ANNAMACHARYA UNIVERSITY

BACHELOR OF BUSINESS ADMINISTRATION (BBA)

E-BUSINESS

Lecture Notes

UNIT 1 – FUNDAMENTALS OF E-BUSINESS

1.1 Meaning of commerce and conventional commerce

Commerce refers to activities connected with the exchange of goods and services. It includes buying, selling and the supporting activities that make exchange possible, such as transport, warehousing, banking, insurance, advertising and communication. Conventional commerce is the traditional form of commercial activity in which buyers and sellers generally interact through physical markets, shops, offices, agents and paper-based documents.

For example, a customer visiting a textile shop, selecting a shirt, paying at the counter and taking the product home is participating in conventional commerce. The transaction may use a card or UPI, but the shopping and delivery process is still largely conducted through a physical outlet.

1.2 Limitations of conventional commerce

Limitation	Explanation	Illustration
Geographical restriction	A shop mainly serves customers who can reach its location or delivery area.	A village store may not reach customers in another state.
Limited operating hours	Sales usually depend on the opening and closing time of the establishment.	A customer cannot normally purchase from a closed shop.
Higher operating cost	Rent, utilities, display space and in-person staffing add to expenses.	A retailer pays rent for a showroom.
Limited product display	Physical shelf and storage space restrict the number of products displayed.	A small shop cannot display thousands of models.
Slower information exchange	Price, stock and order information may require calls or manual records.	A buyer may need to telephone several dealers.
Paper-based administration	Manual invoices, files and registers can take time to process and store.	A paper purchase order may require physical approval.
Market reach constraints	Promotion and distribution may be limited by location and budget.	A local producer may struggle to reach distant buyers.
Difficult comparison	Customers may have to visit several sellers to compare price and features.	Comparing insurance policies physically is time-consuming.

1.3 Meaning and definition of E-Business

E-Business (electronic business) means the use of digital technologies, electronic networks and information systems to conduct, support and manage business activities. It includes online buying and selling, customer service, electronic procurement, supply-chain coordination, digital marketing, online payments, inventory management and communication with business partners.

E-Business is broader than simply selling products through a website. A manufacturer using an integrated system to receive orders, check stock, issue invoices, coordinate transport and communicate with suppliers is also using E-Business.

1.4 E-Business versus conventional commerce

Basis	Conventional commerce	E-Business
Place of activity	Physical shop, office, market or branch.	Website, mobile application, electronic platform or connected business system.
Reach	Often local or regional, depending on distribution.	Can reach customers across regions and countries, subject to law and logistics.

Time	Usually tied to business hours.	Many services and ordering facilities are available around the clock.
Communication	Face-to-face, telephone and paper correspondence.	Email, chat, apps, portals, video and automated notifications.
Records	Often paper-based or separate computer records.	Digital records and integrated databases.
Product information	Physical inspection and salesperson explanation.	Digital descriptions, images, specifications, reviews and demonstrations.
Transaction speed	May involve manual steps and physical visits.	Many steps can be automated and completed electronically.
Personal contact	Usually direct physical interaction.	Often remote; digital support can supplement human contact.
Operating cost	Physical premises and display costs can be substantial.	May reduce some physical costs but requires technology, cybersecurity and platform investment.
Trust and risk	Risks include cash handling, counterfeit goods and physical disputes.	Risks include phishing, data theft, payment fraud and non-delivery.

1.5 Origin and evolution of E-Business

E-Business developed gradually as communication and computing technologies improved. It did not begin only with online shopping. Businesses first used electronic systems to exchange structured documents and automate internal records; later, the internet and mobile technologies made digital transactions accessible to a much wider public.

