School of Cybersecurity

Web Site: https://www.odu.edu/cyber (https://www.odu.edu/cyber/)

Holly Handley, Dean (Interim)
Daniel Takabi, Director

The School of Cybersecurity administers a BS in Cybersecurity, a BS in Cybersecurity with a major in Cyber Operations, a BS in Cybersecurity with a major in Cyber Risk Management, an MS in Cybersecurity, and an interdisciplinary minor in cybersecurity. The School's strategic priority is to deliver exceptional academic programs for both resident and online students to cultivate the cybersecurity workforce and enhance the nation's cybersecurity talent. The School supports undergraduate and graduate students and faculty to achieve healthy and sustainable growth of the cybersecurity program. The mission of the School also includes developing high-impact, cross-disciplinary research initiatives that center on cybersecurity and conducting outreach and community engagement, being a source of cybersecurity expertise to the community, the Hampton Roads region, the Commonwealth of Virginia, and the nation.

Programs

Bachelor of Science Programs

- Cybersecurity (BS) (http://catalog.odu.edu/undergraduate/cybersecurity/cybersecurity-bs/)
- Cybersecurity with a Major in Artificial Intelligence for Cybersecurity (http://catalog.odu.edu/undergraduate/cybersecurity/cybersecurity-artificial-intelligence--for-cybersecurity-bs/)
- Cybersecurity with a Major in Cyber Operations (BS) (http://catalog.odu.edu/undergraduate/cybersecurity/cybersecurity-cyber-operations-bs/)
- Cybersecurity with a Major in Cyber Risk Management (BS) (http://catalog.odu.edu/undergraduate/cybersecurity/cybersecurity-cyber-risk-management-bs/)

Certificate Program

- Cyber Risk Management Certificate (http://catalog.odu.edu/undergraduate/cybersecurity/cyber-risk-management-certificate/)

Minor Program

- Cybersecurity Minor (http://catalog.odu.edu/undergraduate/cybersecurity/cybersecurity-minor/)

Courses

Cybersecurity (CYSE)

CYSE 001 Cybersecurity SFS LeADERS (0 Credit Hours)
This course outlines the curricular and co-curricular requirements for Scholarship for Service Students in the Cyber LeADERS program.

CYSE 100 Cyber Explorers and University Orientation (1 Credit Hour)
This course provides an introduction to cyber hygiene and orientation to university life.

CYSE 200T Cybersecurity, Technology, and Society (3 Credit Hours)
Students will explore how technology is related to cybersecurity from an interdisciplinary orientation. Attention is given to the way that technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

CYSE 201S Cybersecurity and the Social Sciences (3 Credit Hours)
This course addresses the social, political, legal, criminological, and economic dimensions of cybersecurity through a social science framework. Students are introduced to a human-factors approach to understanding cybersecurity threats. Attention is given to the social factors that contribute to cyber incidents and the political and legal mechanisms that are developed to control the behaviors of those who create risks and cybersecurity incidents. The class also explores how cybersecurity is studied by social scientists in various social science disciplines.

CYSE 202G Information Literacy for Cybersecurity (3 Credit Hours)
This course provides an in-depth introduction to information literacy from library and information science, information ethics, and computer science perspectives along with applications to cybersecurity research and professional activity. This course is aligned with Old Dominion University's general education learning outcomes for information literacy.
Prerequisites: ENGL 110C

CYSE 250 Basic Cybersecurity Programming and Networking (3 Credit Hours)
This course introduces the cybersecurity-centric programming and networking concepts. Students will develop problem solving skills by using low-level programming languages (including C and assembly) and learn fundamentals of network protocols. This course is the technical base for students to take cybersecurity major courses. No prior knowledge of programming and networking is assumed.
Prerequisites: MATH 162M or higher

CYSE 270 Linux System for Cybersecurity (3 Credit Hours)
This course introduces the basic operations in major Linux distros for cybersecurity using both graphical interface and command line interface. Students will learn about the basic installation and configuration, file systems management, shell scripts, and user authentication in Linux systems. This course is the technical base for students to take cybersecurity major courses.

CYSE 280 Windows System Management and Security (3 Credit Hours)
This course introduces tools and techniques used to configure, manage and implement Windows and its security-related features. Students will install, configure, manage and secure Windows client & server operating systems and related networking environment using a variety of software tools. This course also details how to mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server, secure virtualization platform, and use new deployment options for enhancing the security.

