

(FOR THE CANDIDATES ADMITTED

23UPA514

DURING THE ACADEMIC YEAR 2023-2024 ONLY)

REG.NO. :

N.G.M.COLLEGE (AUTONOMOUS): POLLACHI

END-OF-SEMESTER EXAMINATIONS: NOVEMBER 2025

B. Com (PA)

MAXIMUM MARKS: 75

SEMESTER- V

TIME: 3 HOURS

PART - III

INFORMATION TECHNOLOGY & E-SECURITY

SECTION – A

(10 X 1 = 10 MARKS)

ANSWER THE FOLLOWING QUESTIONS.

(K1)

1. Which of the following is not a type of E-Commerce?
a) B2B b) B2C c) G2C d) ERP
2. The main feature of E-Commerce is _____
a) Manual transaction b) Ubiquity (anywhere, anytime access)
c) Limited reach d) High paperwork
3. EDI stands for _____
a) Electronic Data Interlink b) Electronic Data Interchange
c) Electronic Digital Information d) Enterprise Data Integration
4. Which of the following is an example of token-based e-payment?
a) Debit card b) Smart card c) Mobile wallet d) Credit card
5. Phishing is related to _____
a) Sending spam mails b) Stealing personal information through fake sites/emails
c) Virus attack d) Unauthorized file download

ANSWER THE FOLLOWING IN ONE (OR) TWO SENTENCES

(K2)

6. Define E-Commerce.
7. What is Mobile Commerce?
8. List two advantages of EDI.
9. What are the three goals of information security?
10. Define Steganography.

SECTION – B

(5 X 5 = 25 MARKS)

ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS. (K3)

11. a) Describe the features of E-Commerce.

(OR)

- b) Examine the types of E-Commerce with examples.

ETHICAL PAPER

(CONTD...2)

12. a) Interpret the term Electronic Payment Systems (EPS).

(OR)

- b) List the components of EDI and explain any two.

13. a) Assess the merits and demerits of online purchases.

(OR)

- b) Describe Mobile Commerce applications.

14. a) "Transmission Media" - Interpret.

(OR)

- b) Distinguish between Spoofing and Phishing.

15. a) Examine any three types of Information Security Threats.

(OR)

- b) Sketch SQL Injection with example.

SECTION – C

(5 X 8 = 40 MARKS)

ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS. (K4OR K5)

16. a) Explain in detail the advantages and disadvantages of E-Commerce.

(OR)

- b) Discuss the business models of E-Commerce – B2B, B2C, C2B, C2C, B2E, G2B with examples.

17. a) Outline the evolution of EDI and its advantages.

(OR)

- b) Discuss the bottlenecks of EDI in detail.

18. a) Analyse the different types of Electronic Payment Systems in detail.

(OR)

- b) Discuss Mobile Commerce in detail with applications.

19. a) Describe the components of a communication system and the basics of Internet.

(OR)

- b) Point out the types of cyber attacks – Spoofing, Phishing, Impersonation, Dumpster Diving.

20. a) Write a detailed note on Authentication methods and Web Security threats.

(OR)

- b) Discuss Computer Forensics and Steganography in detail.

ANSWER KEY

PART - III

23UPA514 – Bachelor of Commerce (Professional Accounting)

SECTION – A **(10 X 1 = 10 MARKS)**

ANSWER THE FOLLOWING QUESTIONS.

(Objective Questions with four Multiple Choices) (K1)

(Qn. No. 1 - 5)

1. Answer: d) ERP
2. Answer: b) Ubiquity
3. Answer: b) Electronic Data Interchange
4. Answer: b) Smart card
5. Answer: b) Stealing personal information through fake sites/emails

ANSWER THE FOLLOWING IN ONE (OR) TWO SENTENCES (K2)

(Qn. No. 6 - 10)

6. Answer: E-Commerce refers to buying and selling of goods and services through electronic networks, primarily the Internet.
7. Answer: Mobile commerce (m-commerce) is the use of mobile devices such as smartphones and tablets to conduct commercial transactions like shopping, banking, or ticket booking.
8. Answer:
 - Faster transaction processing
 - Reduced paperwork and errors
9. Answer: Confidentiality, Integrity, and Availability (CIA).
10. Answer: Steganography is the technique of hiding secret information within another file such as an image, video, or audio, so that the hidden message is not easily detected.

SECTION – B **(5 X 5 = 25 MARKS)**

ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS.

(Qn. No. 11 to 15) Questions for Short Answers with internal choices – 2 questions from each unit. (K3)

11. a) Answer: Features include: Ubiquity, Global Reach, Interactivity, Personalization, Information richness, and Universal standards.
11. b) Answer: The main types of e-commerce are B2C (Business-to-Consumer), B2B (Business-to-Business), C2C (Consumer-to-Consumer), and C2B (Consumer-to-Business), with examples including online retailers, wholesale suppliers, peer-to-peer marketplaces, and freelancer platforms, respectively. Other models include B2G (Business-to-Government), G2B (Government-to-Business), C2G (Consumer-to-Government), and D2C (Direct-to-Consumer), which is a subset of B2C.
- 12.a) Answer: E-payment systems allow customers to pay electronically through credit cards, mobile wallets, e-cash, smart cards, and online banking.

