The University of Arkansas is one of the founding institutions of the NCTA. The program at UALR is 18 credits, delivered synchronously online. The courses are listed below. *Course substitutions accepted with permission of the program coordinator

CSEC 7310 - Foundations of Cybersecurity (Required)

Covers the broad topics of cybersecurity thought including adversarial thinking, risk management, legal and ethical foundations, privacy, human psychology, system thinking, ubiquitous computing, and trust and assurance.

CSEC 7320 - Cybersecurity Operations (Required)

This course examines the processes and technology to defend cyber systems against adversarial threats. Students will develop skills to plan and implement a cybersecurity operations strategy to align with organizational risk.

CSEC 7301 - Teaching Cybersecurity (Required)

This comprehensive course delves into essential aspects of teaching cybersecurity. It explores curriculum guidelines, diverse curriculum models, effective pedagogical strategies, and a wide array of instructional tools and cutting-edge technologies.

CSEC 5318 - Cybersecurity Practicum (Required)

This course offers practical experience in cybersecurity operations through service projects, research, or industry engagement. Students collaborate in real-world cybersecurity environments, applying their knowledge to develop, implement, test, and document security controls.

CSEC 5320 - Privacy Law, Policy and Compliance*

Explores cybersecurity ethics, laws, and policies, emphasizing cybercrime's legal aspects and regulatory compliance frameworks. It fosters understanding of cybersecurity's societal, global, economic, and legal implications.

CSEC 5340 - Advanced Digital Forensics and Incident Response*

This course equips students with the skills for forensic analysis, log preservation, and report creation, preparing them for digital forensics and incident response professions through technical and communication expertise.

UALR Contact: Sandra Leiterman, saleiterman@ualr.edu

National Cybersecurity Teaching Academy

UNIVERSITY OF LOUISVILLE

The University of Louisville is one of the founding institutions of the NCTA. The program at UofL requires 18 credits to qualify for NCTA. It is delivered asynchronously online. The courses are listed below.

CSE 564 - Introduction to Cryptography (Required)

This course introduces the history of cryptology and secret codes. It covers substitution ciphers, transposition codes, polyalphabetic substitutions, rotor machines, bit block ciphers (e.g., DES), and public key encryption (RSA, Knapsack codes, Diffie-Hellman key exchange).

CSE 566 - Information Security (Required)

Technical, legal and policy issues associated with information security. Authentication, trusted computer systems, information encryption, biometrics, computer forensics, and privacy issues. Written and verbal reports are required.

CSE 568 – Computer Forensics (Required)

Course examines legal, legal, administrative, technical and scientific issues in computer forensics, network forensics, information security and trusted systems. Course requires class participation, lab work, team projects, writing and oral presentations.

CSE 590 - Teaching Cybersecurity (Required)

This course delves into essential aspects of teaching cybersecurity.
It explores curriculum guidelines, diverse curriculum models, effective pedagogical strategies, and a wide array of instructional tools and cutting-edge technologies.

Elective Choices:

CSE 590 Computer & Cyber Security
CSE 613 Network Security

Elective Choices:

CSE 631 DatabaseSecurity
CSE 694 ST: Security Projects

UofL Contact: Leigh Ann Elles, leigh.elles@louisville.edu

National Cybersecurity Teaching Academy

WPI

Worcester Polytechnic Institute (WPI) is the newest NCTA institution. The program at WPI is 18 credits, delivered synchronously online. The courses are listed below.

CS 591: Fundamentals in Cybersecurity for Teachers

This course covers network and computer security, addressing intrusion methods, privilege escalation, and defense strategies. Topics encompass networking, OS fundamentals, vulnerabilities, cyber defenses, and security administration.

CS 592: Introduction to Digital Forensics for Teachers

This course explores digital forensics, including forensic lab environment, data acquisition, electronic discovery, legal aspects, technical methodologies in Linux, Mac, and Windows forensics, data hiding and steganography, network, and mobile forensics.

CS 593: Cybersecurity Teaching Methods

This course covers cybersecurity guidelines (e.g., HSCCG, CSEC, CAE Knowledge Units, NCWF) and effective teaching methods, including cultural relevance, knowledge scaffolding, differentiation, assessment, and instructional technologies (e.g., CTFs, competitions).

CS 571: Case Studies in Computer Security

This course examines security challenges and failures holistically, taking into account technical concerns, human behavior, and business decisions. Using case studies, students will explore the interplay among these dimensions in creating secure computing systems and infrastructure.

CS 594: Advanced Digital Forensics and Incident Response for Teachers

This course covers computer forensics fundamentals and focuses on providing practical hands-on experiences. Students learn to use practical digital forensic tools for evidence data acquisition and analysis, data recovery, file system analysis, file carving, data hiding, and network forensics.

CS 587: Cyber Security Capstone Experience

The capstone project has students apply security concepts to real-world problems. Students will propose a project idea in cybersecurity in writing with concrete milestones, receive feedback, and pursue the proposal objectives.

