

BS IN CYBER SECURITY

Overview

Our Bachelor of Science in Cyber Security is a four-year undergraduate program that targets requirements for entry-level cyber security jobs including information security analyst, cybersecurity developer, security administrator, security engineer, penetration tester and others.

The curriculum includes core cyber security courses to prepare students with strong cyber security foundations and equip them with practical cyber security skills. Students in this program will have access to the cutting-edge cyber security lab, cyber forensics and machine learning lab, and Engineering Computing Labs. Our faculty are active in cyber security research and bring their expertise into the classroom. Many courses in the curriculum have hands-on lab and/or research project components so that students can develop practical skills to solve real-world cybersecurity problems. In the capstone class, students will form a group and design/develop cybersecurity applications that can be used in real-life scenarios. Outside the classroom, students can gain professional skills through doing internship in a company or participating in a research project led by the faculty member or joining the UToledo Cyber Security Club to practice the cybersecurity skills to benefit the UToledo community.

Program students will also have the opportunity to enroll in the early admission B.S./M.S. program to get a full year head start in earning their Master of Science in Cyber Security degree at the University of Toledo.

Code	Title	Hours
CSET 1100	Introduction to Computer Science and Engineering Technology	4
PHIL 1010	Introduction To Logic	3
ENGT 1000	Engineering Technology Orientation	1
ENGL 1110	College Composition I	3
Social Science Elective. Select one approved 3 semester hour course from Anthropology (ANTH), Economics (ECON), Geography (GEPL), Political Science (PSC), Psychology (PSY), Social Work (SOCW) or Sociology (SOC).		3
CSET 1200	Object Oriented Programming and Data Structures	3
PHYS 2070	General Physics I	4
PHYS 2075	General Physics I - Lab	1
Select one of the following Communications Elective		3
COMM 2600	Public Presentations	
COMM 2820	Group Communication	
COMM 2840	Interpersonal Communication	
ENGL 2950	Technical Writing	3
MATH 2450	Calculus For Engineering Technology I	4
PHYS 2080	General Physics II	4
PHYS 2085	General Physics II - Lab	1
Multicultural Elective. Select one 3 semester hour course that satisfies the Diversity of U.S. Culture requirement.		3
CSET 2200	PC and Industrial Networks	4
MATH 2460	Calculus For Engineering Technology II	4
CYBR 1400	Ethical Behavior in Computing	4

CSET 2520	Discrete Structures	3
CYBR 2410	Digital Forensics	3
Social Science Elective. Select one approved 3 semester hour course from Anthropology (ANTH), Economics (ECON), Geography (GEPL), Political Science (PSC), Psychology (PSY), Social Work (SOCW) or Sociology (SOC).		3
MATH 2890	Numerical Methods And Linear Algebra	3
ENGT 2000	Professional Development	1
ENGT 3010	Applied Statistics And Design Of Experiments	4
CYBR 3350	Managing Security Projects	3
CYBR 3200	Client-Server Security Models	3
Natural Science Elective. Select one course from: Anatomy/Physiology (EXSC), Astronomy (ASTR), Biology (BIOL), Chemistry (CHEM), Earth, Ecology and Environmental Science (EEES), or Physics (PHYS).		4
CSET 3150	Introduction to Algorithms	4
CSET 3300	Database-Driven Web Sites	4
EECS 4720	Fundamentals of Cyber Security	3
INFS 3400	Information Security, Data Governance, & Ethics in AI	3
CSET 4250	Applied Programming Languages	3
CSET 3600	Software Engineering and Human Interfacing	4
CSET 4350	Operating Systems	3
CSET 4750	Computer Networks And Data Communication	4
EECS 4770	Computer Hacking and Forensic Analysis	3
EECS 4740	Artificial Intelligence	3
Humanities/Multicultural Elective. Select one 3 semester hour Humanities/Fine Arts elective that also satisfies one of the two multi-cultural elective requirements ("double-dip"). Do not select a Philosophy (PHIL) course.		3
ENGT 4050	Senior Technology Capstone	3
CSET 4850	Computer and Network Security	4
Total Hours		123

