CYBERSECURITY (BS)

This major grows out of the enormous importance of network computing and the major challenges to security that these networks pose. Students examine the architecture, properties, management, and performance of both wired and wireless networks, including how to keep them reliable and secure. Students gain the talents and skills necessary for success in today's organizations according to current industry practices: planning, designing, implementing and administering voice and data communication networks; assessing and implementing the communication and security requirements of an organization in the form of a secure communication infrastructure; functioning as an effective member of a network and security services division in an organization.

The Bureau of Labor Statistics indicates high median pay and estimates a 34.7% increase in the demand for information security analysts for the period 2021 to 2031 (the highest growth rate among all computer and information technology occupations, which group is the second fastest growing of all BLS occupation groups).

Related Programs

Major

- Computer Science (BS) (https://catalog.luc.edu/undergraduate/arts-sciences/computer-science/computer-science-bs/)

Minor

- Computer Crime and Forensics Minor (https://catalog.luc.edu/undergraduate/arts-sciences/computer-science/computer-crime-forensics-minor/)
- Computer Science Minor (https://catalog.luc.edu/undergraduate/arts-sciences/computer-science/computer-science-minor/)

Curriculum

Code	Title	Hours
Major Requirements		
COMP 141	Introduction to Computing Tools and Techniques	3
COMP 163	Discrete Structures	3
or MATH 201	Introduction to Discrete Mathematics & Number Theory	
COMP 170	Introduction to Object-Oriented Programming	3
COMP 264	Introduction to Computer Systems	3
COMP 271	Data Structures I	3
COMP 301	Introduction to Computer Security	3
COMP 310	Operating Systems	3
COMP 317	Social, Legal, and Ethical Issues in Computing	3
COMP 340	Computer Forensics	3
COMP 343	Computer Networks	3
COMP 347	Intrusion Detection and Security	3
COMP 348	Network Security	3
COMP 349	Wireless Networking and Security	3
COMP 352	Computer Vulnerabilities	3
MATH 131	Applied Calculus I [1]	3
or MATH 161	Calculus I	or 4
Practicum Capstone [2]		
Select six credit hours from the following:		6
COMP 312	Open Source Software Practicum	
COMP 344	Hands-on Approach to Security & Privacy	
COMP 390	Broadening Participation in STEM (Computing, Math & Science)	
COMP 391	Internship in Computer Science	
COMP 398	Independent Study	
Computer Science Restricted Electives		
Select seven credit hours from the following:		7
CJC 354	Cybercrime	
COMP 272	Data Structures II	
COMP 300-Level Course(s)		
Computer Science Free Elective		
Select one of the following:		3
COMP 125	Visual Information Processing	
COMP 150	Introduction to Computing	
COMP 300-Level 3-credit Course		
Total Hours		**61-62**

[1] By arrangement with the Undergraduate Program Director, the extra credit from MATH 161 Calculus I may be applied towards the "Computer Science Free Electives" category.

[2] See the details of registering for these courses in the Computer Science Department website resources. Students are encouraged to complete these credits during junior and senior years to draw on prior experience. Note:

- COMP 312 and COMP 344 each are a 3-credit course
- COMP 390 is limited to 3 total credits
- COMP 391 and COMP 398 will usually be limited to 6 total credits each, but permission may sometimes be granted for more.

Suggested Sequence of Courses

The below sequence of courses is meant to be used as a suggested path for completing coursework. An individual student's completion of requirements depends on course offerings in a given term as well as the start term for a major or graduate study. Students should consult their advisor for assistance with course selection.

CSEC-BS Sample Schedule

Course	Title	Hours
Year 1		
Fall		
COMP 150	Introduction to Computing [1]	3
COMP 141	Introduction to Computing Tools and Techniques	3
MATH 131	Applied Calculus I [2]	3
CORE: Philosophical Knowledge Tier 1		3
CORE: College Writing Seminar		3
UNIV 101	First Year Seminar	1
	Hours	**16**
Spring		
COMP 170	Introduction to Object-Oriented Programming [3]	3
COMP 163	Discrete Structures	3