WPI Contact: Xiaoyan (Sherry) Sun, xsun7@wpi.edu

National Cybersecurity Teaching Academy

SACRAMENTO STATE

The program at Sacramento State University is 18 credits, delivered synchronously online. The courses are listed below.

CSC 296T: Fundamentals in Cybersecurity for Teachers

This course covers network and computer security, addressing intrusion methods, privilege escalation, and defense strategies. Topics encompass networking, OS fundamentals, vulnerabilities, cyber defenses, and security administration.

CSC 296U: Introduction to Digital Forensics for Teachers

This course explores computer forensics, including cyber-crime scene analysis, electronic discovery, legal aspects, technical methodologies (Linux, Mac, and Windows), data hiding, file recovery, network, and mobile forensics through practical digital tool activities.

CSC 296V: Cybersecurity Teaching Methods for Teachers

This course covers cybersecurity guidelines (e.g., HSCCG, CSEC, CAE Knowledge Units, NCWF) and effective teaching methods, including cultural relevance, knowledge scaffolding, differentiation, assessment, and instructional technologies (e.g., CTFs, competitions).

CSC 296W: Cybersecurity Practicum for Teachers

This course offers hands-on experience in cybersecurity operations through service projects, research, or industry engagement. Students apply their knowledge in developing, implementing, testing, and documenting security controls in real-world settings.

CSC 153: Computer Forensics Principles and Practices

This course covers computer forensics fundamentals, cyber-crime scene analysis, and electronic discovery. Students learn technical methods for security incident investigations, file system analysis, data hiding, and network forensics.

CSC 154: Computer System Attacks and Countermeasures

This course introduces network and computer security, covering intrusion methods, privilege escalation, and system defense. Topics include perimeter defenses, intrusion detection, social engineering, and various attack types.

Sacramento State Contact: Jun Dai, jun.dai@csus.edu

National Cybersecurity Teaching Academy

DAKOTA STATE UNIVERSITY

The program at the Dakota State is 18 credits, delivered asynchronously online. The courses are listed below.

CSC 611 - Cyber Leadership and Ethics

This course explores the critical intersection of leadership and ethics in the realm of cybersecurity and technology. Educators learn how to guide their students in understanding the ethical implications of cyber activities, fostering responsible behavior, and making ethical decisions in a digital world.

CSC 613 - Artificial Intelligence for Educators

This course focuses on the knowledge needed to teach K-12 students about AI concepts and applications. Educators will learn to break down complex AI topics into digestible lessons suitable for different age groups.

CSC 617 - Cybersecurity for Educators

This course equips educators to teach K-12 students about cybersecurity principles and practices. Educators explore various cyber threats, hacking techniques, and protective measures. They develop strategies for translating technical information into engaging and accessible lessons.

CSC 626 - Computer Programming for Educators

Educators develop fundamental computer programming skills. They discover creative ways to introduce coding concepts to students of different ages and skill levels, fostering computational thinking and problem-solving abilities.

CSC 653 - Hardware and Networking for Educators

This course provides educators with a comprehensive understanding of computer hardware components, architecture, and networking basics. They gain the knowledge and teaching strategies necessary to explain complex technical concepts.

CSC 683 - Cybersecurity Practicum

This course focuses on either facilitating K-12 students' hands-on experiences in cyber-related projects, action research, or a thesis option. Educators learn to guide students through the process of applying their theoretical knowledge in real-world settings.

Dakota State Contact: Fenecia Homan, fenecia.homan@dsu.edu

National Cybersecurity Teaching Academy

DePaul University

DePaul University is one of the founding institutions of the NCTA. The program at DePaul is 18 credits, delivered synchronously online. The courses are listed below.
*Course substitutions accepted with permission of the program coordinator

CST400 - Cybersecurity Pedagogy

This course aids cybersecurity educators in teaching effectively, starting with cybersecurity frameworks. It covers pedagogical content knowledge, culturally-relevant approaches, assessment, instructional technologies, and integrating cybersecurity into existing programs.

CST401 - Foundations of Cybersecurity

This course introduces key cybersecurity concepts and practices, emphasizing the security landscape and foundational principles. It covers data, system, and network security, along with human-centric aspects. Students engage in cybersecurity research to address emerging threats and take ownership of their projects.

CST402 - Applied Social Engineering:

Students Investigate social engineering attacks in controlled labs, developing technical, policy, and risk management responses. Including mechanics, persuasion, defense, ATD, false information, ethics, and automation. The final project entails creating and testing a machine learning tool for detecting phishing emails or Twitter trolling.

CST403 - Online M/Disinformation Operations

This hands-on course explores information operations, m/disinformation online. Topics include fact-checking, automated detection, evasion, and the lifecycle of alternative narratives, with historical context. Students work on implementing VoxPop, a social media platform for managing misinformation.

