Cybersecurity

Cybersecurity combines essential computer science with conceptual and practical specialization in security to prepare students for hands-on, deeply technical work in the field. The ability to frame problems, select computational models, design program structures, and develop efficient algorithms is as important in computer science as software implementation skill. All cybersecurity students take the standard computer science course sequence, covering content such as basic programming, object-oriented design, computer architecture and operating systems, computer networks and distributed systems, and algorithmic complexity and computability theory. These courses lay the foundation for cybersecurity-specific coursework.

Cybersecurity coursework covers key areas in the field, from a broad overview of the topical space (including threat modeling, symmetric and asymmetric key cryptography, authentication, access control, social engineering, simple exploits, basic systems security, malware, the cybercrime underground, and advanced persistent threat actors) to deep dives into the design of secure operation systems and applications. Fundamental topics include analyzing prevalent classes of attacks against systems; security vulnerabilities and defense techniques; limitation of damage and strategic recovery; design and implementation of distributed authentication protocols; and existing standardized security protocols and legal infrastructure relating to privacy, data ethics, data security, hacking, automation, and intellectual property. In addition, cybersecurity students have access to a wide array of electives including courses on wireless networking, software vulnerabilities, cybersecurity risk management and assessment, digital forensics, and criminology.

Programs

Bachelor of Science (BS)

- Cybersecurity (https://catalog.northeastern.edu/undergraduate/computer-information-science/cybersecurity/cybersecurity-bs/) (Boston)