CYBERSECURITY, BS

Introduction

Please click here (https://catalog.ucdenver.edu/cu-denver/undergraduate/schools-colleges-departments/college-engineering-design-computing/computer-science-engineering/) to see the computer science department information.

The Bachelor of Science in Cybersecurity degree will allow undergraduate students to combine their passion for computer science with skills to defend computers, servers, mobile devices, electronic systems, networks, users and data from malicious attacks. Skills and experiences will render them immediately useful in today's workforce where cybersecurity—cyber offense and defense—is a growing concern and necessity in both the public and private sector.

Graduates will be able to apply the attained computing and security skills and knowledge to create solutions to real-world problems, and analyze, evaluate, and maintain operational systems in the presence of cyber risks and threats. Graduates will be able to:

- Analyze a complex computing and security problem and apply algorithmic reasoning to identify solutions.
- Design, implement, and evaluate a computing-based solution to meet a given set of computing and security requirements.
- Communicate and function effectively in professional contexts and teams.
- Make informed judgments in computing and security practices based on legal and ethical principles.
- Apply security principles and practices to maintain operations in the presence of threats.

Program Delivery

- This is an on-campus program.

Declaring This Major

- Click here (http://catalog.ucdenver.edu/cu-denver/undergraduate/schools-colleges-departments/college-engineering-design-computing/#policiestext) to go to information about declaring a major.

General Requirements

To earn a degree, students must satisfy all requirements in each of the areas below, in addition to their individual major requirements.

- CU Denver General Graduation Requirements (http://catalog.ucdenver.edu/cu-denver/undergraduate/graduation/)
- CU Denver Core Curriculum (http://catalog.ucdenver.edu/cu-denver/undergraduate/graduation-undergraduate-core-requirements/)
- College of Engineering, Design and Computing Graduation Requirements (http://catalog.ucdenver.edu/cu-denver/undergraduate/schools-colleges-departments/college-engineering-design-computing/#graduationrequirementstext)
- Click here (http://catalog.ucdenver.edu/cu-denver/undergraduate/academic-policies-procedures/) for information about Academic Policies

Program Requirements

1. Students must maintain a minimum 2.0 GPA in all courses applying to major requirements.
2. Students must maintain a minimum 2.0 GPA in all CSCI and CSCY courses attempted.

Undergraduate students in the Department of Computer Science and Engineering are required to have a personal laptop, with the specifications on the CEDC Student Laptop website (https://engineering.ucdenver.edu/laptops/#ac-computer-science-bachelor-of-arts-cs-2).

The BS in cybersecurity requires 120 credits including:

- 24 credits CU Denver core curriculum
- 7 credits mathematics
- 8 credits natural and physical science
- 3 credits engineering design
- 31 credits computer science
- 47 credits cybersecurity

Code	Title	Hours
CU Denver Core Curriculum		**24**
Computer Science Core for Cybersecurity		
CSCI 1410	Fundamentals of Computing [1]	3
CSCI 1411	Fundamentals of Computing Laboratory [1]	1
CSCI 1510	Logic Design [1]	3
CSCI 2312	Object Oriented Programming [1]	3
CSCI 2421	Data Structures and Program Design [1]	3
CSCI 2511	Discrete Structures [1]	3
CSCI 2525	Assembly Language and Computer Organization [1]	3
CSCI 3287	Database System Concepts	3
CSCI 3412	Algorithms [1]	3
CSCI 3453	Operating System Concepts [1]	3
CSCI 3761	Introduction to Computer Networks [1]	3
Cybersecurity Core		
CSCY 2930	Practical System Administration	2
CSCY 3740	Computer Security [1]	3
CSCY 3765	Secure Network and Systems Programming	3
CSCY 4407	Security and Cryptography	3
CSCY 4738	Senior Design I [1]	3
CSCY 4739	Senior Design II	3
CSCY 4741	Principles of Cybersecurity [1]	3
CSCY 4742	Cybersecurity Programming and Analysis [1]	3
CSCY 4743	Cyber and Infrastructure Defense [1]	3
CSCY 4772	Mobile and IoT Security	3
CSCY 4950	Cybersecurity Risk Analysis and Management	3
15 credits of any 3000-level or above Cybersecurity (CSCY) courses not applied to the above 32 credits. Students may apply up to two of the following courses in place of CSCY courses: MATH 3195, CSCI 3415, CSCI 4034, CSCI 4591 & CSCI 4773		15
Mathematics		
MATH 1401	Calculus I [1]	4
MATH 2830	Introductory Statistics	3
Science		**8**

Students must complete a minimum of 8 credits (two courses with associated labs) of natural and physical sciences with labs for science majors. Students may choose to complete ENGR 1300 Chemistry for Engineers as one choice.

BIOL 2010 & BIOL 2011	Organisms to Ecosystems (Gen Bio) and Organisms to Ecosystems Lab (Gen Bio)	
BIOL 2020 & BIOL 2021	Molecules to Cells (Gen Bio) and Molecules to Cells Lab (Gen Bio)	
CHEM 2031 & CHEM 2038	General Chemistry I and General Chemistry Laboratory I	
CHEM 2061 & CHEM 2068	General Chemistry II and General Chemistry Laboratory II	
PHYS 2010 & PHYS 2321	College Physics I and Intro Experimental Phys Lab I	
PHYS 2020 & PHYS 2341	College Physics II and Intro Experimental Phys Lab II	
PHYS 2311 & PHYS 2321 or PHYS 235	General Physics I: Calculus-Based and Intro Experimental Phys Lab I Applied Physics Lab I	
PHYS 2331 & PHYS 2341 or PHYS 236	General Physics II: Calculus-Based and Intro Experimental Phys Lab II Applied Physics Lab II	
ENGR 1130	Chemistry for Engineers	
Engineering Design		
ENGR 1200	Fundamentals of Engineering Design Innovation	3
Total Hours		**120**

[1] Must be completed with a C- or higher.

Measurable Outcomes

The bachelor of science in cybersecurity program must enable its students to attain, by the time of graduation:

- Analyze a complex computing and security problem and apply algorithmic reasoning to identify solutions.
- Design, implement, and evaluate a computing-based solution to meet a given set of computing and security requirements.
- Communicate and function effectively in professional contexts and teams.
- Make informed judgments in computing and security practices based on legal and ethical principles.
- Apply security principles and practices to maintain operations in the presence of threats.

To review the Degree Map for this program, please visit our website (https://www.ucdenver.edu/student/advising/undergraduate/degree-maps/cedc/).