

Syllabus of Cyber Security Course at Undergraduate level



सत्यमेव जयते



ज्ञान-विज्ञान विमुक्तये

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

Contents

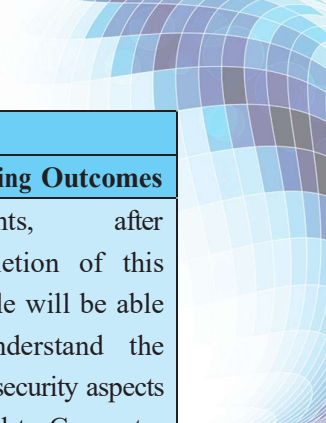
Syllabus of Cyber Security Program at Undergraduate Level

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. Reporting phishing emails. 2. 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. 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 stakeholders, 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.		



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 Anti-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). 2. Security patch management and updates in Computer and Mobiles. 3. Managing Application permissions in Mobile phone. 4. Installation and configuration of computer Anti-virus. 5. Installation and configuration of Computer Host Firewall.		
References	1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010. 2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) 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) 4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd. 5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers. 6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd. 7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.		