

College/Department: EDU

Term: Extended Summer 2025

Number: 555

Credits: 4

Section: 50

Lecture: MC 122 for in-person activities

CRN: xxxxx

Lab: Hybrid (see course schedule for detail)

Contact Hours: 65

Course Dates: June 11– October 31, 2025

Instructor Information

Name: Dianne Burke

Office: MC 407

Phone: 243-7842

Email: dianne.burke@umontana.edu

Office Hours: By appointment

Course Description

Cybersecurity Foundations for K12 Educators prepares participants to incorporate cybersecurity topics into existing curricula and/or to teach ITS 130 *Cybersecurity Essentials* as a dual enrollment offering. Course materials include in-person and video lectures, hands-on lab activities, small group work, and discussion to learn basic cybersecurity concepts.

Course content is grouped into pre-workshop/workshop/post-workshop segments. The pre-workshop segment (10 contact hours) combines synchronous online activities with independent study, and covers course organization, online resources, and initial exposure to cybersecurity topics. The 40-hour workshop occurs in person and pairs deeper exploration of cybersecurity topics with hands-on reinforcement lab activities. During the workshop participants will devote time to cybersecurity lesson plan development. The post-workshop segment (15 contact hours) combines synchronous online activities with independent study and is focused on finalizing lesson plans for the upcoming school year. Participants will also explore a synchronous online cyber competition environment that could be incorporated into lesson plans.

Course Outcomes

- Learn the 7 essential GenCyber concepts: Confidentiality, Integrity, Availability, Defense in Depth, Think Like an Adversary, Simplicity, Computer Ethics.
- Investigate foundational cybersecurity concepts: Basic Networking; Threats and Vulnerabilities; Authentication; Password Security; Hardware Devices; Offensive and Defensive Strategies; and Wireless Security.
- Conduct hands-on activities with social network security, phishing, cryptography, computer ethics, web security, reconnaissance, and cyber defense strategies.
- Explore the UM high school dual enrollment course ITS 130 – Essential Cybersecurity for potential incorporation of content into existing district curricula.
- Utilize online resources for potential incorporation into existing district curricula and to further individual knowledge.
- Develop lesson plans that integrate cybersecurity and privacy concepts.
- Consider how to incorporate Indian Education for All into cybersecurity curricula.
- Optionally use the CompTIA TestOut courseware to prepare for the Security+ certification examination. A voucher for the Security+ certification examination will be provided at no cost to interested participants.

Resources

There is no required text. The course will use a variety of materials to facilitate learning.

Participants will be registered on the Montana Cyber Range as a course supplement. There is no charge to access or use the Range. The course instructor will handle registration tasks and, after receiving an email from the Range, students will complete the registration process.

Participants will have access to the ITS 130 Canvas course shell as part of EDU 555.

If desired, participants will be provided access to the TestOut LabSim Security Pro materials, which serve as preparatory material for the CompTIA Security+ certification exam. There is no charge to access or use the Security Pro materials. The course instructor will handle registration tasks and, after receiving an email from the platform, students will complete the registration process.

If desired, participants will be provided one pre-paid voucher for the CompTIA Security+ certification exam.

Grading

During the course you'll be graded in two areas: lesson homework assignments and lesson plan development.

Assessment:	Weight:
Lesson Homework/Written Assignments	75%
Lesson Plan Development	25%

Grading Scale:	Letter Grade:
90-100%	A
80-89%	B
70-79%	C
60-69%	D

Lesson homework and written assignments

This is worth 75% of your grade. All lessons will have homework assignments that are taken from the presented material.

Many lessons will include a written assignment. Students should submit professionally written responses using correct grammar, spelling, and sentence structure.

Non-lesson plan homework from the in-person workshop is due by **Sunday, August 3, 2025 at 11:55 p.m.**

Lesson Plan Development

This category is worth 25%. Key elements to include are:

- **Define Learning Objectives:** Clearly state what students should learn from the lesson.
- **Connect to Prior Knowledge:** Establish a foundation of what students already know and build upon it.
- **Provide Engaging Instruction:** Utilize various teaching methods, such as direct instruction, guided practice, and independent practice, to keep students actively involved.
- **Include Differentiation:** Consider the diverse needs of learners and provide activities that accommodate different learning styles.
- **Assess Learning:** Use various assessment methods (e.g., observations, quizzes, projects) to gauge student understanding and provide feedback.