12. b) Answer: The components of Electronic Data Interchange (EDI) include EDI Standards, EDI Software (mapping and translation), Trading Partners, Business Applications, and Communication Methods.

13.a) Answer: Merits: Convenience, global access, price comparison, variety.

Demerits: Security risks, fraud, delivery issues, no physical trial.

13. b) Answer: Mobile Commerce (M-Commerce) refers to all commercial activities, including buying, selling, and financial transactions, conducted using a wireless mobile device like a smartphone or tablet. It is a part of e-commerce and enables users to access platforms for shopping, banking, bill payment, and other services without a desktop computer, offering personalized experiences through location-based services and push notifications.

14. a) Answer: Transmission media are communication channels:

Wired: Twisted pair, coaxial, fiber optic.

Wireless: Radio waves, microwave, satellite.

14. b) Spoofing is the act of a hacker disguising themselves as a legitimate entity to appear trustworthy, while phishing is the broader tactic of tricking a victim into revealing sensitive information, often using spoofing as a method within a larger social engineering scheme. In essence, spoofing is a method of impersonation to make an attack convincing, and phishing is the act of using deception to steal data or lure victims to perform an action.

15. a) Answer: Spoofing identity – impersonating a trusted entity.

Denial of Service – overloading systems to shut down services.

Repudiation – denial of sending/receiving a message.

15. b) Answer: Some common SQL injection examples include:

Retrieving hidden data, where you can modify a SQL query to return additional results.

Subverting application logic, where you can change a query to interfere with the application's logic. UNION attacks, where you can retrieve data from different database tables.

SECTION – C

(5 X 8 = 40 MARKS)

ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS.

(Qn. No. 16 to 20 Questions for Long Answers with internal choices – 2 questions from each unit.

(K4 (Or) K5)

16. a) Answer: Advantages: Convenience, global reach, cost reduction, efficiency, personalization.

Disadvantages: Security risks, legal issues, lack of human touch, dependency on technology, delivery challenges.

16. b) Answer: E-commerce business models categorize online transactions by the type of participants involved. Key models include B2B (Business-to-Business), where companies sell to other companies, such as a manufacturer selling to a wholesaler; B2C (Business-to-Consumer), where a business sells directly to an individual, like an online clothing retailer; C2C (Consumer-to-Consumer), where individuals sell to each other, often via a platform like eBay; C2B

(Consumer-to-Business), where individuals offer services or products to businesses, like a freelancer selling services to a company; B2E (Business-to-Employee), where businesses provide services or products to their own employees through online platforms; and G2B (Government-to-Business), where government agencies offer online services to businesses, such as the GST portal for tax filing.

17. a) Answer: From manual systems → proprietary VANs → Internet-based EDI. Advantages: speed, cost efficiency, accuracy, automation.

17. b) Answer: EDI bottlenecks stem from its high implementation and maintenance costs, the complexity of setting up and integrating with existing systems, issues with data mapping and quality, and the inherent lack of flexibility in rigid standards. Further challenges include dependence on partner readiness and technical compatibility, along with the critical need for robust security and ongoing compliance management to address evolving regulations and threats.

18. a) Answer: Token-based, Credit card, Mobile payment, E-cash, E-Cheque – with features, process, advantages & limitations.

18. b) Answer: Mobile commerce (m-commerce) refers to the buying and selling of goods and services using wireless devices like smartphones and tablets, offering enhanced convenience, personalization, and secure payment options through mobile apps and websites. Key applications include mobile banking, e-bill payments, ticket bookings, in-app purchases, and social commerce, which allows direct purchasing from social media platforms. M-commerce provides businesses with a way to drive sales and loyalty by connecting with customers through personalized experiences, location-based services, and push notifications.

19. a) Answer: Components: Sender, message, medium, receiver, feedback, protocols. Basics of Internet: client-server model, domain names, IP addresses, web browsing.

19. b) Answer: Spoofing is the act of an attacker pretending to be a trusted entity by forging their identity, such as an email address or IP address, to gain trust or access. Phishing uses social engineering to trick victims into revealing sensitive information or downloading malware by impersonating legitimate sources, often employing spoofing to increase credibility.

20. a) Answer: Passwords, OTPs, biometrics, digital certificates.

Web threats: XSS, CSRF, SQL Injection.

20. b) Answer: Computer forensics is the discipline of identifying, collecting, preserving, analyzing, and presenting digital evidence from electronic devices for legal purposes, while steganography is the art of hiding data within other files or communications to conceal its existence entirely. Computer forensic experts use reverse steganography, a core technique, to uncover data hidden by steganography by analyzing file integrity and looking for anomalies, such as altered file hashes, which can reveal that data has been hidden and extracted.

.....