Mainframe computers and computerised business records
↓
Electronic Data Interchange (EDI) and electronic funds transfer
↓
Personal computers and business software
↓
Commercial internet, websites and email
↓
Online shopping, electronic marketplaces and digital payment gateways
↓
Smartphones, mobile commerce, cloud services and social commerce
↓
AI-enabled personalisation, automation and connected digital ecosystems

Major stages in the evolution

Stage	Development	Business significance
Computerisation	Use of computers for accounts, payroll, stock and records.	Improved accuracy, storage and processing.
Electronic exchange	EDI and electronic fund transfer between organisations and banks.	Reduced paper documents and repetitive data entry.
Internet adoption	Websites, email and online catalogues.	Expanded communication and market visibility.

E-commerce growth	Online storefronts, carts, order tracking and payment gateways.	Enabled remote ordering and digital retail.
Mobile phase	Smartphones, apps, mobile wallets and QR payments.	Made transactions possible through portable devices.
Integrated digital business	Cloud platforms, analytics, APIs and automation.	Connected customers, suppliers, employees and operations.

1.6 Nature and characteristics of E-Business

- Electronic connectivity: business participants communicate through networks and digital platforms.
- Information intensive: product details, orders, customer records and payments are represented as digital information.
- Interactivity: customers can search, enquire, compare, review and communicate with sellers.
- Automation: routine activities such as order acknowledgement, invoice generation and stock updates can be automated.
- Global and extended reach: digital channels can connect a business with customers beyond its immediate locality.
- Speed and convenience: information and transaction instructions can be exchanged quickly.
- Integration: sales, finance, inventory, logistics and customer relationship systems may share information.
- Measurability: digital activity can generate data about visits, enquiries, conversion and service performance.
- Dependence on technology: devices, software, connectivity, electricity and cybersecurity are important.
- Continuous availability: online systems can support transactions outside conventional business hours, although maintenance and outages may occur.

1.7 Goals and need for E-Business

The main goal of E-Business is to use electronic technology to improve the way an organisation creates value, serves customers and coordinates its operations. It is adopted not merely to have an online presence but to make business processes more responsive, accessible and efficient.

Goal	How E-Business supports it
Customer convenience	Allows product search, enquiries, ordering and service requests through digital channels.
Wider market access	Connects firms with customers and suppliers beyond a physical market area.
Operational efficiency	Reduces repetitive manual work and improves information flow.
Cost management	Can reduce paper, travel and some physical distribution or administrative costs.
Better decisions	Provides sales, inventory and customer data for analysis.
Improved coordination	Connects departments, suppliers, distributors and customers.
Competitive strength	Enables faster service, digital promotion and new business offerings.
Business continuity	Provides alternative channels when physical operations are disrupted.

1.8 Essentials of E-Business

An E-Business system requires a combination of technology, people, processes and controls. A website alone is not sufficient if the organisation cannot manage orders, payment, delivery, customer support and data security.

Essential	Role in E-Business
Digital infrastructure	Computers, servers, mobile devices, networks and reliable connectivity.
Website or application	Customer-facing or partner-facing interface for information and transactions.
Software and databases	Manage product catalogues, customer details, orders, accounts and inventory.
Payment facility	Supports collection and reconciliation of electronic payments.
Security controls	Protect accounts, systems, transactions and confidential information.
Logistics and fulfilment	Handle packing, shipping, delivery, returns and tracking where physical goods are sold.
Customer support	Responds to complaints, enquiries, refunds and service requests.
Human resources	Employees with digital, operational and customer-service skills.
Policies and legal compliance	Set rules for privacy, consumer protection, contracts, records and payments.

1.9 Levels of E-Business

The syllabus refers to levels of E-Business. For teaching purposes, these can be understood as increasing degrees of digital integration within an organisation.

Level	Description	Example
Level 1 – Online presence	The business publishes information electronically but may not accept online orders.	A company website showing address, products and contact details.
Level 2 – Interaction	Customers can enquire, submit forms or communicate online.	A service request form or online quotation enquiry.
Level 3 – Transaction	Customers can place orders and complete payment electronically.	An online store with cart and payment facility.
Level 4 – Integration	Online transactions connect with internal systems such as inventory, accounts and logistics.	An order automatically updates stock and triggers dispatch.
Level 5 – Extended digital ecosystem	The firm coordinates customers, suppliers, service providers and partners through connected platforms.	An integrated marketplace and supply-chain portal.