Two completed lesson plans are due **Wednesday, August 27, 2025 at 11:55 p.m.**

Asking Questions and Communicating with course instructor:

I monitor the Q&A forum in the Canvas shell daily Monday-Friday and check email regularly. I will respond within 24 hours Monday – Friday 8:00 a.m. to 5:00 p.m., and often within a shorter timeframe than 24 hours. Messages received after 5:00 p.m. Friday and over the weekend will be answered on the next business day.

Disability Statement

The University of Montana assures equal access to instruction through collaboration between students with disabilities, instructors, and the Office for Disability Equity (ODE). If you anticipate or experience barriers based on disability, please contact the ODE at: (406) 243-2243, ode@umontana.edu, or visit www.umt.edu/disability for more information. Retroactive accommodation requests will not be honored, so please, do not delay. As your instructor, I will work with you and the ODE to implement an effective accommodation, and you are welcome to contact me privately if you wish.

Scholarly Conduct

- All students must practice academic honesty. Academic misconduct is subject to an academic penalty by the course instructor and/or a disciplinary sanction by the University. All students need to be familiar with the Student Conduct Code. <https://www.umt.edu/missoula-college-learning-center/testing/student-code-of-conduct-2021-pdf>
- Plagiarism, cheating, or direct use of online resources without proper attribution will result in a deduction of points no less than 20% of the total points for the assignment to a zero on the assignment at the instructor's discretion.
- All students are expected to respect the opinions and dignity of all members of the class and act in a dignified manner.
- Using the Internet to research materials and concepts is an integral part of learning in the twenty-first century. Studying with other students is a productive method of learning. A certain amount of collaborating on concepts with other students and using resources found on the Internet in an assignment is recommended. However, copy and paste is not acceptable.

Professionalism

All correspondence and work performed in the course should be completed in a professional manner and be of business quality.

Tentative Course Schedule Extended Summer 2025

Pre-Camp Activities (held online via Zoom). 10 hours total.

- **June 11 6:00 p.m. – 7:00 p.m.** – Program Overview; Course Shell; US Cyber Range; TestOut Platform; Syllabus and Schedule. 1 additional hour of independent work.
- **June 18 6:00 p.m. – 7:00 p.m.** – Confidentiality and Integrity in Cybersecurity; Hands-On Activities. 1 additional hour of independent work.
- **June 25 6:00 p.m. – 7:00 p.m.** – Availability and Defense in Depth in Cybersecurity: Hands-On Activities. 1 additional hour of independent work.
- **July 2 6:00 p.m. – 7:00 p.m.** – Adversarial Thinking and Simplicity in Cybersecurity; Hands-On Activities. 1 additional hour of independent work.
- **July 9 6:00 – 7:00 p.m.** – Computer Ethics; Hands-On Activities. 1 additional hour of independent work.

Post-Camp Activities (held online via Zoom). 15 hours total.

- **July 30 6:00 p.m. – 8:00 p.m.** – Lesson Plan Sharing and Discussion. 3 additional hours of independent work.
- **August 27 6:00p.m. – 8:00 p.m.** – Lesson Plan Sharing and Discussion. 3 additional hours of independent work.
- **October TBD (16 or 17)–** Capture the Flag online activity, Program Feedback, Next Steps. 5 hours.

Camp Activities held in-person at Missoula College July 14-18, 2025. 40 hours total. See next page for schedule.

