <b>Offered:</b> every fall.</p>
<p><b>CYB 506 Cybersecurity Certification Preparation</b> <span style="float: right;"><b>1.5 Credits</b></span></p> <p>This course is designed to prepare students for industry-recognized cybersecurity certifications, such as CompTIA Security+ or Certified Ethical Hacker (CEH). Participants will collaborate with the instructor to develop a personalized study plan, covering essential exam topics. Weekly meetings will focus on reviewing study materials, discussing best practices, and reinforcing key concepts. At the end of the course, students will take the target certification exam to validate their knowledge and skills. <b>Prerequisite:</b> CYB 500. <b>Offered:</b> every fall, spring, &amp; summer.</p>	<p><b>CYB 550 Techniques to Analyze and Evaluate Malware</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>This course teaches a wide range of skills required to do malware analysis. Students will understand how cybersecurity analysts who evaluate malware perform their job and will learn the same skills they apply on a daily basis. The lecture component of the course will explain malware analysis concepts while the lab components will have students apply the concepts learned on actual malware. Specific topic coverage includes: Introduction to Malware Analysis, Basic Static Analysis Techniques, Advanced Static Analysis Techniques, Basic Dynamic Analysis Techniques, Advanced Dynamic Analysis Techniques, Basics of Assembly Language and Disassembly, Debugging, Disassembly with IDA and Ghidra, Packers and Cryptors, Android Malware, Malware Obfuscation Techniques, and Risk Mitigation . <b>Prerequisite:</b> CYB 500 (can be taken simultaneously). <b>Corequisite:</b> CYB 550L. <b>Offered:</b> every fall.</p>
<p><b>CYB 510 Cybersecurity Policies, Ethics, and Law</b> <span style="float: right;"><b>3 Credits</b></span></p> <p>This course focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series. <b>Offered:</b> spring and summer.</p>	<p><b>CYB 550L Techniques to Analyze and Evaluate Malware Lab</b> <span style="float: right;"><b>0 Credits</b></span></p> <p>Required lab for CYB 550. <b>Corequisite:</b> CYB 550. <b>Offered:</b> every fall.</p>

<b>CYB 580 Cybersecurity Seminar</b>	<b>3 Credits</b>	<b>CYB 620 Applied Cryptography</b>	<b>3 Credits</b>
This a graduate seminar course in which students will give oral presentations of scientific data. Students attend presentations as well as prepare and present on various topics in cybersecurity for faculty and other students. The seminars is expected to enhance the student's public speaking skills and to provide experience in preparing scientific presentations for professional settings. To help students improve as speakers, each student will receive feedback from fellow students and the instructor.		This course will introduce the concepts of modern cryptography, including a combination of both theoretical foundations and practical applications of cryptography used in the real world. This course complements all of the CYB 5xx cybersecurity courses by taking a deeper look into cryptography to grasp a better understanding of cryptographic primitives, algorithms, attacks, and protocols. At the end of this course, students will have a proper foundation of modern cryptography and be able to apply cryptographic techniques in the design and analysis of secure computing systems.	
<b>Offered:</b> occasionally.		<b>Prerequisites:</b> CYB 520 and CYB 540 (CYB 540 can be taken concurrently).	
<b>CYB 599 Cybersecurity Special Topics</b>	<b>3 Credits</b>	<b>Corequisite:</b> CYB 620L.	
Current topics in Cybersecurity of interested to faculty and students. Possible topics include: Malware Analysis & Reverse Engineering, Bitcoin & Cryptocurrencies, Machine Learning & Security, Computer Forensics, etc.		<b>Offered:</b> every fall.	
<b>Prerequisites:</b> CYB 500 can be taken concurrently. <b>Corequisite:</b> CYB 599L.		<b>CYB 620L Applied Cryptography Lab</b>	<b>0 Credits</b>
<b>Offered:</b> every fall.		Required lab for CYB 620	
<b>CYB 599L Cybersecurity Special Topics Lab</b>	<b>0 Credits</b>	<b>Corequisite:</b> CYB 620.	
Required lab for CYB 599		<b>Offered:</b> every fall.	
