

Syllabus of Cyber Security Course at Post Graduate level

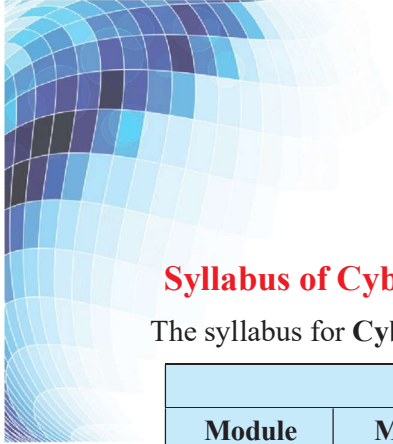


सत्यमेव जयते



ज्ञान-विज्ञान विमुक्तये

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

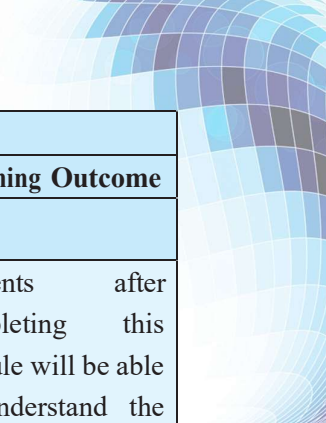


Syllabus of Cyber Security Program at Post Graduate Level

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 news, cyber 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.		
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. 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. 2. List out security controls for computer and implement technical security controls in the personal computer. 3. List out security controls for mobile phone and implement technical security controls in the personal mobile phone. 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. 2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley. 3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. 4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press. 5. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication. 6. Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.		