UMBC
AN HONORS UNIVERSITY IN MARYLAND

CYBERSECURITY GRADUATE PROGRAMS

Rockville, MD

Whether you already have a degree in an information technology discipline or are seeking to expand your knowledge of cybersecurity for your own professional development, UMBC's graduate cybersecurity programs will leverage your experience toward a range of opportunities within the cybersecurity and cyber operations profession.

Graduates of UMBC's cybersecurity program will be well-suited for management and operational positions within government and private industry in such areas as:

- Network and Information Security
- Intelligence
- Cyber Operations
- Law Enforcement and Counterintelligence
- System and Operational Requirements Analysis
- IT and Cybersecurity Procurement
- Cybersecurity Exercise, Test and Evaluation

Our offerings include:

Master in Professional Studies: Cybersecurity

The MPS is designed to prepare computer science, information systems, and other technology professionals working in the IT and cybersecurity field to fill management and leadership roles in their organization. Multidisciplinary coursework blends practical management-oriented courses with more technically focused courses, allowing students to develop a formal graduate educational program that best meets their individual career development needs.

Post Baccalaureate Certificate in Professional Studies: Cybersecurity Strategy and Policy

This four-course graduate certificate is available to students with a variety of backgrounds working in technology field. Students may choose to take this certificate by itself, or they may take this certificate and then later complete the master's. If a student is accepted into the M.P.S.: Cybersecurity, all four certificate courses count toward that degree.

Costs

Maryland Resident
Tuition per credit: $530 (plus mandatory fees)*

Non-Resident
Tuition per credit: $878 (plus mandatory fees)*

For more information on tuition and fees, please visit: ***www.umbc.edu/sbs.***

**For Academic Year 2013/2014*

Admission Requirements

For M.P.S.:

- A Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, Math, or Information Systems is recommended, however degrees from other fields (such as Criminal Justice, Public Policy) may be acceptable given relevant work experience in the cybersecurity or cyber operations field.
- GRE scores are not required for admission
- Applicants should have a minimum undergraduate GPA of 3.0 on a 4.0 scale

For Graduate Certificate:

- There are no specific constraints on the type of Bachelor's degree required, however students with an academic or professional background in computer science or information systems are encouraged to apply.
- GRE scores are not required for admission
- Applicants should have a minimum undergraduate GPA of 3.0 on a 4.0 scale

International Students:

- A Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, Math, or Information Systems is recommended, however degrees from other fields (such as Criminal Justice, Public Policy) may be acceptable given relevant work experience in the cybersecurity or cyber operations field.
- Minimum undergraduate GPA of 3.0 on 4.0 scale
- Graduate Record Exam (GRE) scores with a minimum combined score of 306. Verbal Reasoning should be at least 153 and Analytical Writing at least 4.5. GRE scores are not required if your undergraduate degree was completed at an accredited U.S. university.
- TOEFL Scores: Minimum scores 597 (Written), 247 (computerized), 99 (iBT). Scores must be less than 2 years old. iBT Score Breakdown: Writing (23), Listening (23), Reading (25), Speaking (28, 23 acceptable if have 2 years' work experience in supervisory or management position in the U.S.) **OR**
- IELTS Score: Minimum score of 7.5 required

For More Details

umbc.edu/cybersg

Dr. Richard Forno, Graduate Program Director
richard.forno@umbc.edu

MRP20131002

Master in Professional Studies: Cybersecurity (30 Credits)

The ten-course master's degree combines courses in cybersecurity strategy, policy, and management with more technical courses that allows students to develop a formal graduate educational program that best meets their individual career development needs.

Degree Requirements

Required Core Courses (21 credits)

- CYBR 620: Introduction to Cybersecurity
- CYBR 623: Cybersecurity Law & Policy
- CYBR 624: Cybersecurity Project
- CYBR 650: Cybersecurity Management
- ENMG 652: Management, Leadership, and Communication
- ENMG 658: Financial Management **OR**
- ENMG 672: Decision & Risk Analysis
- One additional related elective course approved by Cybersecurity Graduate Program Director

Elective Courses (9 credits) Choose three, such as:

- CMPE 685: Principles of Communications Networks
- CYBR 621: Cyber Warfare
- CYBR 622: Global Cyber Capabilities and Trends
- Special Topics Courses (e.g., Applied Network Security, Standards & Compliance, Malware Analysis) that are offered on a rotating or periodic basis.
- Other relevant graduate courses approved by Cybersecurity Graduate Program Director

Some electives may require academic or professional pre-requisites; check with the specific department or program to determine eligibility and suitability.

Post Baccalaureate Certificate in Professional Studies: Cybersecurity Strategy and Policy

This four-course graduate certificate can be completed in a year. Because these courses are not technical, this program is available to students with a variety of undergraduate backgrounds looking for a solid introduction to cybersecurity concepts. Students may choose to take this certificate by itself and/or then decide to apply for the M.P.S. in Cybersecurity. Once completed, all four certificate courses will count toward that degree.

Four Required Courses (12 credits)

- CYBR 620: Introduction to Cybersecurity
- CYBR 621: Cyber Warfare
- CYBR 622: Global Cyber Capabilities and Trends
- CYBR 623: Cybersecurity Law & Policy

Why Cybersecurity

Cybersecurity has emerged as a critical domain of global competition that reaches across the social, economic, political and military realms of influence.

The infusion of the Internet and its related networked technologies into nearly every aspect of society, business, and government presents a target of opportunity for adversaries. As a result, nations and international organizations are developing new operational doctrines, advanced cyberwarfare capabilities, cybersecurity enhancements and the necessary domain-focused human capital needed to achieve or maintain their interests in cyberspace.

Why UMBC?

- UMBC is uniquely positioned to provide education and training that respond to the state's need for qualified technical professionals in the cybersecurity field:
- For four years running (2009-2012), UMBC was ranked #1 in the U.S. News and World Report's list of "national up-and-coming" universities.
- UMBC is certified as a Center of Academic Excellence in Information Assurance Education (CAE) as well as a Center of Academic Excellence in Research (CAE-R) sponsored by the National Security Agency and Department of Homeland Security (DHS). Students attending UMBC are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program (IASP) and/or Federal CyberCorps Scholarship for Service (SFS).

Program Location:

UMBC at the Universities at Shady Grove
Camille Kendall Academic Center
9636 Gudelsky Drive
Rockville, MD 20850