



Syllabus for CYBER SECURITY Undergraduate Level

Paper Title: Cyber Security

Paper Code: UGCSSE305

Total Credit: 3

Total Contact Hours: 45 Hours

Total Marks: 80 (Written: 40 + Internal:20 + Practical: 20)

L-T-P: 1-1-1

Course Introduction: The Cyber Security course introduces undergraduate students to the fundamentals of cyberspace, cyber threats, cyber laws, social media safety, and digital security practices. It helps students understand how to protect personal information, use digital technologies safely, and recognize common online frauds and cyber-crimes. The course develops essential digital awareness and responsible online behaviour required for academic, professional, and everyday life in the digital age.

Target Students: This course is intended for **B.A. Third Semester undergraduate students** who seek to improve their digital literacy and cyber security awareness.

Course Objective:

1. Introduce the concepts of cyberspace and the importance of cyber security.
2. Explain the architecture of cyberspace and the regulation of internet infrastructure.
3. Classify cyber-crimes and analyse common cyber threats, including financial frauds, and malware attacks.
4. Familiarize students with the IT Act 2000, its amendments, and organizations addressing cyber-crime in India.
5. Provide an overview of social media platforms, their security issues, and best practices for safe usage.
6. Explore e-commerce components, security threats, and preventive measures for digital payment frauds.
7. Discuss tools and techniques for securing digital devices and endpoint security management.
8. Emphasize best practices for maintaining password policies and managing third-party software.
9. Highlight the role of laws, regulations, and case studies in understanding and addressing cyber security challenges.



The main outcomes of learning Cyber Security:

1. Fundamental Knowledge of Cyber Security
2. Awareness of Cyber Threats
3. Networking and System Security Skills
4. Incident Response and Risk Management
5. Ethical and Legal Awareness
6. Recognize and Report Cyber-crimes

Syllabus

Unit-I: Introduction to Cyber security

Lectures-Tutorials-Practicals: 5-0-0 | Hours: 5

Defining cyberspace and overview of computer and web-technology, Importance of cyber security, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Internet infrastructure for data transfer and governance, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security.

Unit-II: Cyber-crime and Cyber law

Lectures-Tutorials-Practicals: 5-1-2 | Hours: 10

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, Reporting of cyber-crimes, Legal perspective of cyber-crime, IT Act 2000 and its amendments, Organisations dealing with Cyber-crime and cyber security in India, Case studies.

Unit-III: Social Media Overview and Security

Lectures-Tutorials-Practicals: 5-1-2 | Hours: 10

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.





Unit-IV: E-Commerce and Digital Payments

Lectures-Tutorials-Practicals: 5-1-2 | Hours: 10

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, Aadhar enabled payments, Digital payments related common frauds and preventive measures, RBI guidelines on digital payments and customer protection in unauthorised banking transactions.

Unit-V: Digital Devices Security, Tools and Technologies for Cyber Security

Lectures-Tutorials-Practicals: 5-1-2 | Hours: 10

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, Wi-Fi security, Configuration of basic security policy and permissions.

Evaluation Pattern

External		Internal	
MCQ	1x10=10	Assignment	1x10=10
Short Question	5x6=30	Quiz	1x10=10
Practical	2x10=20	Total	20
Total	60		

Reference Book:

- Chimwanda, E. (2025). *Cybersecurity essentials you always wanted to know: A practical guide to cybersecurity, risk management, encryption, cloud security & security frameworks*. Mumbai, India: Vibrant Publishers.
- Kumar, K. (2011). *Cyber law: Intellectual property and e-commerce security*. New Delhi, India: Dominant Publishers & Distributors.
- Mishra, R. C. (2002). *Cyber crime: Impact on the new millennium*. New Delhi, India: Authors Press.