S.S. JAIN SUBODH P.G. COLLEGE, JAIPUR
(AUTONOMOUS)
Syllabus
Skill Enhancement Course(SEC)
(For BBA III sem)

Credits: 2
Classes per week:- 2

Maximum Marks:-50
EoSE:-35
CIA:-15

Introduction to Cyber Security

Unit - I

Introduction to Cyber Space, History of Internet, Cyber Crime, Information Security, Computer Ethics and Security Policies, email security, securing web browser, Antivirus, Guidelines for secure password and wi-fi security, Guidelines for setting up a Secure password, Two-steps authentication, Password Manager

Unit -II.

Guidelines for basic Windows security, Guidelines for social media security, Tips and best practices for safer Social Networking, User Account Password, Smartphone security guidelines, Online Banking, Credit Card and UPI Security, Online Banking Security, Mobile Banking Security, Security of Debit and Credit Card, POS Security, Security of Micro ATMs, e-wallet Security Guidelines

Unit -III

Social Engineering, Types of Social Engineering, How Cyber Criminal Works, how to prevent for being a victim of Cyber Crime, Cyber Security Threat Landscape and Techniques, Emerging Cyber Security Threats, Cyber Security Techniques, Firewall

Unit-IV

Cyber Security Initiatives in India, Cyber Security Incident Handling, Cyber Security Assurance, IT Security Act, Hackers-Attacker-Countermeasures, Web Application Security, Digital Infrastructure Security, Defensive Programming, Information Destroying and Recovery Tools, Destroying Sensitive Information

Suggested Books and References –

1. V. S. Bagad, I. A. Dhotre and Manish Khodaskar, "Information and Cyber Security", Technical Publications, 2nd Edition, 2019.
2. Surya Prakash Tripathi, RitendraGoel and Praveen Kumar Shukla, "Introduction to Information Security and Cyber Laws", Dreamtech Press, 1st Edition, 2014.
3. Nilakshi Jain and Dhananjay R. Kalbande, "Digital Forensic: The Fascinating World of Digital Evidences", Wiley, 1st Edition, 2016.
4. R. K. Tiwari, P. K. Sastry and K. V. Ravikumar, "Computer Crime and Computer Forensic", Select Publisher, 1st Edition 2002.

Course Learning Outcomes:

By the end of the course, students should be able to:

1. Develop an awareness of the importance of cybersecurity in today's digital landscape.
2. Learn how to secure social media accounts, e-payments, computer and mobile data.
3. Stay updated on the latest trends and developments in the field of cybersecurity.
4. Explore the various types of cyber threats, including malware, phishing, ransomware, and social engineering.
5. Understand the motivations behind cyber-attacks and the potential impact on individuals and organizations.
6. Gain exposure to common cybersecurity tools and technologies.

Checked
Ashish
17/9/25