CST404 - Human-Center Security

This course applies behavioral theories in cybersecurity, covering economic decision-making, biases, signal detection, and more. Students undertake individual projects applying these theories to practical cybersecurity scenarios, with recommended readings outside of assignments.

CST405 - Cybersecurity Practicum

This course focuses on designing and executing practical cybersecurity projects. It covers defining assumptions, data collection, analysis, and implications for cybersecurity science and practice. Project topics include network, software, system security, cyber-physical systems security, and human-centered security.

DePaul Contact: Filipo Sharevski, fsharevs@cdm.depaul.edu

National Cybersecurity Teaching Academy

THE UNIVERSITY OF ARIZONA

The program at the University of Arizona is 18 credits, delivered asynchronously online. The courses are listed below. Course substitutions approved by the department.

CYBV 500: Security Programming

Advances the concepts and principles of development of practical applications supporting cybersecurity and digital investigation activities created through Python programming. Students will build on programming fundamentals using Python elements, secure programming standards, and developing applications for cybersecurity.

CYBV 501: Principles of Cybersecurity

Advances the concepts and principles of cybersecurity across different disciplines, threats, and technologies. Students will examine cybersecurity attackers' techniques, skills, motives, and vulnerabilities within programming, operating systems, networks, data, and web interfaces.

CYBV 529: Cyber Law, Ethics, and Policy

Provides students with an advanced look at the ethical, legal, and policy issues that arise in the field of cyber and technology. Students will gain the knowledge to operate in the current cyber and technology landscape, and the tools to analyze and respond to issues in this complex and evolving landscape.

CYBV 626: Traffic Analysis

Examines the methods by which today's security protocols and their implementations are deemed secure and reliable. Students will examine and research methods for quantifying the level of protection provided by existing protocols, including formalized approaches to this type of assessment.

CYBV 660: Zero Trust Defensive Techniques

Explores the implemtation of Zero Trust Architecture (ZTA) principles in a legacy network. Students will address quatify effectiveness as ZTA is incrementally implemented in design and architecture before addressing cloud security topics in data, platform, infrastructure, apps, operations, and risk & compliance.

CYBV 696: Special Topics

Aids cybersecurity educators in understanding concepts to develop materials for their students. Cybersecurity topics include foundational knowledge units, first principles, and risk management. Students will focus on instructional technologies, competitions, courseware, and integrating curriculum.

University of Arizona Contact: Paul Wagner, paulewagner@arizona.edu

National Cybersecurity Teaching Academy

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

The program at the UMGC is 18 credits, delivered asynchronously online. The courses are listed below.

CTCH 605 Introduction to Cybersecurity

A study of the basics of cybersecurity and the application of cyber methodologies to cyber architectures, services, protocols, algorithms, software components, and programming languages. Focus is on becoming familiar with the important roles that security management, security architecture, operations security, and physical security play in cybersecurity. Discussion covers the impact of cyber terrorism and national security on cybersecurity. Activities include hands-on, real-world experience with state-of-the-art tools and technologies in a lab-intensive environment.

CTCH 615 Cybersecurity Threats and Analysis

An introduction to tools and tactics to manage cybersecurity threats, identify various types of common threats, analyze organizational exposure to threats, and collect and analyze cybersecurity intelligence. The goal is to analyze common security failures and identify specific design principles that have been violated. Emphasis is on the interaction between security and system usability and the importance of minimizing the potential for harm by modern threats, attacks, and usability challenges.

CTCH 625 Cybersecurity for Systems and Networks

A study of key security issues and procedures in systems and networks. The objective is to identify security issues within LANs, WANs, and network operating systems; identify system threats and network infrastructure design weaknesses; determine security flaws in the network infrastructure protocols; and explain the security of data at rest in systems. Topics include modern systems and network hardening tools, techniques, and practices.

CTCH 645 Cyber Exploitation Methodologies

A comprehensive study of cyber exploitation methodologies. The objective is to identify the latest tools, techniques, and ethical hacking practices. Emphasis is on applying state-of-the-art tools and technologies in a lab-intensive environment that provides hands-on, real-world experience.

CTCH 665 Digital Forensics and Incident Response

A detailed exploration of the tools and technologies commonly used in forensic examinations best practices. Topics include procedures for securing and validating evidence, including digital media and physical memory, and for recovering artifacts and analyzing, reporting, and presenting results in both criminal and civil situations. Experience with mobile forensic analysis is provided.

CTCH 651 Cybersecurity Pedagogy

An advanced examination of methods of teaching cybersecurity to high school students. The objective is to examine educational guidelines and frameworks related to cybersecurity, equipping learners with pedagogical content knowledge necessary to transform cybersecurity subject matter into student learning. Topics include culturally relevant teaching methods, scaffolding, differentiation, assessment, and cybersecurity instructional technologies.

UMGC Contact: Dr. Brandie Shatto brandie.shatto@umgc.edu