<b>Corequisite:</b> CYB 599.		<b>CYB 655 Cybersecurity Operations</b>	<b>3 Credits</b>
<b>Offered:</b> every fall.		Defending an enterprise network from attackers and adversaries gets more complicated every year - this course aims to give students a taste of the different technologies and disciplines that are needed to detect and investigate potential intrusions. Topics covered include building and tuning logging infrastructure, detection engineering, honeypot deployments, threat intelligence, purple teaming, and incident response. The course is designed with an emphasis on hands-on, practical skills that are in common use in the cybersecurity industry today.	
<b>CYB 600 Secure Software Engineering</b>	<b>3 Credits</b>	<b>Prerequisite:</b> CYB 540 and CSC 530. <b>Corequisite:</b> CYB 655L.	
The purpose of this course is to provide secure programming practices that are necessary to develop applications that withstand cyber-attacks and common software exploits. The first part of the course will cover the fundamentals of software security and implementing a continuous risk management framework throughout the software development lifecycle. The second part of the course will cover the Seven Touchpoints for software security as well as code reviews and software penetration testing. Finally, we will look at adopting a secure development lifecycle (SDL) in an enterprise setting.		<b>Offered:</b> every fall.	
<b>Prerequisite:</b> CYB 500 and CSC 610. <b>Corequisite:</b> CYB 600L.		<b>CYB 655L Cybersecurity Operations Lab</b>	<b>0 Credits</b>
<b>Offered:</b> every spring.		Defending an enterprise network from attackers and adversaries gets more complicated every year - this course aims to give students a taste of the different technologies and disciplines that are needed to detect and investigate potential intrusions. Topics covered include building and tuning logging infrastructure, detection engineering, honeypot deployments, threat intelligence, purple teaming, and incident response. The course is designed with an emphasis on hands-on, practical skills that are in common use in the cybersecurity industry today.	
<b>CYB 600L Secure Software Engineering Lab</b>	<b>0 Credits</b>	<b>Prerequisite:</b> CYB 540 and CSC 530. <b>Corequisite:</b> CYB 655.	
Required lab for CYB 600		<b>Offered:</b> every fall.	
<b>Corequisite:</b> CYB 600.		<b>CYB 680 Cybersecurity Research</b>	<b>3 Credits</b>
<b>Offered:</b> every spring.		A research experience in Cybersecurity conducted with and under the supervision of a faculty advisor.	
<b>CYB 610 Cybersecurity Project</b>	<b>3 Credits</b>	<b>Prerequisite:</b> CYB 500/L and program director approval.	
This course requires the culmination of knowledge and laboratory experience gained from the MS in Cybersecurity program as students will have the opportunity to design and implement a graduate capstone project. Students may complete this project for a real-world application or in a laboratory-setting that pertains to the greater field of cybersecurity. Students must defend their work in an open project defense and complete a written report of their work before a letter grade is awarded.		<b>Offered:</b> as needed.	
<b>Prerequisite:</b> CYB 520.		<b>CYB 697 Cybersecurity Internship</b>	<b>3 Credits</b>
<b>Offered:</b> every fall, spring, & summer.		The application of the knowledge and skills acquired from the MS in Cybersecurity program in a real-world professional setting. Students will be responsible for arranging a practicum/internship with a business or organization that is related to cybersecurity. The outline of work duties and evaluative methods are established by the student and the internship mentor/supervisor and approved by the faculty advisor prior to initiation of the course.	
<b>CYB 611 Cybersecurity Thesis</b>	<b>3 Credits</b>	<b>Prerequisite:</b> CYB 500.	
The purpose of the thesis course is to provide students the opportunity to work with a faculty advisor on a research problem in cybersecurity. Completion of the thesis will require scholarly research methods to produce a significant thesis document that is comparable to a peer-reviewed publication. This course should be taken during the last semester of the MS program and the final thesis and oral presentation (defense) will be evaluated by a faculty committee before a grade is awarded.		<b>Offered:</b> every fall, spring, & summer.	
<b>Prerequisite:</b> CYB 610.		<b>CYB 699 Advanced Cybersecurity Topics</b>	<b>3 Credits</b>
<b>Offered:</b> every fall & spring.		In depth study of a topic related to cybersecurity.	
		<b>Prerequisite:</b> permission of instructor.	
		<b>Offered:</b> occasionally.	