BISK Amplified™ | UNIVERSITY OF LOUISVILLE®

CYBERSECURITY WORKFORCE PROGRAM

Online Program Guide

About Us

OUR MISSION

To Amplify Potential Through Transformational Learning Experiences

Bisk Amplified leads the way in online education and development solutions. We partner with your organization to provide your team members next generation education benefits from our top universities. As your dedicated partner, we enhance your organization's education benefits, boosting team skills and achieving talent goals.

OUR VALUES

Be Bold **Be Humble** **Be Remarkable**

OUR HISTORY

Bisk was founded in 1971 by Nathan Bisk to offer seminars to help people prepare for the CPA exam. As an entrepreneur and visionary, he saw the need to evolve the traditional classroom, so he pioneered distance learning via audio cassettes, to video cassettes, to computer software, to online learning. Bisk has helped top-tier universities launch online programs for more than 20 years, supporting more than two million enrollments around the world.

FOR BUSINESSES AND ORGANIZATIONS

Transformative Corporate Learning

Take your talent to the next level with online degrees and certificates from top-tier universities. We build the bridge between companies looking to upskill and retain their workforce, employees wanting to earn credentials, and universities offering exceptional online learning programs.

Since inception, we've supported more than

150	250	2 Million+
Degree Programs	Certificate Programs	Enrollments Throughout the World

UNIVERSITY OF LOUISVILLE®

Why Choose Louisville

Founded in 1798, the University of Louisville (UofL) fosters student success, groundbreaking research, and strong local and global connections. A Carnegie-recognized Research 1 and Community Engaged university, UofL drives innovation and creates opportunities that transform lives. UofL's online programs are nationally recognized by U.S. News & World Report for their

UofL is uniquely positioned to address the growing need for cybersecurity professionals through its "Pathways Coalition," a national initiative to develop a skilled cybersecurity workforce. As the lead institution, UofL partners with top universities and community colleges nationwide, all recognized as National Centers of Academic Excellence (NCAE) in Cyber Defense by the NSA. With over a decade of experience in cybersecurity education, UofL is driving the creation of a cutting-edge curriculum to protect critical systems and advance the field.

DIGITAL TRANSFORMATION CENTER

The University of Louisville Digital Transformation Center transforms the access, awareness, design and use of technology to embrace digital agility and enhance learning and discovery in the commonwealth.

Their mission is to empower the future of learning, research, and technology through collaboration, community of practice and partnerships.

Program Overview

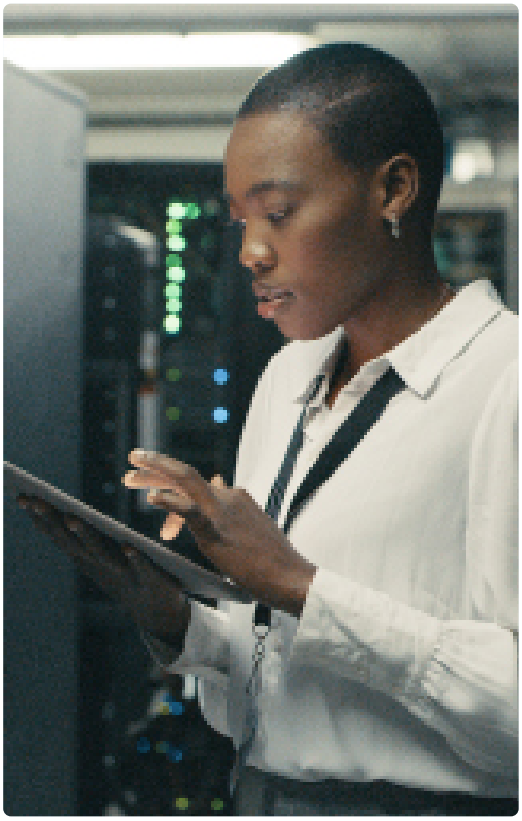
Build Your Future in Cybersecurity

Cyber threats are evolving, and so should your career. The University of Louisville's 100% online Cybersecurity Workforce Program empowers you to develop the skills needed to thrive in one of the fastest-growing industries – your way.

Whether you're just starting out or advancing your expertise, this program offers flexible, industry-aligned training designed for real-world impact. Specialize in healthcare or logistics through tailored concentration paths, and position yourself for success.

Flexible, Asynchronous Learning

- Upskill on your terms with courses designed to fit your schedule.
- Complete individual bundles in just 90 days or the full program in 6 months.
- No final exams—your knowledge is assessed through tests, microcredentials, and a final case study tailored to your chosen concentration.
- Access faculty support through office hours or scheduled sessions whenever guidance is needed.



How Does It Work?

1. **Choose Your Path:** Select the program level or specialized bundle that matches your goals and schedule.
2. **Learn from Experts:** Access coursework designed and taught by industry professionals, blending theory with practical application.
3. **Apply Your Skills:** Complete real-world capstone projects and lab-based assignments to solidify your learning.