CORE: Historical Knowledge Tier 1		3
CORE: Ethics		3
CORE: Scientific Knowledge Tier 1		3
	Hours	**15**
Year 2		
Fall		
COMP 271	Data Structures I	3
COMP 264	Introduction to Computer Systems	3
COMP 301	Introduction to Computer Security	3
CORE: Theology and Religious Studies Tier 1		3
CAS Language Requirement 101 level [4]		3
	Hours	**15**
Spring		
COMP 272	Data Structures II	3
COMP 317	Social, Legal, and Ethical Issues in Computing	3
COMP 348	Network Security	3
CORE: Societal & Cultural Knowledge Tier 1		3
CAS Language Requirement 102 level		3
	Hours	**15**
Year 3		
Fall		
COMP 343	Computer Networks	3
COMP 310	Operating Systems	3
COMP 347	Intrusion Detection and Security	3
COMP Free Elective		1
CORE: Literary Knowledge & Experience Tier 1		3
CORE: Artistic Knowledge & Experience		3
	Hours	**16**
Spring		
COMP 340	Computer Forensics	3
COMP 349	Wireless Networking and Security	3
CORE: Theology and Religious Studies Tier 2		3
CORE: Scientific Knowledge Tier 2		3
CORE: Historical Knowledge Tier 2		3
	Hours	**15**
Year 4		
Fall		
COMP 352	Computer Vulnerabilities	3
COMP Practicum (3)		3
CORE: Literary Knowledge & Experience Tier 2		3
CORE: Societal & Cultural Knowledge Tier 2		3
CORE: Philosophical Knowledge Tier 2		3
	Hours	**15**
Spring		
COMP Free Elective		3
COMP Practicum		3
COMP Free Elective if COMP 150 not taken		3
CAS Elective		3
CAS Elective		3
	Hours	**15**
	Total Hours	**122**

1. COMP 150 Introduction to Computing will apply to COMP Free Electives; students with prior experience in computer programming, for example a high school course modeled on the Exploring Computer Science or Computer Science Principles curriculum may replace this course with a different COMP Free Elective at any time during the program. A score of 4 or 5 on the AP CS Principles Exam will earn actual credit for this course.
2. May substitute MATH 161 Calculus I and may use the extra credit towards COMP Free Electives.
3. A score of 4 or 5 on the AP CS A Exam will earn credit for this course.
4. Language must be completed through the 102 course level or through an exam.

General Notes

- Credits never can be double-counted for different categories of the requirements for the major. But a course may satisfy a major requirement and also satisfy a University and/or College requirement (e.g., Core, residency, Engaged Learning, Writing Intensive).
- It is usually not meant to combine a computing major or minor with another, the principal exception being CCFR-MINR; see more detail in the double-dipping rules (https://catalog.luc.edu/undergraduate/arts-sciences/computer-science/#policiestext).
- With permission, the extra credit from MATH 161 Calculus I or 300 level MATH, PHYS, or STAT **for double majors** can be applied to the "Computer Science Restricted Electives" or "Computer Science Free Elective" categories.)

College of Arts and Sciences Graduation Requirements

All Undergraduate students in the College of Arts and Sciences are required to take two Writing Intensive courses (6 credit hours) as well as complete a foreign language requirement at 102-level or higher (3 credit hours) or a language competency test. More information can be found here (https://www.luc.edu/cas/college-requirements/).

Additional Undergraduate Graduation Requirements

All Undergraduate students are required to complete the University Core, at least one Engaged Learning course, and UNIV 101. SCPS students are not required to take UNIV 101. Nursing students in the Accelerated BSN program are not required to take core or UNIV 101. You can find more information in the University Requirements (https://catalog.luc.edu/undergraduate/university-requirements/) area.

Learning Outcomes

- Understanding of Cybersecurity Fundamentals: This includes knowledge of how to protect and defend computer systems and networks by ensuring their availability, integrity, authentication, and confidentiality.
- Proficiency in Identifying and Mitigating Threats: Graduates should be able to identify potential threats and vulnerabilities in a system, and know how to put measures in place to mitigate them.

- Knowledge of Cybersecurity Tools and Technologies: Students should be proficient in using current tools and technologies to prevent and detect cyber threats.
- Skills in Risk Management: This includes understanding how to assess the risk to a system, how to quantify that risk, and how to implement measures to manage it.
- Understanding of Legal and Ethical Issues: Graduates should understand the legal, ethical, and professional issues involved in cybersecurity, such as privacy concerns, intellectual property rights, and cybercrime laws.
- Incident Response Skills: Students should be able to develop and implement an effective incident response strategy to reduce the impact of security breaches and network intrusions.
- Knowledge of Cryptography: Students should understand the principles of cryptography and how it is used to secure data.