CYSE 300 Introduction to Cybersecurity (3 Credit Hours)
This course provides an overview of the field of cybersecurity. It covers core cybersecurity topics including computer system architectures, critical infrastructures, cyber threats and vulnerabilities, cryptography, information assurance, network security, and risk assessment and management. Students are expected to become familiar with fundamental security concepts, technologies and practices, and develop a foundation for further study in cybersecurity.
Prerequisites: MATH 162M or permission of the instructor

CYSE 301 Cybersecurity Techniques and Operations (3 Credit Hours)
This course introduces tools and techniques used to secure and analyze large computer networks and systems. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform forensic investigation, and practice techniques for penetration testing.
Prerequisites: MATH 162M and CYSE 270 or permission of the instructor

CYSE 368 Cybersecurity Internship (3-6 Credit Hours)
Internships provide a personalized exploration of structured employment within the major. This course mandates an initial or ongoing internship that the student obtains, as assignments are rooted in their concurrent internship experience. Course assignments will define the employment relationship, articulate learning outcomes, and offer opportunities for reflection to enhance the student's academic, career, and professional readiness. Students must complete 50 hours of site work per course credit.
Prerequisites: The student's internship placement must be coordinated with the site supervisor and approved by the School of Cybersecurity's Internship Director

CYSE 395 Topics in Cybersecurity (1-3 Credit Hours)
Study of selected topics in cybersecurity.
Prerequisites: junior standing

CYSE 404 Law and Digital Forensics (3 Credit Hours)
This course will focus on the intersection of digital forensics and the criminal justice system, namely how digital forensics is understood and applied to key criminal justice, constitutional and statutory considerations within the criminal justice system. Students will explore such topics as the nature and types of cybercrime; search and seizure principles in the digital world; finding, handling and maintaining chain of custody of digital evidence; interviewing individuals relating to digital evidence and related activities; and testifying in court about digital evidence matters.
Prerequisites: Junior standing or permission of instructor

CYSE 406 Cyber Law (3 Credit Hours)
This course tackles two major cyber law subjects. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from traditional civil, and to a lesser extent, traditional criminal perspectives. The second part will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace are in compliance with U.S. law, regulations, directives and policies. The course will also introduce students to miscellaneous cybersecurity topics such as the Federal Acquisition Requirements.
Prerequisites: junior standing

CYSE 407 Digital Forensics (3 Credit Hours)
This course introduces the basic concepts and technologies of digital forensics. Students will learn the fundamental techniques and tools utilized for collecting, processing, and preserving digital evidence on computers, mobile devices, networks, and cloud computing environments. Students will also engage in oral and written communication to report digital forensic findings and prepare court presentation materials.
Prerequisites: declared major and junior standing

CYSE 409 Crime and Computer Applications (3 Credit Hours)
The purpose of this interdisciplinary course is to introduce students to the ways in which computers are involved in the commission and the investigation of crime. Students will learn the fundamentals of cryptography and steganography and the tools used to perform these activities Students will also use forensic software to identify, gather, and verify relevant digital evidence. Cross-listed with CRJS 409.
Prerequisites: CRJS 310 or permission of instructor

CYSE 410/510 Artificial Intelligence (AI) Methods and Models (3 Credit Hours)
This course offers an introduction to Artificial Intelligence (AI). Students will explore the field's fundamental concepts, techniques, and applications. Methods, such as Generative AI (GenAI) that enable machines to learn and process information, and models, such as machine learning (ML) that uses data sets to recognize patterns and make decisions without human intervention will be covered. The course is designed for non-specialists and does not require prior computer science or programming knowledge.
Prerequisites: Permission of the instructor

CYSE 416/516 Cyber Defense Fundamentals (3 Credit Hours)
This course focuses on cybersecurity theory, information protection and assurance, and computer systems and networks security. The objectives are to understand the basic security models and concepts, learn fundamental knowledge and tools for building, analyzing, and attacking modern security systems, and gain hands-on experience in cryptographic algorithms, security fundamental principles, and Internet security protocol and standards. (Offered fall)
Prerequisites: permission of the instructor
Pre- or corequisite: ECE 355 or equivalent or permission of the instructor

CYSE 417 Digital Leadership (3 Credit Hours)
This course explores technology as it relates to leadership experiences. Theories, case studies and real world examples are analyzed to show both successful and unsuccessful uses of online and digital approaches that inform leaders' communication strategies. Students will explore how their own digital identities may impact their futures as leaders. They will also learn how to create digital identities that will shape their professional identities throughout their careers.
Prerequisites: Junior standing or permission of instructor

CYSE 419/519 Cyber Physical System Security (3 Credit Hours)
Cyber Physical Systems (CPS) integrate computing, networking, and physical processes. The objectives of this course are to learn the basic concepts, technologies and applications of CPS, understand the fundamental CPS security challenges and national security impact, and gain hands-on experience in CPS infrastructures, critical vulnerabilities, and practical countermeasures.
Prerequisites: ECE 355 or permission of the instructor

CYSE 420/520 Applied Machine Learning in Cybersecurity (3 Credit Hours)
This course introduces the concepts and technologies of machine learning with a focus on applications related to cybersecurity. The objectives are to learn fundamental knowledge and practical experience and identify the use case of machine learning techniques in cybersecurity. The course will discuss traditional and advanced machine learning techniques, e.g., neural network, deep convolutional neural network, generative adversarial network, and transfer learning algorithms. Students will engage in oral and written communication by reporting and presenting the materials of the course project.
Prerequisites: CYSE 250 or permission of the instructor

