# Syllabus of Cyber Security Course at Undergraduate and Post Graduate level



**The University Grants Commission**
Bahadur Shah Zafar Marg
New Delhi – 110002
www.ugc.ac.in

# Contents

# Syllabus of Cyber Security Course at Undergraduate and Post Graduate 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 proposed syllabus.**

(a) Cyber security as a subject needs to be incorporated at Graduation and Post-Graduation level in all the streams.

(b) A separate syllabus for Graduation and Post-Graduation program to be prepared.

(c) The syllabus should incorporate all the essential elements of cyber security so that the students at the Graduation and Post-Graduation level understand the essence and concept of cyber security as a whole.

(d) The syllabus of cyber security at the Undergraduate level to be pitched at basic and mid-level wherein the syllabus at Post Graduate 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.

(e) 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 |
| (l) | Cyber security plan and crisis management | Advanced |
| (m) | Security controls | Advanced |
| (n) | Risk based assessment, audit and compliance | Advanced |
| (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 and Post 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 cyberattacks, cyber crimes, vulnerabilities and remedies thereto.

(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 o n 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 proposed 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.<br>2. Checklist for reporting cyber crime online.<br>3. Reporting phishing emails.<br>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.<br>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 Payament 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.<br>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 | 1. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).<br>2. Setting and configuring two factor authentication in the Mobile phone.<br>3. Security patch management and updates in Computer and Mobiles.<br>4. Managing Application permissions in Mobile phone.<br>5. Installation and configuration of computer Anti-virus.<br>6. Installation and configuration of Computer Host Firewall.<br>7. Wi-Fi security management in computer and mobile. | | |
| References | 1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.<br>2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)<br>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)<br>4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.<br>5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.<br>6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.<br>7. Fundamentals of Network Security by E. Maiwald, McGraw Hill. | | |

## Syllabus of Cyber Security Program at Post Graduate Level

7. The syllabus for **Cyber Security Program at Post Graduate Level** is as under: -

| Cyber Security Program at Post Graduate Level | | | |
|---|---|---|---|
| **Module** | **Module Name** | **Module Contents** | **Learning Outcome** |
| **Module-I** | Overview of Cyber security | Cyber security increasing threat landscape, Cyber security terminologies- Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker., Non-state actors, Cyber terrorism, Protection of end user machine, Critical IT and National Critical Infrastructure, Cyberwarfare, Case Studies. | Students after completing this module will be able to understand the basic terminologies related to cyber security and current cyber security threat landscape. They will also develop understanding about the Cyberwarfare and necessity to strengthen the cyber security of end user machine, critical IT and national critical infrastructure. |
| **Module-II** | Cyber crimes | Cyber crimes targeting Computer systems and Mobiles- data diddling attacks, spyware, logic bombs, DoS, DDoS, APTs, virus, Trojans, ransomware, data breach., Online scams and frauds- email scams, Phishing, Vishing, Smishing, Online job fraud, Online sextortion, Debit/ credit card fraud, Online payment fraud, Cyberbullying, website defacement, Cyber-squatting, Pharming, Cyber espionage, Cryptojacking, Darknet- illegal trades, drug trafficking, human trafficking., Social Media Scams & Frauds- impersonation, identity theft, job scams, misinformation, fake newscyber crime against persons - cyber grooming, child pornography, cyber stalking., Social Engineering attacks, Cyber Police stations, Crime reporting procedure, Case studies. | After completion of the module, students will have complete understanding of the cyber-attacks that target computers, mobiles and persons. They will also develop understanding about the type and nature of cyber crimes and as to how report these crimes through the prescribed legal and Government channels. |

| Cyber Security Program at Post Graduate Level | | | |
|---|---|---|---|
| **Module** | **Module Name** | **Module Contents** | **Learning Outcome** |
| **Practical** | 1. Platforms for reporting cyber crimes.<br>2. Checklist for reporting cyber crimes online. | | |
| **Module-III** | Cyber Law | Cyber crime and legal landscape around the world, IT Act,2000 and its amendments. Limitations of IT Act, 2000. Cyber crime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, IoT, Blockchain, Darknet and Social media, Cyber Laws of other countries, Case Studies. | Students after completing this module will be able to understand the legal framework that exist in India for cyber crimes and penalties and punishments for such crimes, It will also expose students to limitations of existing IT Act,2000 legal framework that is followed in other countries and legal and ethical aspects related to new technologies. |
| **Module IV** | Data Privacy and Data Security | Defining data, meta-data, big data, non-personal data. Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries- General Data Protection Regulations(GDPR),2016 Personal Information Protection and Electronic Documents Act (PIPEDA)., Social media- data privacy and security issues. | After completing this module, students will understand the aspects related to personal data privacy and security. They will also get insight into the Data Protection Bill,2019 and data privacy and security issues related to Social media platforms. |
| **Practical** | 1. Setting privacy settings on social media platforms.<br>2. Do's and Don'ts for posting content on Social media platforms.<br>3. Registering complaints on a Social media platform. | | |

| Cyber Security Program at Post Graduate Level | | | |
|---|---|---|---|
| **Module** | **Module Name** | **Module Contents** | **Learning Outcome** |
| **Module V** | Cyber security Management, Compliance and Governance | Cyber security Plan- cyber security policy, cyber crises management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy. | Students after completing this module will understand the main components of cyber security plan. They will also get insights into risk-based assessment, requirement of security controls and need for cyber security audit and compliance. |
| **Practical** | 1. Prepare password policy for computer and mobile device.<br>2. List out security controls for computer and implement technical security controls in the personal computer.<br>3. List out security controls for mobile phone and implement technical security controls in the personal mobile phone.<br>4. Log into computer system as an administrator and check the security policies in the system. | | |
| **References** | 1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.<br>2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.<br>3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.<br>4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.<br>5. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.<br>6. Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning. | | |

## Practical Work

8. The practical list has been suggested for the applicable modules; however, the faculty may expand the list as per the syllabus content duly taking into consideration the emerging nature of cyber threats and incumbent protective measures to guard against such threats.

# TEACHING SCHEME

## Cyber security Program at Undergraduate Level and Postgraduate Level

| Sl. No | Course Title | Teaching Scheme at UG and PG Level | | |
|---|---|---|---|---|
| | | L/T | P | C |
| 1 | Cyber Security | 3 | 1 | 4 |

**Legend:**

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

**Notes:**

1 Credit: 1 Hour for Lecture/Tutorial

1 Credit: 2 Hour for Practical/Projects

**Terms of Reference for Credit Scheme ( 3+1)**

- There are total of 90-96 working days (15 -16 Weeks) in a semester.
- 1 Credit = 15 Hours, therefore 3 Credits = 45 hours (3*15=45)
- In a week, (3 lectures of theory, each period of one hour duration every week-.45 hours in a semester) and 1 practical session of two hours ( 30 hours in a semester)

**Notes:**

1 C: 1 Hour for Lecture/Tutorial

C: 2 Hour for Practical/Projects

**Terms of Reference for Credit Scheme (3+1)**

- There are total of 90-96 working days (15 -16 Weeks) in a semester.
- 1 Credit = 15 Hours, therefore 3 Credits = 45 hours (3*15=45)
- In a week, 3 lectures of theory, each period of one hour duration every week, (45 hours in a semester) and 1 practical session of two hours. (30 hours in a semester)

**NOTE : As far as transaction of these courses at UG and PG 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, practicals and tutorials. The proposed 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.**

***