

F.Y.B.Com Syllabus

Computer Applications – II (SEMESTER II)

GE2: Generic Elective as per CBCS

Credits: 3(Theory)+1(Practical) Marks: 100(Theory 75 + Practical 25)
Lectures: 45, Practical Lab: 15 Sessions Batch Size: 20 Students per batch

One Theory Lecture = One Hour & One Practical Lab Session = Two Hours

Course Objectives: To understand computer networking concepts, e-commerce technology and business applications; understand principles of cyber security, online threats and cyber laws and prepare students to adopt safe practices.

Unit I Basics of Computer Networking

(Lectures: 6, Practical Lab 2 Marks Th-15, Pr-2).

Networking basics, Need for computer networks, Types of networks-LAN, MAN, WAN, Network Components – H/W, Software, Communication channels, Network Devices, Network topologies.

Lab1

Basic Networking Setup of PC, Network commands like ipconfig, ping, traceroute, nslookup / dig etc, Setup of Home Router / Wifi Hotspot, Understanding of Firewall and Basic Firewall Setup, File and Printer Sharing, connecting to share, Setup of Email Clients like Outlook, FTP Clients and Upload / Download. Finding out public address, connection speeds etc.

Unit II E-Commerce

(Lectures: 10, Practical Lab 07 Marks Th-15, Pr-15).

Definition, E-commerce and Trade Cycle, Electronic Markets, Electronic Data Interchange and Internet Commerce, Types of E-commerce :Business to Business E-Commerce, Business to Consumer E-Commerce. Consumer to Consumer, Electronic Payment Systems: Smart Cards –

Credit Cards – Wallets, Risks, E-Retail, Concept and Examples, E-Banking, Features and services, M-Commerce, Products and services

Lab2

E-commerce

- ☐ *Attempt to purchase a product online from any E-Commerce Site. Proceed till payment gateway. Check digital certificates (such as ebay.in and amazon.com)*
- ☐ *Write a review of an E-Commerce Site visited include: Site description, Site Design, ease in navigation , process for purchasing items, security, privacy, customer service, best features of site etc..*
- ☐ *An E-commerce site case study: Include*

Target market/audience: who uses this service?

Revenue model: where does the money come from?

How are they promoting their products in the marketplace? ,

Unit III Emerging threats in Cyber Space

(Lectures: 15, Practical Lab 02 Marks Th-25, Pr-2).

Introduction to cyber space, Malware threats- Definition and types (Virus/ worms, Trojan, Rootkits, Spyware, Keyloggers). Social Engineering, Cyber Crimes – Definition, Types (DOS, Intellectual Property Rights and related crimes, Unauthorized access to computer system or networks, Theft of information contained in electronic form, Cyber Stalking, Identity Theft, E-mail Spoofing, E-mail bombing, Online gambling, Sale of illegal articles, Cyber Defamation, Salami attack, Phishing, Pharming, Data Diddling, logic bombs, Web jacking, Theft of computer system, physically damaging a computer system, Cyber warfare, Cyber terrorism.)

Lab3

Installation and Configuration of any free Antivirus Package eg. AVG/Avast etc., Using Antivirus Package for Threat Detection, Browser security and Safety such as Understanding SSL and Certificates, checking URL of site for Phishing attempts, Email Headers and Tracking, Identification of Phishing Emails

Unit IV Cyber Safety, IT Act and Cyber forensic

(Lectures: 14, Practical Lab 04 Marks Th-20, Pr-6).

Online Privacy – Introduction, Significance, Privacy Policy, Sensitive Personal Information, Social media – Usage, Safety. Online shopping – Introduction, Safety measures (Encryption of data authentication, SSL, Digital signatures, Digital Certificates), Online payments – Introduction, Types, Safe practices.

Cyber Laws: Evolution and Need for cyber law, The legal perspectives – Indian perspective, Global perspective, Information Technology Act(ITA) 2000, Provisions related to E-commerce, Provisions for cyber-crimes, Information Technology (Amendment)(ITAA) Act 2008, Adjudicating officer, CERT-IN- its role and powers.

Reporting Cyber Crimes, Cyber Forensics: Introduction, Evidence collection, Data Recovery, Cloning of Devices, Forensic Investigation phases – Acquisition and preservation, Authentication, Analysis, Documenting Evidence, Presentation of Evidence, Media sanitization.

Lab4.1

Keeping passwords cyber secure-Choosing strong passwords, Privacy settings on Facebook, Social Media Safety, Payment Systems Security concerns and Safe Practices, Online Banking Security features, OpenPGP Tools.

Lab4.2

Use of Investigation tools such as Winhex for forensic investigation, Data Recovery using winhex, Use of Free data recovery tools like Recuva, Mapping a given list of cyber-crimes to appropriate ITAA Act 2008 offence listed in http://www.naavi.org/ita_2008/index

Reference Books and web references

1. Rick Lehtinen and G. T. Gangemi, *Computer Security Basics*, O'Reilly Media, Inc.; 2nd Edition, 2006
2. Wall, David, (2007). *Cyber Crime: The Transformation of Crime in the Information Age*. Polity Publishing
3. Michael cross, *Scene of the Cyber Crime*, Syngress Publishing, Elsevier Publishing, 2nd Edition, ISBN 13: 978-1-59749-276-8
4. Chander, Harish, *Cyber Laws and IT Protection*, ISBN: 978-81-203-4570-6

5. Nina Godbole, SunitBelapure, "Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiely India Pvt.Ltd., ISBN - 978-81-265-2179-1
6. *Frontiers of Electronic Commerce* Ravi Kalakota & Andrew B Whinston, Pearson Education.
7. Bruce Schneier, "Applied Cryptography-Protocols, Algorithms and Source code in C", 2nd Edition, Wiely India Pvt Ltd, ISBN 978-81-265-1368-0
8. Cyber Laws, <http://deity.gov.in/content/cyber-laws>
9. www.cert.org