1.10 Procedure of an E-Business transaction

A typical online purchase involves a sequence of activities. The exact steps differ across businesses, but the following flow represents a common transaction.

Customer visits website / mobile application
↓
Searches product or service and checks details
↓
Selects item and adds it to cart
↓
Provides delivery and contact information

↓
Chooses payment method and authorises payment
↓
System confirms order and records transaction
↓
Seller processes, packs or activates the order
↓
Goods / service delivered; customer receives updates
↓
After-sales support, feedback, return or refund if applicable

1.11 Parties to E-Business transactions

Party	Role	Example
Buyer / customer	Initiates enquiry, places order and pays.	Individual purchasing a book online.
Seller / merchant	Lists goods or services and fulfils the order.	Retailer operating an online store.
Platform / marketplace	Connects buyers and sellers and may provide listing, payment or dispute facilities.	An online marketplace.
Payment service provider	Facilitates electronic payment authorisation and settlement.	Payment gateway or acquiring service.
Bank / financial institution	Maintains accounts and supports payment processing.	Customer's issuing bank.
Logistics provider	Stores, transports and delivers physical products.	Courier company.
Government / regulator	Creates and enforces applicable rules and standards.	Tax or consumer-protection authority.
Technology / security provider	Provides hosting, software, authentication and security services.	Cloud or cybersecurity service provider.

1.12 Advantages and limitations – a balanced view

E-Business can improve convenience, speed, reach and information access. However, its benefits depend on reliable technology, customer trust, secure systems, effective delivery and appropriate management. A digital business may still face high customer-acquisition costs, cyberattacks, platform dependence and return-management challenges.

UNIT 2 – E-BUSINESS

2.1 Advantages of E-Business

Advantage	Explanation	Example
Convenience	Customers can access information and place orders remotely.	Ordering groceries through an app.
Wider reach	A firm can communicate with customers in multiple locations.	A local handicraft seller listing products nationally.
Time saving	Search, ordering and routine communication can be completed quickly.	An online ticket booking.
Lower transaction effort	Automated forms and digital records reduce repetitive manual work.	Electronic purchase order processing.
Customer information	Digital systems help understand customer preferences and buying patterns.	Product recommendations based on browsing or purchase history.
Faster communication	Order updates, email and messaging support quick interaction.	SMS or app notification after dispatch.
Product variety	Online catalogues can display a wider range than a small physical outlet.	A marketplace listing products from many sellers.
Business flexibility	Digital channels can support new services and operating models.	Subscription-based delivery service.
Improved coordination	Suppliers, sales and inventory teams can share information.	A stock update triggers replenishment.

2.2 Disadvantages and challenges of E-Business

Disadvantage / challenge	Explanation	Possible response
Cybersecurity risk	Accounts, payments and customer information may be targeted.	Use strong authentication, updates, monitoring and staff training.
Privacy concerns	Personal data may be collected or misused.	Collect only necessary data and apply clear privacy controls.
Technology dependence	Internet, electricity or platform failure can interrupt operations.	Maintain backups, continuity plans and support channels.
Lack of physical inspection	Customers may not examine a product before purchase.	Provide accurate images, specifications and return policies.
Delivery and returns	Physical products require packaging, shipping and reverse logistics.	Use reliable logistics and transparent tracking.
Intense competition	Customers can compare many sellers quickly.	Differentiate through quality, service and trust.
Digital divide	Some customers lack devices, connectivity or digital skills.	Offer accessible design and assisted/offline options.
Fraud and fake listings	Fraudulent sellers or misleading offers can damage trust.	Verify sellers, monitor listings and provide dispute processes.
Initial investment	Platforms, software, cybersecurity and skilled staff require spending.	Plan investment according to business size and risk.

