



**PROF. RAJENDRA SINGH (RAJJU BHAIYA) UNIVERSITY,  
PRAYAGRAJ**

**(Offered by Department of Computer Science)**

# **Course Title: Cyber Security**

**Course Code – IO10023T**

**Credit: 03**

**MM: 100 (40+60)**

---

## **Vocational / Skill Enhancement Course**

**(Session: January 2024-25 Onwards)**



सत्यमेव जयते



ज्ञान-विज्ञान विमुक्तये

**The University Grants Commission**  
Bahadur Shah Zafar Marg  
New Delhi – 110002  
[www.ugc.ac.in](http://www.ugc.ac.in)

## Contents

S. No.	Particulars	Page No.
1.	<b>Introduction</b>	3
2.	<b>Terms of Reference</b>	3
3.	<b>Essential Components of Cyber security</b>	3
4.	<b>Program Educational Objectives (PEOs)</b>	4
5.	<b>Program Specific Outcomes (PSOs)</b>	4
6.	<b>Syllabus of Cyber Security Program at Undergraduate Level</b>	5

## TEACHING SCHEME

### Cyber security Program at Undergraduate Level and Postgraduate Level

Sl. No	Course Title	Teaching Scheme at UG Level		
		L/T	P	C
1	Cyber Security	2	1	3

#### Legend:

**L:** Lectures      **T:** Tutorials      **P:** Practical/Projects      **C:** Credits

**NOTE :** As far as transaction of these courses at UG level in HEIs is concerned, HEIs may invite Cyber Security/Computer/IT qualified faculty or else Experts from Industry/Subject Matter Experts to take the lectures, practical and tutorials. The syllabus gives broad guidelines and teachers who would teach the subject will have enough flexibility to strike the balance between time vis-a-vis depth of coverage.

# Syllabus of Cyber Security Course at Undergraduate level

## Introduction

The evolution of Information Communication Technology (ICT) and growing security concerns demands flexible and generally comprehensive approach to the issue of cyber security. The rapid growth of ICT has raised various complex questions which need to be addressed. A need has been felt to address cyber security broadly, as also in sufficient depth so that even students from non-technical streams will develop a more complete picture of the cyber security issues. The syllabus has been prepared with an aim to create more aware, responsive and responsible digital citizens, thereby contributing effectively to an overall healthy cyber security posture and ecosystem.

## Terms of Reference


### 2. Terms of Reference (TOR) for drafting the syllabus.

- (a) The syllabus should incorporate all the essential elements of cyber security so that the students at the Graduation level understand the essence and concept of cyber security as a whole.
- (b) The syllabus of cyber security at the Undergraduate level to be pitched at basic and mid-level should cover mid and advanced level concepts, duly considering the fact that Post Graduation students would have exposure to the basic concepts of cyber security in the preceding degree.
- (c) The syllabus should have sufficient depth so that even students from the non-technical streams can develop a complete picture of cyber security.

## Essential Components of Cyber security

3. People, Process and Technology are the important pillars of the Cyber security, as to how, effectively the aspects related to these components fit into the curriculum considering the cyber threat landscape forms part of the content structuring and syllabus formation. With this backdrop, the following aspects, as tabulated below, have been taken into consideration in the syllabus formation: -

Sl. No.	Content	Level
(a)	Essential components of cyber security	Basic
(b)	Cyber security threat landscape	Basic
(c)	Cyber crime and its types	Basic – Medium
(d)	Remedial and mitigation measures	Basic
(e)	Reporting of Cyber crime	Basic



Sl. No.	Content	Level
(f)	Cyber Law	Basic
(g)	Data privacy and security	Basic
(h)	E-Commerce, Digital payments and its security	Medium
(i)	Overview of Social media and its security	Medium
(j)	Cyber security of digital devices	Medium
(k)	Tools and technology for cyber security	Medium
(o)	Cyber security best practices and do's and don'ts	Medium
(p)	Platforms to report and combat cyber crime	Basic
(q)	Practical hands-on	Basic-Medium and Advanced

### Program Educational Objectives (PEOs)

4. The exposure of the students to Cyber Security program at Graduate level should lead to the following: -
  - (a) Learn the foundations of Cyber security and threat landscape.
  - (b) To equip students with the technical knowledge and skills needed to protect and defend against cyber threats.
  - (c) To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
  - (d) To expose students to governance, regulatory, legal, economic, environmental, social and ethical contexts of cyber security.
  - (e) To expose students to responsible use of online social media networks.
  - (f) To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societal context.
  - (g) To select suitable ethical principles and commit to professional responsibilities and human values and contribute value and wealth for the benefit of the society.