University of Montana 2025 EDU 555 In-Person Workshop					
Tentative Schedule July 14 - 18, 2025					
Time	Monday	Tuesday	Wednesday	Thursday	Friday
8:00 AM	Welcome/Agenda				
8:15 AM	Review of Pre-Camp Lessons and Activities/NICE Framework	Access Control, Authentication, Authorization	Network and Password Attacks	Data Classification	Indian Education for All Considerations
8:30 AM					
8:45 AM				Networking and the OSI Model	Governance and Risk Management
9:00 AM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	CyberSeek and Career Options
9:15 AM					
9:30 AM					
9:45 AM					
10:00 AM	Break				
10:15 AM	Threats, Vulnerabilities, and Mitigations	Network Architecture: Devices, Firewalls, VPN	Vulnerability Management and Scanning	Hardening and Wireless Networking	Lesson Plan Development: Topic Selection and Objective Identification; Content Research
10:30 AM					
10:45 AM					
11:00 AM					
11:15 AM					
11:30 AM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	Progress Check-In/Discussion
11:45 AM					
12:00 PM	Lunch				
12:15 PM					
12:30 PM					
12:45 PM	Cryptography and Hashing	Network Architecture: Switches, Routers, and Vulnerabilities	Alerting and Monitoring: Penetration Testing	Secure Protocols; Web Application Security	Lesson Plan Development: Instructional Method Selection; Supporting Material; Student Activities; Formative and Summative Assessments
1:00 PM					
1:15 PM					
1:30 PM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	
1:45 PM					
2:00 PM					
2:15 PM					
2:30 PM	Break				
2:45 PM	Encryption and PKI	Resiliency and Site Security: Physical Threats, Reconnaissance, Intrusion Detection	Incident Response Simulation Exercise	Resources: OWASP; MITRE; NVD; CWE; CVE; CVSS	Lesson Presentations and Feedback
3:00 PM					
3:15 PM					
3:30 PM	Lab Activity	Lab Activity		Case Study Exercise	
3:45 PM					
4:00 PM	K-12 Adaptations and Implementation Discussion				
4:15 PM					
4:30 PM					
4:45 PM					
5:00 PM	Wrap-up/Reflection				

University of Montana 2025 Gencyber Summer Teacher Camp
Tentative Schedule

Time	Monday	Tuesday	Wednesday	Thursday	Friday
8:00 AM	Welcome/Agenda				
8:15 AM	Review of Pre-Camp Lessons and Activities/NICE Framework	Access Control, Authentication, Authorization	Network and Password Attacks	Data Classification	Indian Education for All Considerations
8:30 AM					
8:45 AM	Networking and the OSI Model			Governance and Risk Management	Cybersecurity Ethics
9:00 AM					
9:15 AM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	CyberSeek and Career Options
9:30 AM					
9:45 AM					
10:00 AM	Break				
10:15 AM	Threats, Vulnerabilities, and Mitigations	Network Architecture: Devices, Firewalls, VPN	Vulnerability Management and Scanning	Hardening and Wireless Networking	Lesson Plan Development: Topic Selection and Objective Identification; Content Research
10:30 AM					
10:45 AM					
11:00 AM					
11:15 AM					
11:30 AM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	Progress Check-In/Discussion
11:45 AM					
12:00 PM	Lunch				
12:15 PM					
12:30 PM					
12:45 PM					
1:00 PM	Cryptography and Hashing	Network Architecture: Switches, Routers, and Vulnerabilities	Alerting and Monitoring: Penetration Testing	Secure Protocols; Web Application Security	Lesson Plan Development: Instructional Method Selection; Supporting Material; Student Activities; Formative and Summative Assessments
1:15 PM					
1:30 PM					
1:45 PM	Lab Activity	Lab Activity	Lab Activity	Lab Activity	
2:00 PM					
2:15 PM					
2:30 PM	Break				
2:45 PM	Encryption and PKI	Resiliency and Site Security: Physical Threats, Reconnaissance, Intrusion Detection	Incident Response Simulation Exercise	Resources: OWASP; MITRE; NVD; CWE; CVE; CVSS	Lesson Presentations and Feedback
3:00 PM					
3:15 PM					
3:30 PM	Lab Activity	Lab Activity		Case Study Exercise	
3:45 PM					
4:00 PM	K-12 Adaptations and Implementation Discussion				
4:15 PM					
4:30 PM					
4:45 PM	Wrap-up/Reflection				
5:00 PM					

Any changes to the schedule will be reflected in the course shell.