By 10Pie.com

Cybersecurity is a branch of computer science that primarily deals with the maintenance of security systems in computers and prevents data phishing and virus attacks from taking place.

It is a vast subject of study and requires the study of network security, cryptography, computer forensics, information security, programming, application security, etc. In this guide, you will learn the cybersecurity syllabus in various streams of study like B Tech, BSc, MCA, and PG diplomas.

Cybersecurity Syllabus For B. Tech

B.Tech is the degree that students get if they pursue any engineering discipline. For example, if the student wants to study cybersecurity, cryptography, and network security, the student may pursue a course on B. Tech in computer science engineering. The units and subjects covered under Cryptography and Network Security in B. Tech Computer Science include:

Unit 1: Attacks On Computers And Computer Security

An introduction to the different threats to computer systems, the need for computer security systems, the different security approaches, the different principles of security management, and the different types of virus attacks over the internet.

Unit 2: Cryptography

It introduces cryptography, plaintext and ciphertext, substitution and transportation techniques, encryption and decryption, asymmetric and symmetric vital cryptographic, and what the students mean by the critical range and key size.

Unit 3: Symmetric Key Algorithm

It is an introduction to the symmetric key algorithm, the different types and modes of algorithms, an overview of symmetric key cryptography, an overview of DES or Data Encryption Standard algorithm, IDEA (International Data Encryption Algorithm) algorithm, and Rivest Cipher 5 or RC5 algorithm.

Unit 4: Asymmetric Key Algorithm, RSA, and Digital Signature

It is an introduction to the topics mentioned above, an overview of asymmetric key cryptography, the RSA algorithm, what symmetric and asymmetric cryptographies can do together, digital signature, and fundamental concepts of a message digest and hash function.

Unit 5: Protocols Of Internet Security And User Authentication

It involves the fundamental concepts of the topics mentioned above, the meaning and an overview of SSL protocol, the fundamentals of authentication, password, authentication token, and different types of authentication like Certificate-based and biometric-based.

Unit 6: Electronic Mail Security And Firewall

The fundamentals of mail security, what privacy is and how to protect it, an overview of S/MIME, the basics of a firewall, the different types of firewalls, the different configurations of firewalls, and what is a DMZ network.

BSC Cyber Security Syllabus

BSc in cybersecurity is also prominent in today's world of evolving technologies and the internet. BSc in cybersecurity combines theoretical and practical subjects to help students learn about ethical hacking, cryptography, and network security. The primary subjects studied in the course, according to semesters, are discussed below:

Semester 1

The theory subjects studied this semester include fundamentals of computing using C language, the mathematics required for learning cybersecurity and computer science, English communication, python programming, and knowledge of computer networks. In addition, lab work is done on programming with C language, python language, and the basics of computer networks.

Semester 2:

The theory classes include subjects like computer organization and architecture, data structures and algorithms (DSA), knowledge of environmental science, building knowledge of ethical hacking and defense of computer systems, and object-oriented programming concepts. Laboratory work includes data structures and algorithms, object-oriented programming, and ethical hacking.

Semester 3:

Theory classes include database management systems (DBMS), Distributed databases, security architectures and models, operating systems and system programming, analysis of the vulnerability, penetration testing, incident handling, and cyber threats modeling. In addition, laboratory work on DBMS and Operating systems and programming using LINUX is included in the syllabus.

Semester 4

The theory syllabus includes cryptography and information security, cloud computing, ethical hacking systems, defense certifications, software engineering and designing

softwares using UML, and the study of advanced computer networks and securities (TCP/IP, wireless, etc.).
In addition, the semester includes practical work on cryptography and information security, software engineering and the use of UML, and advanced concepts of computer networks and security models in the labs.

Semester 5

The theory subjects of this semester deal with

- cyber forensics
- cyber laws and ethics
- analysis of malware
- reverse engineering
- enterprise security architecture and its designs
- visualization techniques and cyber security models
- detection of intrusion and prevention systems
- IT infrastructure auditing
- big data and IoT security
- disaster recovery
- business continuity management
- data science algorithms,
- study of complexities in cybersecurity
- biometric security

The lab works this semester includes lab work on forensics and malware analysis.

