CYBERSECURITY (MS)

As cybersecurity becomes an increasingly valuable discipline to protect organizations' devices, networks, software, and data from cyber threats and attacks, the demand for skilled well-trained cybersecurity professionals will continue to grow. This program equips students with the skills and experience needed to begin or advance a successful career in cybersecurity. The Cybersecurity MS program offers a balance of technical and experiential learning through interdisciplinary coursework, innovative instruction, and opportunities to engage in research, competitions, and internships. Guided by Loyola's faculty, composed of active researchers and experienced practitioners, students develop advanced knowledge and earn first-hand experience in cybersecurity fundamentals, threat analysis, secure system design, incident detection and response, ethical hacking and penetration testing, artificial intelligence and machine learning, and more.

Related Programs

Master's

- Computer Science (MS) (https://catalog.luc.edu/graduate-professional/graduate-school/arts-sciences/computer-science/computer-science-ms/)
- Information Technology (MS) (https://catalog.luc.edu/graduate-professional/graduate-school/arts-sciences/computer-science/information-technology-ms/)

Curriculum

Code	Title	Hours
Required Courses		
COMP 401	Computer Security	3
COMP 417	Social and Ethical Issues in Computing	3
COMP 447	Intrusion Detection and Computer Forensics	3
COMP 448	Network Security	3
COMP 452	Introduction to Computer Vulnerabilities	3
Elective Courses		
Select five of the following courses:		15
COMP 410	Operating Systems	
COMP 431	Cryptography	
COMP 440	Computer Forensics Investigations	
COMP 443	Computer Networks	
COMP 445	Internet of Things Device and Application Security	
COMP 449	Wireless Networking and Security	
COMP 451	Enterprise Networking	
COMP 471	Theory of Programming Languages	
COMP 479	Machine Learning	
COMP 487	Deep Learning	
COMP 488	Computer Science Topics	
COMP 490	Independent Project [1]	
COMP 499	Internship [2]	
Total Hours		**30**

[1] This consists of participating in cybersecurity competitions and/or cybersecurity research.

[2] Up to 6 credit hours allowed.

Suggested Sequence of Courses

Course	Title	Hours
Year One		
Semester I		
COMP 401	Computer Security	3
COMP 417	Social and Ethical Issues in Computing	3
COMP 400-Level Elective		3
	Hours	**9**
Semester II		
COMP 447	Intrusion Detection and Computer Forensics	3
COMP 452	Introduction to Computer Vulnerabilities	3
COMP 400-Level Elective		3
	Hours	**9**
Year Two		
Semester I		
COMP 448	Network Security	3
COMP 400-Level Elective		3
COMP 400-Level Elective		3
	Hours	**9**
Semester III		
COMP 400-Level Elective		3
	Hours	**3**
	Total Hours	**30**

Graduate & Professional Standards and Regulations

Students in graduate and professional programs can find their Academic Policies in Graduate and Professional Academic Standards and Regulations (https://catalog.luc.edu/academic-standards-regulations/graduate-professional/) under their school. Any additional University Policies supersede school policies.

Learning Outcomes

- Security Fundamentals: Strong understanding of the fundamental principles and concepts of cybersecurity, including confidentiality, integrity, availability, authentication, and authorization.
- Threat Analysis: Ability to identify and assess security threats and vulnerabilities and develop strategies to mitigate cybersecurity attacks.
- Secure System Design: capacity to design and implement secure systems and networks, considering security at all stages of the development lifecycle.
- Incident Detection and Response: Skills to detect, respond to, and recover from cybersecurity incidents, including malware infections, data breaches, and denial-of-service attacks.
- Ethical Hacking and Penetration Testing: Competency in the areas of ethical hacking and penetration testing. This includes adherence to ethical principles and professional standards for cybersecurity, the ability to assess the security of systems and networks and recommend remediation strategies.