Be the best line of defense against hackers

An organization’s most valuable asset is its data — which makes the people who protect that data indispensable. With our Bachelor of Science in Cybersecurity, you’ll prepare to play a vital role in stopping cyber threats within any organization. And you’ll take just one 5-week course at a time, so you can balance work and life on the path to your degree.

In the BSCYB program, you’ll learn to:

- Apply mathematics, science and engineering principles in the cyber domain.
- Determine the computing requirements needed to solve technical problems.
- Create processes to protect all assets of a computer infrastructure.
- Use techniques, skills and tools to evaluate modern cybersecurity issues.
- Build security risk assessments for enterprise management.

Study the areas that interest you most with elective tracks in Ethical Hacking, Security Compliance, Risk Management, Penetration Testing and Computer Forensics. You can also specialize your BSCYB degree with a Cybersecurity Policy and Governance Certificate.

What sets us apart?

When you choose our online Bachelor of Science in Cybersecurity, you can:

**Gain real-world industry skills**
Industry certification shows employers you’ve taken extra steps to gain the skills required for the job. Courses in this program do not lead to certification, but can educationally prepare you to sit for the following exams:

**Waive required courses**
Through our Prior Learning Assessment (PLA) process, you can apply to have coursework waived for any relevant industry or professional certifications you’ve earned from organizations such as CompTIA, Microsoft or EC-Council.

**Save on certification exams**
When you complete the industry-aligned coursework, you can request a voucher for a discount on the associated certification exam.
Projected job growth: 32%

According to the Bureau of Labor Statistics, the job growth for information security analysts is projected to be 32 percent between 2018 and 2028. A Bachelor of Science in Cybersecurity degree can help prepare you to be an:

- IT Security Analyst
- Data Security Administrator
- Information Security Specialist
- IT Specialist
- Systems Analyst
- Information Systems Supervisor

Information not specific to University of Phoenix.

Networking opportunities

Access powerful networking tools through our PhoenixLink™ career services platform. Take advantage of personal career coaching. Search and apply for jobs, or make your résumé visible to employers. Connect with employers and alumni through career fairs and mixers. It’s all about connections. And we help you make them.

Learning outcomes

Along with the knowledge and skills related to the University Learning Goals, students who graduate with this degree should gain program-specific knowledge, skills and abilities. Each college creates a set of Program Student Learning Outcomes (PSLOs) to describe the knowledge, skills or attitudes students will possess upon completion of the program of study. By the time you complete your Bachelor of Science in Cybersecurity, you should be able to perform these learning outcomes.

University of Phoenix is accredited by the Higher Learning Commission (HLC), hlccommission.org. Since 1978, University of Phoenix has been continually accredited by the Higher Learning Commission and its predecessor.
Bachelor of Science in Cybersecurity

Course length: 5 weeks  
Total credits required: 120  
Max. number of transfer credits: 90

Requirements and prerequisites

You'll need 120 credits to complete this program. These may be earned from a combination of required and elective courses. Your course schedule may vary based on any relevant industry or professional certifications or transferable credits.

Earn your degree faster

Transfer the credits you already have, or waive coursework through our Prior Learning Assessment (PLA) process. You could get credit for any relevant industry or professional certifications you've earned from organizations such as CompTIA, Microsoft or EC-Council.

Core courses

- CYB100: Cyber Domain
- CYB425: Security Analyst Procedures And Methodology
- CYB415: Project Cybersecurity Policy And Governance
- CYB433: Project Pen Testing Plan
- CYB233: Ethical Hacking Part 3
- CYB135: Object-oriented Security Scripting
- CYB405: Information Systems Governance
- CYB120: Computer Network Defense Part 1
- CYB140: Computer Network Defense Part 2
- CYB225: Linux Fundamentals
- CYB455: Project Digital Forensics
- CYB492: Capstone Bachelor Implementation
- CYB207: Risk Frameworks
- CYB360: Wireless Security
- CYB445: Risk Assessment
- CYB209: Compliance Management, Certification And Accreditation
- CYB110: Foundations Of Security
- CYB205: Infrastructure Administration
- CYB211: Applied Security Part 1
- CYB409: Information Systems Leadership, Projects And Operations
- CYB350: Security Team Participation
- CYB490: Capstone Bachelor Design
- CYB229: Ethical Hacking Part 1
- CYB429: Sec. Analyst Database, Wireless And Cloud Perimeter Testing
- CYB453: Network, Wireless, Web, Email And Mobile Forensics
- CYB451: Computer Forensics Lab
- CYB407: Information Systems Risk Controls And Auditing Management
- CYB411: Information Systems Core Competencies
- CYB427: Security Analyst Network Threat Testing
- CYB435: Project Pen Testing Execution And Report
- CYB130: Object-oriented Scripting Language
- CYB150: Computer Network Defense Part 3
- CYB235: Project Ethical Hacking
Bachelor of Science in Cybersecurity

- CYB227: Sniffing And Network Analysis
- CYB449: Computer Forensics Investigative Process
- CYB413: Strategic Planning And Finance
- CYB431: Security Metrics And Testing Security Analysis
- CYB215: Project Cyber Operations