BA Semester - VII

Course Code	**UA07HMICOP01**	Title of the Course	**Cyber Security and Security Measures**
Total Credits of	**4**	Hours per Week	**4 (2 Theory + 2 Practical per Batch)**

Course Objectives:	1. To understand the fundamentals of cyber security and digital threats, cyber threats, cyber crimes, and security vulnerabilities. 2. To develop awareness of cyber laws, ethics, and safe online practices. 3. To develop knowledge of security management practices and risk mitigation. 4. To familiarize students with cyber laws, ethics, and emerging security technologies.

Course Content		
Unit	Description	Weightage* (%)
1.	**Fundamentals of Cyber Security:** Introduction to Cyber Security, Need and Importance of Cyber Security, Cyber Space and Digital Environment. Security Challenges in the Digital Era **Security Concepts:** Confidentiality, Integrity, Availability. **Types of Cyber Threats and Vulnerabilities:** Malware, Virus, Worm, Trojan Horse, Spyware, Ransomware, Social Engineering Attacks, Phishing, Vishing and Smishing, Identity theft, Importance of Cyber Security in Modern Society	25%
2.	**Security Issues in E-Commerce Platforms:** **Data Breaches:** Unauthorized access to customer databases resulting in leakage of: • Personal information • Addresses • Contact details • Payment information **Payment Fraud** • Credit card fraud • Debit card fraud • Fake payment confirmations • Chargeback fraud **Phishing Attacks:** Fraudulent emails or websites designed to: • Steal login credentials • Obtain banking details • Trick users into making payments **Malware and Ransomware:** Malicious software may: • Steal customer data • Encrypt business information	25%

	• Disrupt online business operations **Account Takeover:** Attackers gain unauthorized access using: • Weak passwords • Password reuse • Credential theft	
3.	**Security Issues in Social Media Platforms** **Privacy Violations:** Users often share: • Personal details • Photos and videos • Location information Improper handling can lead to privacy breaches. **Identity Theft:** Attackers may • Create fake profiles • Impersonate individuals • Conduct fraud using stolen identities **Social Engineering:** Manipulating users into revealing • Passwords • OTPs • Personal information **Account Hijacking:** Unauthorized access due to • Weak passwords • Phishing attacks • Malware infections **Cyberbullying and Harassment:** Misuse of social media for • Threatening users • Online abuse • Defamation **Spread of Malware and Fake Links:** Attackers distribute • Malicious advertisements • Infected files • Fraudulent websites	25%
4.	**Security Measures for E-Commerce and Social Media** **Technical Measures** • Secure Socket Layer (SSL) Certificates • Data Encryption • Firewalls • Anti-malware Software • Regular Security Audits **User-Level Measures** • Strong Passwords • Multi-Factor Authentication (MFA) • Avoiding Suspicious Links • Regular Password Updates • Privacy Settings Management **Best Practices for Safe Digital Usage** For E-Commerce Users • Shop only on trusted websites.	

	• Verify HTTPS security. • Use secure payment gateways. • Monitor transaction records. For Social Media Users • Limit personal information sharing. • Enable two-factor authentication. • Accept requests only from known persons. • Report suspicious activities immediately. **Cyber Law and Information Technology Act, 2000:** Introduction to Cyber Law	

Suggested practical list are as under:

#	Practical Title	Learning Outcome
1	**Identifying Common Cyber Threats** – Visit sample websites/videos showing malware, phishing, ransomware, spyware, and social engineering attacks. Prepare a comparison table of each threat, its characteristics, and preventive measures.	Understand different cyber threats and their impact.
2	**CIA Triad Demonstration** – Create a document and demonstrate Confidentiality (password protection), Integrity (hash/checksum comparison), and Availability (cloud backup/local backup).	Understand Confidentiality, Integrity, and Availability through practical examples.
3	**Password Strength Analysis** – Use an offline/open-source password strength checker or browser password manager to evaluate different passwords. Compare weak and strong passwords and prepare guidelines.	Learn secure password creation and authentication concepts.
4	**Security Evaluation of E-Commerce Websites** – Compare three popular e-commerce websites based on HTTPS, SSL certificate, privacy policy, payment options, and security features. Prepare an evaluation report.	Identify security features in e-commerce platforms.
5	**Recognizing Phishing Websites and Emails** – Examine sample phishing emails and fake shopping websites. Identify suspicious URLs, spelling mistakes, fake payment pages, and security indicators.	Learn to identify phishing attacks.
6	**Secure Online Shopping Checklist** – Simulate an online purchase without making payment. Verify HTTPS, SSL certificate, seller ratings, return policy, payment gateway, and transaction security.	Practice safe online shopping habits.
7	**Privacy Settings Audit on Social Media** – Review privacy settings of a social media account (or demo account). Configure profile visibility, post visibility, location sharing, and friend request settings. Document the changes.	Learn privacy management on social media.
8	**Fake Profile and Identity Theft Awareness** – Compare genuine and fake social media profiles using publicly available examples. Identify warning signs such as profile picture, followers, posts, and account age.	Recognize identity theft and fake profiles.
9	**Social Engineering Case Study** – Analyze real-world cases of phishing, OTP fraud, account hijacking, cyberbullying, or fake links. Identify attack methods and preventive measures. Present findings in class.	Understand social engineering attacks and defenses.