2.3 Mobile Commerce (M-Commerce)

Mobile Commerce, commonly called M-Commerce, refers to commercial activities carried out through wireless handheld devices, especially smartphones and tablets. It is an important part of E-Business

because mobile devices allow users to search, communicate, purchase, pay and receive services while away from a fixed computer.

Features of M-Commerce

- Portability: a mobile device can be carried by the user.
- Wireless access: transactions can be conducted through mobile data or Wi-Fi.
- Location awareness: with permission, services may use location information.
- Personalisation: applications can present content based on user preferences.
- Instant notifications: users receive alerts about orders, payments and offers.
- Mobile authentication: PINs, biometrics and one-time passwords may be used.
- App-based interaction: businesses can provide dedicated applications or mobile-friendly websites.

Applications of M-Commerce

Application	Description
Mobile banking	Checking balances, transferring funds, paying bills and managing accounts through a bank app.
Mobile shopping	Searching, ordering and tracking products through a shopping application.
Mobile payments	Paying through UPI apps, wallets, QR codes or contactless facilities where supported.
Ticket booking	Booking travel, cinema and event tickets through mobile platforms.
Food and grocery delivery	Ordering food or household items and tracking delivery.
Location-based services	Finding nearby outlets, offers or service providers, subject to user permission.
Mobile financial services	Accessing investment, insurance and other financial service information through apps.

M-Commerce transaction flow

Open a mobile app or mobile-friendly website
↓
Authenticate or create an account
↓
Search / select product or service
↓
Enter required order details
↓
Choose mobile payment method
↓
Approve payment securely
↓
Receive confirmation and transaction reference
↓
Track delivery or access the digital service

Benefits and limitations of M-Commerce

Benefits	Limitations
Access from almost any location with connectivity.	Small screen may make complex tasks difficult.
Quick notifications and payment approval.	Loss or theft of a device can create account risk.
Convenient app-based experience.	Poor network may interrupt a transaction.
Supports location-based and personalised services.	Privacy and location-data concerns may arise.
Can serve customers who do not use desktop computers.	Apps require updates and compatible devices.

2.4 E-Business and E-Commerce

E-Commerce (electronic commerce) generally refers to electronic buying and selling of goods and services and the related online transactions. E-Business is a wider concept that includes E-Commerce as well as internal and external business processes supported by digital technology. Thus, every online sale is an E-Commerce activity and can be part of E-Business, but every E-Business activity is not necessarily an online sale.

Basis	E-Commerce	E-Business
Scope	Relatively focused on electronic commercial transactions.	Broader; includes transactions and supporting business processes.
Main focus	Buying, selling, ordering and payment.	Overall digital operation and coordination of business.
Activities	Online catalogue, cart, checkout and order processing.	E-Commerce plus procurement, HR systems, CRM, supply chain and internal collaboration.
Participants	Usually buyers, sellers and transaction intermediaries.	Customers, employees, suppliers, partners, managers and public agencies.
Example	A customer purchases a phone online.	The seller integrates online sales with inventory, accounting, supplier ordering and customer support.

2.5 E-Markets and E-Business

An electronic market or E-Market is a digital environment in which buyers and sellers exchange information and conduct commercial transactions. It may be operated by a marketplace, industry consortium, company or public procurement platform. E-Markets are one important component of E-Business.

Functions of E-Markets

- Product and service listing: sellers publish descriptions, prices and availability.
- Search and comparison: buyers compare products, sellers and terms.
- Matching: platforms connect buyers with suitable sellers.
- Negotiation: some platforms support quotation requests, bidding or price negotiation.
- Transaction support: ordering, payment and order confirmation may be integrated.
- Trust mechanisms: ratings, reviews, seller verification and dispute processes may be provided.
- Market information: participants can observe demand, price movements and product trends.

Types of E-Markets

Type	Meaning	Illustration
Independent marketplace	A third-party platform connects many buyers and sellers.	A general online shopping marketplace.
Buyer-oriented marketplace	A large buyer creates a platform for suppliers to respond to purchasing requirements.	An organisation's electronic procurement portal.