Semester 6

Use of artificial intelligence in cybersecurity and industrial use cases, advanced ethical hacking concepts, an overview of blockchain technology and cryptocurrencies, overview and fundamentals of penetration testing, risk management, and global certifications. The semester includes project work generally on implementing AI in the cybersecurity field.

Cybersecurity Syllabus For MCA

MCA, or Master of Computer Application, is a high-demand field for people wanting to continue their studies in computer applications. One can pursue a degree after graduation with a bachelor's degree. The course stretches for two years and is spread across four semesters. The subjects covered under the MCA cybersecurity course include:

Semester 1:

The first semester introduces the student to cyber security, Linux server administration, network security, dot net framework, C sharp programming, and other web frameworks.

The semester also includes practicals on network security, dot net technology, and web frameworks inside a lab.

Semester 2

This semester introduces the student to advanced concepts of JAVA and J2EE, cybersecurity laws, Cryptographic techniques, Data programming and administration, concepts of ethical hacking, and network management. In addition, there are lab works on cryptography, ethical hacking, and JAVA and J2EE.

Semester 3

The third semester in MCA cybersecurity introduces the student to fundamentals of Android application development, cyber forensics, compiler design, development of e-commerce using Magento, and web application security fundamentals. In addition, there are lab works on Android, cyber forensics, web application security, and a small project.

Semester 4

The final semester of the course is mainly focused on real-life work experience in the industry as an intern and then joining the workforce as a permanent employee. The semester also helps the student gather essential insights on IT company analysis and poster presentation. Project work and dissertation typically involve planning or designing and development, testing or reporting, and presentation of the work and a viva voce.

PG Diploma In Cybersecurity Syllabus

PG Diploma is also a form of higher studies but not a regular master's that people follow after their bachelor's. Most PG Diploma degrees are of one year. However, some can be as short as six months, while others can stretch up to two years. A diploma mainly deals with the hands-on approach to cybersecurity problems in companies. The subjects that students have to deal with when studying Cybersecurity for PG Diploma involve the following:

First Semester

The first semester of the PG Diploma in Cybersecurity helps students know the fundamentals of cybersecurity, concepts of networking and network security, security of operating systems and cyber forensics, and basics of web application and security. There is also a project included in the semester.

Second Semester

In the second semester of the PG Diploma in Cybersecurity, students must study the fundamentals of cryptography, cyber crimes, cyber laws, forensic investigation, and mobile security concepts and attend a seminar on paper presentation. The students then

go for industrial training, where they learn the hands-on approaches required in the cybersecurity industry and submit a final project-cum-assignment.

What Are The Subjects Included In The Cybersecurity Course?

A student pursuing a degree in cybersecurity has to study multiple subjects. Almost all of these relate to computer science and laws surrounding cyber crimes.

Network Security

Network security mainly includes the policies and practices required to stop or detect or monitor suspicious activities, access, and misuse of computer systems. Cybersecurity is essential because it helps students know how to protect sensitive data and keep the systems stable and free from unauthorized usage.

Cryptography

Cryptography or cryptology is a subject that helps codify or encrypt data to prevent unauthorized use. It is one of the most critical subjects in cybersecurity since it helps establish an algorithm that keeps data safe and private and only allows the sender and receiver to read the message. It has great utility in the social media messaging apps of today.

Ethical Hacking

Ethical hacking is a subject that deals with breaking into computer systems for the sake of public security and doing everything lawfully, maintaining all ethics, rules, and regulations. It is an essential subject to learn because it helps the student gain access to a potential cyber criminal and gain access to their plans, which can prevent data breaches and phishing.

