B.A. (VS) Modern Office Management

Semester V

DISCIPLINE SPECIFIC ELECTIVE COURSE – DSE-5.2

Cyber Crimes and Laws

CREDIT DISTRIBUTION, ELIGIBILITY AND PRE-REQUISITES OF THE COURSE

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Cyber Crimes and Laws (DSE-5.1)	**4**	**3**	**1**	**-**	**12th Pass**	**-**

Learning Objectives: The course aims to create an understanding of cyber-crimes and familiarize the students with the application of cyber laws in business and day to day life.

Learning Outcomes: After completion of the course, learners will be able to:

1. analyse cyber risk associated with online activities and develop related cyber hygiene.
2. prepare protocols for safe working in the verticals having varied access points, data sources, network, and system-related issues in online activities.
3. work safely in global virtual space conforming to the regulatory framework and not falling under the ambit of cybercrimes.
4. generate and preserve electronic evidence for personal and professional use.
5. analyse the cases and find pertinent facts for resolutions on managerial cyber issues.

Unit 1: Introduction to Cybercrimes **9 hours**

Computer crime and cybercrimes; Distinction between cybercrime and conventional crimes; Kinds of cybercrimes - cyber stalking, cyber terrorism, forgery and fraud, crimes related to IPRs, cyber defamation, computer vandalism, cyber forensic.

Unit 2: Contemporary Business Issues in Cyber Space **9 hours**

Web-Centric Business, E-Business, and its significance, Instant messaging platform, social networking sites and mobile applications, security risks, Cyber jurisdiction, E-forms; Electronic Money Transfer and UPI, Privacy of Data and Secure Ways of Operation in Cyber Space.

Unit 3: Legal framework and Cyber Laws in India **9 hours**

Definitions under IT Act, 2000; Authentication of Electronic Records; Electronic Governance; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Applications and usage of electronic records and Digital Signatures in Government and its Agencies; Retention of Electronic Records, Intermediaries, and their liabilities; E-signatures.

Unit 4: Regulatory Framework and International Perspective **9 hours**

Regulation of Certifying Authorities; Appointment and Functions of Controller; License to issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences; Regulations of PPI (Pre- Payment Instruments) by RBI, Overview of GDPR and Indian data protection regime.

Unit 5: Case Laws **9 hours**

1. Communication Device-Section 2(ha) of the Information Technology (Amendment) Act, 2008-'State v Mohd. Afzal and others (2003), VIIAD (Delhi) 1, 107(2003) DLT385, 2003(71) DRJ178, 2003(3) JCC1669'
2. Computer Network-Section 2 (j) of the Information Technology (Amendment) Act, 2008 'Diebold System Pvt Ltd. v The Commissioner of Commercial Taxes, (2006), 144 STC, 59 (Kar)'
3. Electronic Record Sec. 2 (t)- 'Dharambir v Central Bureau of Investigation 148 (2008) DLT 289'
4. Penalty for Damage to Computer or Computer System- Section 43-'Umashankar Sivasubramanian v ICICI Bank, 18.04.2010. (Petition No. 2462/2008)'
5. Tampering with Computer Source Documents-Section 65-'Syed Asifuddin and Ors.v The State of Andhra Pradesh &Anr. 2006 (1) ALD Cri 96, 2005 CriLJ 4314'
6. Punishment for sending offensive messages-Sec. 66A- 'SMC Pneumatics (India) Pvt. Ltd v JogeshKwatra", Suit No. 1279/2001'
7. Punishment for Identity Theft-Section 66C- 'CBI v Arif Azim Case Judicial Reports (Criminal) 2003 (2) page 272'
8. Punishment for Cheating by Personating by using Computer Resource-section 66D- 'National Association of Software and Service Companies (NASSCOM)v Ajay Sood. (2005) F.S.R. 38; 119 (2005) DLT 596, 2005 (30) PTC 437 Del'
9. Punishment for Publishing or Transmitting Obscene Material in Electronic form section 67-'Avnish Bajaj v State (N.C.T.) of Delhi, (2005) 3 Comp, LJ 364 (Del), 116(2005) DLT427, 2005(79) DRJ576'
10. Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act, etc., in Electronic Form-Section 67A-'R v Graham Waddon., Southwark [Crown Court, 30/6/1999]'

Exercises:

The learners are required to:

1. Discuss recent cyber-crime cases reported in dailies and spread awareness about various cyber offences and remedies available.
2. Conduct a survey to ascertain the awareness about various cybercrimes in their nearby locality and prepare easy do's and don'ts for most problematic areas.
3. Enlist cyber hygiene and usage of e-signatures/digital signatures in daily life for improved cyber hygiene.
4. Describe and evaluate the procedure of recording and maintaining electronic evidence, filing online and offline complaints in Cyber Cells.
5. Analyse recent cases related to various cybercrimes and draw implications for managers.

Suggested Readings

- Arora, S., & Arora, R. (2021). *Cybercrimes and laws*, New Delhi: Taxmann Pvt. Ltd.
- Brian, C. (2012). Cyber Law: The Law of the Internet and Information Technology. Pearson Education.
- Gusai, O. P. (2019). Concept Building Approach to Cybercrimes and Cyber Laws: Indian and International Perspective, Delhi: Cengage Learning India Pvt. Ltd.
- Sharma J. P., and Kanojia, S. (2018). E-Business and Cyber Laws. New Delhi: Bharat Law House Pvt Ltd.

Additional Resources

- Joseph, P.T. (2012). *E-Commerce-An Indian Perspective*. PHI
- Rattan, J. (2022). *Cyber Crime and Information Technology*, Bharat Law House, Pvt Ltd.

Notes:

1. **Suggested readings shall be updated and uploaded on the college website from time to time.**
2. **Examination scheme and mode shall be prescribed by the Examination branch, University of Delhi from time to time.**