### Program Specific Outcomes (PSOs)

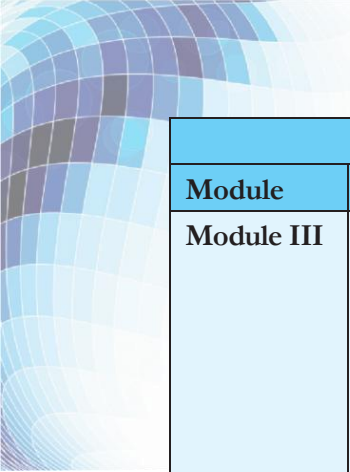
5. Upon completion of the degree program, students will be able to:-
  - (a) Understand the cyber security threat landscape.
  - (b) Develop a deeper understanding and familiarity with various types of cyber attacks, cyber crimes, vulnerabilities and remedies there to.
  - (c) Analyse and evaluate existing legal framework and laws on cyber security.
  - (d) Analyse and evaluate the digital payment system security and remedial measures against digital payment frauds.

- (e) Analyse and evaluate the importance of personal data its privacy and security.
- (f) Analyse and evaluate the security aspects of social media platforms and ethical aspects associated with use of social media.
- (g) Analyse and evaluate the cyber security risks.
- (h) Based on the Risk assessment, plan suitable security controls , audit and compliance.
- (i) Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.
- (j) Increase awareness about cyber-attack vectors and safety against cyber-frauds.
- (k) Take measures for self-cyber-protection as well as societal cyber-protection.

### Syllabus of Cyber Security Program at Undergraduate Level

6. The syllabus at Undergraduate level academic program is as under: -

Cyber security Program at Undergraduate Level			
Module	Module Name	Module Content	Learning Outcomes
Module I	Introduction to Cyber security	Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security.	After completion of this module, students would be able to understand the concept of Cyber security and issues and challenges associated with it.
Module II	Cyber crime and Cyber law	Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies.	Students, at the end of this module, should be able to understand the cyber crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.
Practical	1. Checklist for reporting cyber crime at Cyber crime Police Station. 2. Checklist for reporting cyber crime online. 3. Reporting phishing emails. 4. Demonstration of email phishing attack and preventive measures.		



Cyber security Program at Undergraduate Level			
Module	Module Name	Module Content	Learning Outcomes
Module III	Social Media Overview and Security	Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies.	On completion of this module, students should be able to appreciate various privacy and security concerns on online Social media and understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms.
Practical	1. Basic checklist, privacy and security settings for popular Social media platforms. 2. Reporting and redressal mechanism for violations and misuse of Social media platforms.		
Module IV	E-Commerce and Digital Payments	Definition of E-Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorised banking transactions. Relevant provisions of Payment Settlement Act, 2007,	After the completion of this module, students would be able to understand the basic concepts related to E-Commerce and digital payments. They will become familiar with various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds.
Practical	1. Configuring security settings in Mobile Wallets and UPIs. 2. Checklist for secure net banking.		

Cyber security Program at Undergraduate Level			
Module	Module Name	Module Content	Learning Outcomes
Module V	Digital Devices Security, Tools and Technologies for Cyber Security	End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	Students, after completion of this module will be able to understand the basic security aspects related to Computer and Mobiles. They will be able to use basic tools and technologies to protect their devices.
Practical	<ol style="list-style-type: none"> <li>1. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).</li> <li>2. Setting and configuring two factor authentication in the Mobile phone.</li> <li>3. Security patch management and updates in Computer and Mobiles.</li> <li>4. Managing Application permissions in Mobile phone.</li> <li>5. Installation and configuration of computer Anti-virus.</li> <li>6. Installation and configuration of Computer Host Firewall.</li> <li>7. Wi-Fi security management in computer and mobile.</li> </ol>		
References	<ol style="list-style-type: none"> <li>1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.</li> <li>2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)</li> <li>3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)</li> <li>4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.</li> <li>5. Cyber Laws: Intellectual Property &amp; E-Commerce Security by Kumar K, Dominant Publishers.</li> <li>6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.</li> <li>7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.</li> </ol>		

\*\*\*\*\*