Information Security

Information security is that branch of cybersecurity that helps protect sensitive information from unauthorized access. Cybersecurity students must learn information security to efficiently inspect, modify, record, and disrupt any information they want for the public peace. Students must also know all the rules, regulations, and laws behind keeping hold of such information.

Computer Forensics

Computer forensics is a branch of cybersecurity that deals with finding pieces of evidence used to investigate, identify, and store valuable information from a computer system used to do criminal activities. The subject helps students discover secrets and evidence that can lead to cybercrime and give them the required punishment.

Computer Network

The computer network is a branch of computer science that shows how interconnected computers function using network nodes and how the network uses digital interconnections and protocols to communicate. Learning about the subject helps students know how data transmission works and what are its technical aspects. It also helps them gauge how secure the data is and how they can secure it.

Artificial Intelligence

Artificial intelligence, or AI, is a subject that helps machines learn things on their own using appropriate programming and machine learning concepts. AI is a highly demanded skill in the industry, and jobs related to AI development pay well. For example, cybersecurity requires AI to reduce the time taken in doing particular work and also helps scan vast amounts of data without the requirement of humans.

Cybersecurity Course Fee

The list below shows the fee structure of different cybersecurity courses worldwide.

Cybersecurity Course Fee In India

BTech Computer Science	₹2,00,000 to ₹10,00,000	Four years
BSc Cybersecurity	₹1,40,000 to ₹2,00,000	Three years
MCA Cybersecurity	₹1,00,000 to ₹3,00,000	Two to three years
PG Diploma Cybersecurity	₹1,00,000 to ₹3,00,000	One year

Cybersecurity Course Fee In The USA

BTech Computer Science	$20,000 to $60,000	Four years
BSc Cybersecurity	$20,000 to $60,000	Four years
MCA Cybersecurity	$78,000 to $141,000	One to two years
PG Diploma Cybersecurity	$6000 to $45,000	One year

By 10Pie.com

Cybersecurity Course Fee In Australia

BTech Computer Science	AUD20,000 to AUD 70,000	Three years
BSc Cybersecurity	AUD20,000 to AUD 70,000	Three years
MCA Cybersecurity	AUD58,620 to AUD 103,057	Two years
PG Diploma Cybersecurity	AUD 36,249 to AUD 85,900	One year

Cybersecurity Course Fee In Canada

BTech Computer Science	CAD1535 to CAD 55,500	Three to four years
BSc Cybersecurity	CAD1535 to CAD 55,500	Three to four years
MCA Cybersecurity	CAD16,880 to CAD 37,966	One to two years
PG Diploma Cybersecurity	CAD12,000 to CAD 21,000	One to two years

Cybersecurity Course Fee In The UK

BTech Computer Science	GBP27,000 to GBP 36,000	Three years
BSc Cybersecurity	GBP27,000 to GBP 36,000	Three years
MCA Cybersecurity	GBP27,000 to GBP 40,000	Nine months to one year
PG Diploma Cybersecurity	GBP15,000 to GBP 21,000	One year

Top Colleges Cyber Security In India, The US, and The UK

If a student wants to learn cybersecurity in-depth, the student has to join a good college anywhere in the world. This list shows some of the best colleges with cybersecurity discipline worldwide.

Top Cybersecurity Colleges In India

- MAKAUT

- IIT Kanpur
- Anna University
- Brainware University
- Amity University
- SRM Villiammai Engineering College

Top Cybersecurity Colleges In The US

- Carnegie Mellon University
- Massachusetts Institute Of Technology
- University of California - Berkeley
- Purdue University
- Stanford University
- University of Illinois At Urbana - Champaign

Top Cybersecurity Colleges In Australia

- University of Wollongong
- University of New South Wales
- Queensland University Of Technology
- University of Melbourne
- Monash University

Top Cybersecurity Colleges In Canada

- University of Toronto
- University of British Columbia
- University of Waterloo
- Carleton University
- Ryerson University

Top Cybersecurity Colleges In The UK

- Oxford University
- Cambridge University
- Imperial College London
- Edinburgh University
- University of Manchester