Curriculum

COURSE CODE	COURSE TITLE	COURSE CODE	COURSE TITLE	COURSE CODE	COURSE TITLE
Degree Requirements: 18 Credit Hours					
CSE 501	Cryptography and Network Security	CSE 502	Security Risk Assessment and Auditing	ITE 503	Research Methods and Communications
CSE 511	Advanced Ethical Hacking and Penetration Testing	CSE 512	Advanced Cyber Digital Forensics	CSE 530	Advanced Selected Topics in Cybersecurity
Thesis Requirements: 9 Credit Hours					
CSE 591A	Master's Thesis in Cybersecurity-Part 1	CSE 591B	Master's Thesis in Cybersecurity- Part 2		
Elective Courses: 3 Credit Hours					
CSE 513	Major Elective				

Major Electives Basket					
ITE 501	Cloud Computing	ITE 504	Big Data Analytics	ITE 510	Advanced Data Communication and Computer Networks
ITE 515	Artificial Intelligence				

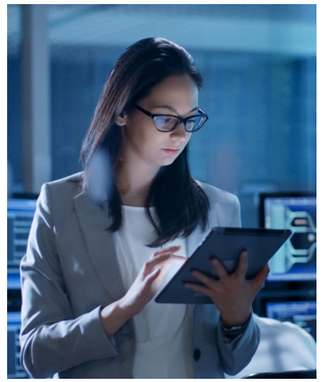
MASTER OF SCIENCE IN

CYBERSECURITY

جامعة أبوظبي
Abu Dhabi University
College of Engineering

ORACLE Academy

Networking Academy



Program Overview

The Master of Science in Cybersecurity (MSCS) program at Abu Dhabi University is designed to equip students with the knowledge, skills, and hands-on experience needed to tackle modern cybersecurity challenges. With the increasing reliance on digital infrastructure, organizations worldwide require cybersecurity professionals who can assess risks, defend against cyber threats, and ensure the integrity of digital systems.

This program offers a comprehensive curriculum that covers essential areas such as cryptography, ethical hacking, digital forensics, risk assessment, and advanced topics in cybersecurity. It is structured to accommodate both fresh graduates and working professionals, enabling them to enhance their technical expertise and leadership capabilities.

The MSCS program is aligned with industry standards and global cybersecurity frameworks, ensuring that graduates are well-prepared for roles in government agencies, financial institutions, healthcare, telecommunications, and other sectors where cybersecurity is critical. Additionally, students have opportunities to engage in cutting-edge research, collaborate with industry experts, and participate in cybersecurity competitions and conferences.

By joining this program, students will gain not only technical proficiency but also strategic insight into cybersecurity governance, compliance, and policy-making—essential skills for those aiming to take on leadership roles in the field.

Career Prospects

With cyber threats evolving rapidly, organizations across industries are in urgent need of skilled cybersecurity professionals. Graduates of the Master of Science in Cybersecurity program will be well-equipped to take on leadership and technical roles in both private and public sectors, including:

- **Cybersecurity Analyst** – Protects organizations by detecting, analyzing, and responding to cyber threats.
- **Ethical Hacker (Penetration Tester)** – Simulates cyberattacks to identify vulnerabilities before real attackers do.
- **Network Security Engineer** – Designs and implements secure network infrastructures to prevent breaches.
- **Digital Forensics Investigator** – Investigates cybercrimes, gathering digital evidence for law enforcement and legal proceedings.
- **Security Risk Auditor & Compliance Officer** – Ensures organizations comply with cybersecurity regulations and best practices.
- **Cloud Security Specialist** – Secures cloud-based environments and data from unauthorized access.
- **Chief Information Security Officer (CISO)** – Leads an organization's cybersecurity strategy and risk management.

The demand for cybersecurity professionals is growing rapidly, with reports indicating a global shortage of skilled experts. Graduates can expect lucrative career opportunities, with positions available in government agencies, financial institutions, healthcare, telecommunications, defense, and multinational corporations. The MSc in Cybersecurity provides the technical expertise and leadership skills needed for fast-track career progression and higher earning potential.