DAKOTA COLLEGE AT BOTTINEAU

Course Syllabus

Course Prefix/Number/Title: CIS 141 Introduction to Cybersecurity

Number of Credits: 3 semester credits

Course Description: This course will provide an introduction to concepts related to Cybersecurity. Students will learn safe practices which can be deployed to secure computer systems. Students will gain an understanding of different tools which can be used to defend attacks on computer systems. Special emphasis will be given to systems and applications that non-CS majors will likely to encounter in daily life. In addition to lecture classes, security lab exercises will be conducted to perform hands-on experiments on safe security practices.

Pre-/Co-requisites: None

Course Objectives: Students will learn basic cyber security terminology; have skills for keeping up to date on cyber security issues; and be able to identify information assets. Identify main malware types; awareness of different malware propagation methods; and skills for preventing malware infections. Describe cryptography terminology; be able to use cryptography for email; be aware of applications of cryptography

Instructor: Trisha Haman

Office: Dakota College Downtown, 120 East Burdick Expressway - Minot

Office Hours: 9:00-10:00 MWF; noon-1:00 T, Th; virtual or office appointments available M-F between 2:00-4:00, as needed

Phone: 701-858-3313

Email: trisha.haman@dakotacollege.edu

Lecture/Lab Schedule: 1:00-1:50 MWF

Textbook(s): Open Educational Resources - No Textbook Required

Course Requirements: Grades will be calculated by dividing total points earned by total points available. You will need access to a desktop or laptop computer to take this class. You cannot use a phone, tablet or Chromebook to take this class.

Tentative Course Outline:
Week 1: Introduction and Threat Landscape
Week 2: Understanding Current Threats and Securing Digital Information
Week 3: Authentication, Passwords, Two-factor Authentication
Week 4: Endpoint Security
Week 5: Malware, Viruses and Protection
Week 6: Networking and Communications
Week 7: Privacy and Standards
Week 8: Cryptography and Encryption
Week 9: Digital Signatures and Certificates
Week 10: Network Security, Firewalls, VPN and IDS
Week 11: Cloud and Virtualization Security
Week 12: When Your Defenses Fail and Incident Response

Week 13: Laws and Computers
Week 14: Managing security risks
Week 15: Cybersecurity Resilience
Week 16: Case Project and Final

Grading Scale: A = 90-100% • B = 80-89% • C = 70-79% • D = 60-69% • F = 0-59%

General Education Competency/Learning Outcome(s) OR CTE Competency/Department Learning Outcome(s): Employs industry specific skills in preparation for workplace readiness. Learning Outcome #1: Promote and facilitate the effective integration of technology in both professional and personal use. Learning Outcome #2: Efficiently use computers, operating systems, and application software. Learning Outcome #3: Create, organize, distribute and store information. Learning Outcome #4: Employ sound problem-solving skills.

Relationship to Campus Focus: The course focuses on knowledge and application of technology. Cybersecurity is essentially applied technology with a defensive purpose. Where knowledge explains how attacks happen, application is about preventing and responding to them.

Classroom Policies:

- Students are required to complete all class activities.
- Attendance is vital to success. Absences and arrangements must be made with the instructor prior to class time.
- The instructor reserves the right to remove anyone causing disruptions or showing disrespect to others. The instructor will interpret and declare what is considered disruptive or disrespectful behavior.
- Students are to silence or turn cell phones off during class.

Student Email Policy:
Dakota College at Bottineau is increasingly dependent upon email as an official form of communication. A student's campus-assigned email address will be the only one recognized by the Campus for official mailings. The liability for missing or not acting upon important information conveyed via campus email rests with the student.

Academic Integrity:
According to the DCB Student Handbook, students are responsible for submitting their own work. Students who cooperate on oral or written examinations or work without authorization share the responsibility for violation of academic principles, and the students are subject to disciplinary action even when one of the students is not enrolled in the course where the violation occurred. The Code detailed in the Academic Honesty/Dishonesty section of the Student Handbook will serve as the guideline for cases where cheating, plagiarism or other academic improprieties have occurred.

Disabilities or Special Needs:
Students with disabilities or special needs (academic or otherwise) are encouraged to contact the instructor and Disability Support Services.

Title IX:
Dakota College at Bottineau (DCB) faculty are committed to helping create a safe learning environment for all students and for the College as a whole. Please be aware that all DCB employees (other than those designated as confidential resources such as advocates, counselors, clergy and healthcare providers) are required to report information about such discrimination and harassment to the College Title IX Coordinator. This means that if a student tells a faculty member about a situation of sexual harassment or sexual violence, or other related misconduct, the faculty member must share that information with the

College's Title IX Coordinator. Students wishing to speak to a confidential employee who does not have this reporting responsibility can find a list of resources on the DCB Title IX webpage.

AI Student Policy:
Unless otherwise indicated in the course syllabus, or in individual instructions for course assignments, or in the absence of the express consent of the course instructor, students are not allowed to utilize generative AI to help produce any of their academic work. Any violation of this policy will be considered an act of academic dishonesty as outlined within the Dakota College Code of Student Life.

RESPONSIBILITIES

Students	• Responsible to follow the syllabus and assignment instructions regarding use of generative AI for all academic work. • Obtain permission of the instructor prior to the use of generative AI that is outside of the syllabus or assignment instructions. Provide appropriate rationale for how the use of generative AI will enhance the learning experience for the assignment. • In instances where generative AI is permissible, appropriately cite the generative AI program used and indicate where in the assignment it was used, in a brief submission statement.
Faculty	• Determine if the use of generative AI could enhance student learning in any assignment of project. • Clearly indicate in all course syllabi if generative AI is allowable for any academic work. • If allowable, give specific parameters for how and when generative AI may be used. • If a violation of generative AI for the individual course/syllabus is suspected, discuss the concern with the student. If violation is still suspected, inform the appropriate semester coordinator/program director.