10	**Implementing Multi-Factor Authentication (MFA)** – Enable MFA on a Google, Microsoft, or other demo account. Observe login behavior before and after enabling MFA. Document the process.	Understand the role of MFA in account security.
11	**Browser Security and Safe Browsing** – Configure browser security settings including password manager, safe browsing, pop-up blocker, cookie permissions, and privacy options. Compare default and secure settings.	Learn browser security best practices.
12	**Cyber Law Case Study (IT Act 2000)** – Study one cybercrime case reported in India. Identify the nature of the crime, applicable provisions of the Information Technology Act, 2000, and preventive measures.	Understand the application of cyber law in real-life scenarios.

Suggested Software/Resources

- Web browser (Chrome, Firefox, Edge)
- Browser Developer Tools (for SSL certificate inspection)
- Google Account/Microsoft Account (for MFA demonstration)
- Free password strength checker (offline preferred)
- Sample phishing email repositories (educational)
- VirusTotal (URL/file analysis without downloading malware)
- Public cyber awareness portals (CERT-In, Cyber Dost)

Teaching-Learning Methodology	Theory (50%) + Practical (50%) Practical: Practical are based on above Units. (Weightage 50%) – Two Practical periods per week per batch. Multiple teaching approaches: Lectures and discussion, exploration and inquiry, cooperative group work, demonstration, and presentation. Traditional classroom teaching as well as online/ICT based teaching practices. Hands on training through required ICT tools.

Sr. No.	Details of the Evaluation / Exam Pattern	50 Marks (%)	25 Marks (%)
1	Class Test (at least one)	15 (30%)	10 (40%)
2	Quiz (at least one)	15 (30%)	05 (20%)
3	Active Learning	05 (10%)	----
4	Home Assignment	05 (10%)	05 (20%)
5	Class Assignment	05 (10%)	----
6	Attendance	05 (10%)	05 (20%)
Total Internal (%)		50 (100%)	25 (100%)
University Examination (%)		50 (100%)	25 (100%)

Model for Theory Courses		
CEE (50%)		
Exam Pattern	**50 Marks**	**25 Marks**
Class Test (at least one)	15 (30%)	10 (40%)
Quiz (at least one)	15 (30%)	05 (20%)
Active Learning	05 (10%)	--
Home Assignment	05 (10%)	05 (20%)
Class Assignment	05 (10%)	--
Attendance	05 (10%)	05 (20%)
Total	50 (100%)	25 (100%)

Evaluation Pattern		
Sr. No.	Details of the Evaluation	Weightage
1.	Internal Written / Practical Examination (As per CBCS R.6.8.3) Internal Continuous Assessment in the form of Practical, Viva-voce, Quizzes, Seminars, Assignments, Attendance (As per CBCS R.6.8.3)	50%
2.	University Examination (Theory 50% + Practical 50%)	50%

Course Outcomes: Upon successful completion of the course, students will be able to:	
1.	Understand the concept of cybersecurity in digital platforms.
2.	Identify security threats faced by e-commerce websites and their users
3.	Analyze security risks associated with social media platforms.
4.	Evaluate best practices for safe use of e-commerce and social networking services.

Suggested References:	
Sr. No.	References
1.	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (Second Edition) by Nina Godbole & Sunit Belapure,Wiley India
2.	Information Technology Law and Practice (6^{th} Edition) by Vakul Sharma, Universal Law Publishing
3.	Cyber Law in India (Revised Edition) by Farooq Ahmad, Allahabad Law Agency

4.	Introduction to Cyber Security (Latest Edition) by Anand Shinde, Technical Publications
5.	Cyber Security Essentials by Charles J. Brooks, Christopher Grow et al., John Wiley & Sons
6.	Cyber Laws and Information Technology (Latest Edition) by Yatindra Singh, Universal Law Publishing
7.	Computer Security Fundamentals (4th Edition) by William Easttom, Pearson
8.	Guide to Cyber Laws by Rodney D. Ryder, Wadhwa and Company
10.	Cyber Crime: Investigation, Prevention and Protection – CRC Press.
11.	Information Technology Act, 2000 with Allied Rules – Universal Law Publishing.
12.	Cyber Law (3rd Edition, 2023): An Exhaustive Section-wise Commentary on the Information Technology Act by Pavan Duggal, LexisNexis India
13.	Information Technology Act 2000 with Rules and Allied Laws Government Publication

On-line resources to be used if available as reference material
On-line Resources
Indian Cyber Law, Information Technology Act, 2000, data protection, digital evidence, and cybercrime laws. https://www.youtube.com/@PavanDuggalCyberlawUniversity?utm_source=chatgpt.com
NALSAR University of Law. Lectures and webinars on cyber law, privacy law, and technology law. https://www.youtube.com/@NALSARUniversityofLaw?utm_source=chatgpt.com
CERT-In (Indian Computer Emergency Response Team) — Cybersecurity advisories, awareness material, and incident reporting. https://www.cert-in.org.in?utm_source=chatgpt.com

*****