Choose Your Concentration: Healthcare or Logistics

Cybersecurity solutions aren't one-size-fits-all. That's why our program allows you to specialize:

Healthcare: Protect sensitive patient data and address unique cybersecurity challenges in the medical field.

Logistics: Secure the supply chain with solutions tailored to today's fast-paced, globalized economy.

Explore the Right Path for You

The Cybersecurity Workforce Program offers a range of courses to choose from. To learn every module available, select the full 6-month program. Looking for an accelerated option? University of Louisville offers 3 “levels” of courses with 7-8 modules, each lasting 4 months. Specialized bundles have as little as 3 modules and can be completed in as quickly as 90 days.

Explorer Level

Ideal for beginners or those new to cybersecurity. Learn the foundational concepts in a supportive, accessible environment.

Micro-Credential

4 Months

$1,200

Practitioner Level

Perfect for those with some experience looking to apply their knowledge and deepen their skills with real-world scenarios.

Micro-Credential

4 Months

$1,200

Professional Level

Tailored for seasoned professionals aiming to master advanced topics, tackle complex challenges, and lead cybersecurity

Micro-Credential

4 Months

$1,120

Full Program

For learners wanting to grasp the full scope of cybersecurity. Participants are equipped with the skills needed to protect digital environments.

Professional Development Certificate

6 Months

$2,530

Specialized Bundles

- Foundational Bundle
- Network Bundle
- Cloud Bundle
- Internet of Things Bundle
- Database Bundle
- Cryptography Bundle
- Artificial Intelligence Bundle
- Blockchain Bundle
- Security Bundle

Learning Outcomes: What You'll Gain

Participants of the Cybersecurity Workforce Program will leave with:

- **Practical, In-Demand Skills:** Build expertise in tools and strategies that address today's cybersecurity challenges.
- **Industry Credentials:** Earn non-credit workforce certificates and digital badges to boost your professional profile.
- **Career Advancement:** Unlock opportunities in roles like network security analyst, ethical hacker, IT manager, or cybersecurity consultant.
- **Specialized Knowledge:** Apply cybersecurity solutions specific to healthcare or logistics through hands-on case studie.

Position yourself as a trusted expert in one of the world's most critical and high-demand fields.

Why Employers Value UoL Graduates

Employers trust graduates of the University of Louisville's Cybersecurity Workforce Program because they:

- Bring **real-world, hands-on experience** to the table.
- Are equipped with **in-demand tools and strategies** aligned with industry needs.
- Complete a **comprehensive, well-rounded curriculum** that prepares them to excel in any cybersecurity role.

Frequently Asked Questions

How long does the program take?

Courses range from 90 days to 6 months, depending on the program or bundle you choose.

Do I need prior experience in IT?

No! The Explorer Level bundle is designed for those new to IT or cybersecurity.

Will I earn a certification?

You'll earn a non-credit workforce certificate and may also receive digital badges from select technology providers.

Curriculum

The Cybersecurity Workforce Program at the University of Louisville offers a comprehensive curriculum designed to cater to various learning preferences and career objectives. The program is structured into several tiers and specialized bundles, each comprising multiple modules. Below is a detailed breakdown:

Full Course (23 Modules)

Database Management

Provides an overview of fundamental concepts of databases and database management, including aspects of database design, management systems, data models, normalization, SQL, basic security, and alternatives to relational databases.

Security Principles & Foundation

Offers an introduction to cybersecurity terminology, best practices, principles, standards, and the planning and management of cybersecurity functions and assets.

Network Foundations

Discusses the foundations of computer networks, covering network architecture, the OSI model, TCP/IP protocol stack, physical layer concepts, data link layer protocols, network layer protocols, transport layer protocols, application layer concepts, and an overview of wireless networking technologies.

Artificial Intelligence

Provides an overview of fundamental AI techniques and approaches, including the history of AI, knowledge and reasoning, problem-solving, learning approaches, practical considerations, and responsible AI, with case studies from cybersecurity and healthcare applications.

IT Basics

Offers a basic understanding of the components in an information technology system and their roles in system operation.

Privacy-Legal Foundations & Ethics

Examines legal, privacy, and ethical issues of information security in the electronic and internet environment, particularly in healthcare.

Coding

Introduces problem-solving techniques and the computer program development process through coding in a high-level language, covering program structure, data types, variables, operations, expressions, input/output, control structures, functions, data structures, and software design techniques.

Cryptography

Provides an overview of the cryptography field and its applications, introducing statistical properties of digital data, basic cryptographic methods, and standards such as DES, AES, RSA, and ElGamal, with applications like data encryption, message authentication, and digital signatures.

Cyber Threat Hunting

Covers the basics of cyber threat hunting in a secure operations center, including understanding the adversary's mindset and methods to identify new and emerging cyber threats through log analysis, event correlation, open-source threat intelligence, use of AI, honeypots, and threat sharing, with practical exercises in a simulated threat environment.

Information Security

Provides basic competency in the principles of information security as they relate to computing systems, particularly at the operating system level, focusing on fundamental security design principles, the adversarial model, data security, virtualization, viruses and malware, and operating-system-specific information security concepts for both desktop and mobile systems.