Combined bachelor's to master's- Cyber Security

Undergraduate students accepted to the BS to MS in Cyber Security option will be admitted to the MS in Cyber Security and allowed to complete up to three graduate level classes (nine credit hours) during their final academic year of undergraduate studies. Students admitted into the pipeline program must apply for admission to the College of Graduate Studies for the semester that they intend to matriculate. They will then continue in to the graduate program upon completion of the undergraduate degree requirements. The graduate coursework (up to nine hours) may be applied to completion of both undergraduate and graduate degree requirements. It will be the joint responsibility of the faculty and administrators in the undergraduate and graduate programs to supervise students admitted to the combined program option, to ensure that the limit of nine hours taken as an undergraduate is strictly enforced, and to request that the College of Graduate Studies change their matriculation from Undergraduate to Graduate when they meet all undergraduate degree requirements.

The following provisions apply for classes taken for graduate credit: 1) graduate classes taken at The University of Toledo only after the

student is accepted in the program, 2) EECS 5720, EECS 5770, and EECS 5740 may be included in the approved nine semester hours of graduate credit taken as an undergraduate. Students interested in the combined program must submit a graduate admission application to the College of Graduate Studies.

First Year

First Term		Hours
CSET 1100	Introduction to Computer Science and Engineering Technology	4
PHIL 1010	Introduction To Logic	3
ENGT 1000	Engineering Technology Orientation	1
ENGL 1110	College Composition I	3
Social Science Elective		3
Hours		14

Second Term

CSET 1200	Object Oriented Programming and Data Structures	3
PHYS 2070	General Physics I	4
PHYS 2075	General Physics I - Lab	1
Communication Elective		3
ENGL 2950	Technical Writing	3
Hours		14

Second Year

First Term

MATH 2450	Calculus For Engineering Technology I	4
PHYS 2080	General Physics II	4
PHYS 2085	General Physics II - Lab	1
CSET 2200	PC and Industrial Networks	4
Multicultural Elective		3
Hours		16

Second Term

MATH 2460	Calculus For Engineering Technology II	4
CYBR 1400	Ethical Behavior in Computing	4
CSET 2520	Discrete Structures	3
CYBR 2410	Digital Forensics	3
Social Science Elective		3
Hours		17

Third Year

First Term

MATH 2890	Numerical Methods And Linear Algebra	3
ENGT 2000	Professional Development	1
ENGT 3010	Applied Statistics And Design Of Experiments	4
CYBR 3350	Managing Security Projects	3
CYBR 3200	Client-Server Security Models	3
Hours		14

Second Term

Natural Sciences Elective		4
CSET 3150	Introduction to Algorithms	4
CSET 3300	Database-Driven Web Sites	4

EECS 4720	Fundamentals of Cyber Security	3
Hours		15

Fourth Year

First Term

INFS 3400	Information Security, Data Governance, & Ethics in AI	3
CSET 4250	Applied Programming Languages	3
CSET 3600	Software Engineering and Human Interfacing	4
CSET 4350	Operating Systems	3
CSET 4750	Computer Networks And Data Communication	4
Hours		17

Second Term

Humanities/Multicultural Elective		3
EECS 4770	Computer Hacking and Forensic Analysis	3
EECS 4740	Artificial Intelligence	3
ENGT 4050	Senior Technology Capstone	3
CSET 4850	Computer and Network Security	4
Hours		16
Total Hours		123

- 1. An ability to analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.
- 2. An ability to design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- 3. An ability to communicate effectively in a variety of professional contexts.
- 4. An ability to recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
- 5. An ability to function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
- 6. An ability to apply security principles and practices to maintain operations in the presence of risks and threats.