CYSE 421/521 Generative AI in Cybersecurity (3 Credit Hours)
This course provides an in-depth examination of the intersection between Generative AI (Gen AI) and Cybersecurity. It focuses on the dual nature of advanced AI systems as both enhancers and potential threats to security infrastructure. Students will acquire a comprehensive understanding of the underlying principles, algorithms, and practical applications of Gen AI models in the discovery of attack vectors, identification of cyber threats, and automation of security tasks. Additionally, the course will address defensive strategies aimed at mitigating the risks stemming from AI-driven cyberattacks.
Prerequisites: Permission of instructor

CYSE 425W/525 Cybersecurity Strategy and Policy (3 Credit Hours)
This writing intensive course explores cybersecurity policy and strategy and introduces students to the essentials of strategy development and policy making in cybersecurity. Topics considered include planning principles in cyber strategy; risk management and cybersecurity policy; the connections between cybersecurity policies, businesses, and governmental institutions; the knowledge, skills, and abilities needed to develop and implement cybersecurity policy; the social, political and ethical implications that arise in cybersecurity policies and strategies; strategies to assess cybersecurity policy; and the ties between national security and cybersecurity policy.
Prerequisites: ENGL 110C and ENGL 211C or ENGL 221C or ENGL 231C with a grade of C or better and CYSE 200T or IT 200T or POLS 101S

CYSE 426/526 Cyber War (3 Credit Hours)
This course explores the national security dimensions of cybersecurity and examines cyber war in international relations. Exploration of cyber war begins with an examination of cybersecurity as a component of national security and investigates the topics of U.S National Cybersecurity and other national approaches to cyber war. The topics of cyber deterrence, cyber as a military domain, the roles of international organizations in cyber war, cyber terrorism, the role of social media, and information warfare will be discussed. The international dimension of cybersecurity is also discussed.
Prerequisites: CYSE 200T or POLS 101S or permission of the instructor

CYSE 430/530 Introduction to Cybersecurity Risk Management (3 Credit Hours)
This course addresses the broad topic of risk management and how risk, threats, and vulnerabilities impact information systems. Areas of instruction include how to assess and manage risk based on defining an acceptable level of risk for information systems. Elements of a business impact analysis (BIA), business continuity plan (BCP), disaster recovery plan (DRP), and computer incident response team (CIRT) plan will also be discussed.
Prerequisites: CYSE 300

CYSE 431/531 Advanced Techniques Cybersecurity Risk Management (3 Credit Hours)
Expert-level approach on the Risk Management Framework (RMF) system Authorization to Operation (ATO), including Continuous cATO. Curriculum that is aligned to the NIST SP 800-53, Revision 5. Advanced topics include Assess and Authorize, System Categorization, Security Control Assessment, System Test Results, Plan of Action and Milestones (POA&M), and Continuous Monitoring (CONMON).
Prerequisites: CYSE 430

CYSE 432/532 Cyber Risk CSF/CMMC (3 Credit Hours)
This course introduces cybersecurity, the NIST Cybersecurity Framework (CSF), and the Cybersecurity Maturity Model Certification (CMMC) program. Topics to be addressed include the risk management fundamentals, IT risk management, and cyber risk controls; cyber threats and vulnerabilities; data security and sanitization; the NIST CSF, including its core functions, categories, and subcategories; and the CMMC comprising its levels, domains, and implementation guidelines.
Prerequisites: CYSE 431

CYSE 433/533 Cyber Risk FedRAMP/Audit (3 Credit Hours)
This course explores the Federal Risk and Authorization Management Program (FedRAMP) and Auditing. Topics to be addressed include an overview of the FedRAMP framework, including its objectives, components, and stages; the needed documents and guidelines to develop system security plans and security assessment reports; the NIST Risk Management Framework (RMF) comprising its different stages and the adoption mechanism; FISMA compliance and auditing assessment; and real-world case studies and future challenges.
Prerequisites: CYSE 432

CYSE 450 Ethical Hacking and Penetration Testing (3 Credit Hours)
This course introduces the basic terminologies used in ethical hacking and useful tools in relation to penetration testing on Kali Linux. Students will learn to explore the vulnerabilities in various systems and operate the industry-leading tools and framework to perform the penetration testing on different target systems.
Prerequisites: CYSE 270 and CYSE 301 or permission of the instructor

CYSE 494 Entrepreneurship in Cybersecurity (3 Credit Hours)
This course is designed to help students enhance their personal and professional development through innovation guided by faculty members and professionals. It offers students an opportunity to integrate disciplinary theory and knowledge through developing a nonprofit program, product, business, or other initiative. The real-world experiences that entrepreneurships provide will help students understand how academic knowledge leads to transformations, innovations, and solutions to different types of problems. The course can be delivered either as an independent project for individual students or as group projects similar to those sometimes offered in topics courses.
Prerequisites: Approval by the Director of the Center for Cybersecurity Education and Research

CYSE 495/595 Topics in Cybersecurity (1-3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described in information distributed to academic advisors.
Prerequisites: permission of the instructor

CYSE 497/597 Tutorial Work in Special Topics in Cybersecurity (1-3 Credit Hours)
Independent reading and study on a topic to be selected under the direction of an instructor. Conferences and papers as appropriate.
Prerequisites: Senior standing and approval of the instructor