Network Security

Discusses fundamental concepts and principles of network security, covering topics such as networking basics, network traffic signatures, cryptography, wireless networking, wireless security, firewalls, intrusion detection and prevention systems, virtual private networks, and web security.

Cognitive Computing

Provides lectures and labs on deep learning and machine learning using a combination of tools such as cognitive services APIs and deep learning frameworks, with applications in healthcare, including consumer/user engagement and discovery applications like drug discovery and analysis of human health, and discussions on cybersecurity vulnerabilities in the Internet of Medical Things.

Data Mining

Offers an overview of basic concepts in data mining and main methodologies and approaches used for knowledge discovery from data, covering the definition of the data mining field, data mining process, data preprocessing, predictive and descriptive data mining, evaluation of data mining models, and privacy and security of data, with case studies from healthcare.

Cloud Foundations

Exposes students to current practices in cloud computing, including cloud service models (IaaS, PaaS, SaaS), technologies supporting cloud computing such as virtualization, motivating factors, benefits and challenges of the cloud, cloud storage, performance and systems issues, disaster recovery, federated clouds, data centers, and cloud security, with exposure to a leading public cloud computing platform.

Blockchain

Introduces blockchain with a modularized approach, focusing on the skills for each aspect of blockchain, with practical labs based on applications like bitcoins.

Forensics

Covers the fundamentals of digital forensics, including historical issues, key concepts, tools and techniques, and reporting methods, with practical exercises using various open-source tools.

Database Security

Provides an overview of fundamental concepts of database security, including access control and data protection.

Cloud Security

Introduces cybersecurity for the cloud, teaching students to apply classic security techniques to modern cloud security problems, analyzing recent cloud security vulnerabilities using standard, systematic techniques, and constructing security solutions for web service case studies.

Internet of Things (IoT)

Provides basic knowledge and understanding of fundamental concepts of IoT, including an overview from a design perspective, technical building blocks, machine learning and data analytics in IoT, communication and security challenges, and common industry use cases.

Post Quantum Cryptology

Covers foundational principles and techniques of quantum technology, including basic quantum mechanics, quantum information theory, quantum algorithms (e.g., Grover's search and Shor's factoring), quantum error-correcting codes, and quantum computing applications such as quantum encryption and quantum key distribution, with hands-on experience using IBM Q Experience quantum devices.

Risk Analysis

Provides an overview of fundamental techniques and approaches to identify, assess, and mitigate cybersecurity risk, including identification of cybersecurity risks, assessment and mitigation approaches, with case studies related to cybersecurity risk analysis in the healthcare industry.

Robotic Process Automation Analysis

Provides lectures and labs on the system architecture enabling robotics and common use cases for robotics in healthcare, covering characteristics of operating systems enabling robotics, common threats and cyber-attacks to robotic systems, ethical issues related to the use of robotics, and the need for cybersecurity to enable trust in robotic operations.

Capstone Project

The purpose of this capstone project is for the participants to apply knowledge and skills acquired during the Cybersecurity Healthcare certificate program to a project involving actual data in a realistic setting. During the project, participants will engage in the entire process of analyzing a real-world cybersecurity project or case study and apply suitable methods to address the problem. Both the problem statements for the capstone project assignments and any relevant datasets will represent real-world domains similar to those that participants might typically encounter within healthcare-related industry, government, or non-governmental organizations (NGOs).

Explorer Level

- Database Management
- Security Principles & Foundation
- Network Foundations
- Artificial Intelligence
- IT Basics
- Privacy-Legal Foundations & Ethics
- Coding
- Cryptography

Practitioner Level

- Cyber Threat Hunting
- Information Security
- Network Security
- Cognitive Computing
- Data Mining
- Cloud Foundations
- Blockchain
- Forensics

Professional Level

- Database Security
- Cloud Security
- Internet of Things (IoT)
- Post Quantum Cryptology
- Risk Analysis
- Robotic Process Automation Analysis
- Capstone Project

Specialized Bundles

Foundational Bundle
IT Basics
Privacy-Legal Foundations & Ethics
Security Principles & Foundations

Network Bundle
Network Foundations
Information Security
Network Security

Database Bundle
Database Management
Database Security
Cyber Threat Hunting

Cryptography Bundle
Cryptography
Post Quantum Cryptology
Forensics

Artificial Intelligence (AI) Bundle
Artificial Intelligence
Cognitive Computing
Robotic Process Automation Analysis

Internet of Things (IoT) Bundle
Internet of Things (IoT)
Network Foundations

Blockchain Bundle
Coding
Artificial Intelligence
Cognitive Computing

Risk Management Bundle
Risk Analysis
Cloud Security
Capstone Project in Healthcare

Cloud Bundle
Network Foundations
Information Security
Network Security
Cloud Foundations

BISK Amplified™ | UNIVERSITY OF LOUISVILLE®

Visit us at **mycourses.biskamplified.com/louisville**
or call us at: **(833) 999-1978.**

v02282025