Seller-oriented marketplace	A seller or group of sellers provides a digital channel for buyers.	A manufacturer's online dealer portal.
Industry / vertical marketplace	Focuses on a particular industry or product category.	A platform for industrial components.
Horizontal marketplace	Offers products or services across multiple industries.	A broad business-to-business trading portal.

2.6 E-Business and the Internet

The internet is a global network of interconnected computer networks. It provides the communication infrastructure through which websites, email, cloud applications, online marketplaces and many E-Business services operate. The World Wide Web is a service that uses the internet to access linked pages and applications through browsers.

Internet technologies used in E-Business

Technology	Business use
Websites and browsers	Present product information, customer portals and online stores.
Email	Send quotations, invoices, order confirmations and customer communication.
Search engines	Help users discover products, services and business information.
Cloud computing	Provides online software, storage and computing resources.
Databases	Store product, customer, supplier, order and payment-related records.
APIs	Allow separate systems to exchange data and services.
Encryption and secure protocols	Help protect information transmitted between devices and services.
Analytics	Measure website activity, sales performance and customer behaviour.

Advantages and risks of internet-based business

Internet connectivity makes digital business scalable and accessible, but it also exposes organisations to online threats. A business must consider availability, confidentiality, integrity, authentication and privacy. It should also design websites for usability and accessibility, maintain backups and provide alternative support when online systems are unavailable.

UNIT 3 – BUSINESS MODELS FOR E-BUSINESS

3.1 Meaning of a business model

A business model is a description of the logic through which an organisation creates, delivers and captures value. It explains the target customer, value proposition, resources, activities, partners, channels, costs and revenue sources. In E-Business, digital technologies and networks are central to one or more of these elements.

3.2 Meaning and importance of E-Business models

An E-Business model explains how a business uses electronic networks and digital systems to conduct transactions, provide services and generate value. A clear model helps the organisation identify customers, select technology, plan revenue, manage operating costs and distinguish itself from competitors.

- Clarifies the target market and customer needs.
- Identifies the value offered through digital channels.
- Shows how products, services or information reach customers.
- Identifies revenue sources such as sales, subscriptions, commission or advertising.
- Helps estimate technology, marketing, fulfilment and security costs.
- Supports strategic planning and performance evaluation.
- Makes it easier to compare alternative ways of operating digitally.

3.3 Models based on the nature of transacting parties

These models classify E-Business according to the parties that interact. The letters identify the participants: B = Business, C = Consumer/Citizen, and G = Government.

Model	Meaning	Example	Key feature
B2B – Business to Business	A business sells or provides products/services to another business.	A wholesaler supplies goods to a retailer through an online portal.	Bulk orders, negotiated prices and repeat relationships.
B2C – Business to Consumer	A business sells directly to an individual consumer.	A customer buys a book from an online retailer.	Product catalogue, cart, payment and delivery.
B2G – Business to Government	A business supplies goods or services to a government department or agency.	A company submits an electronic tender to supply computers.	Formal procurement rules, tendering and compliance.
C2C – Consumer to Consumer	Individuals transact with other individuals through a platform or directly.	A person sells a used bicycle through an online classified platform.	Peer listings, trust and platform mediation.
C2G – Citizen to Government	An individual uses a digital channel to make a payment, submit information or request a public service.	A citizen pays a municipal fee online.	Digital access to public services and payments.
G2G – Government to Government	Government departments or agencies exchange information and services electronically.	Two departments exchange records through a secure government system.	Inter-agency coordination and information sharing.

B2B model

In B2B transactions, both the buyer and seller are business organisations. Transactions may involve raw materials, components, machinery, software, professional services or wholesale goods. The buying

process often includes product specifications, quotations, purchase orders, credit terms, delivery schedules and repeat contracts.

- Advantages: efficient procurement, wider supplier choice, better record keeping and improved coordination.
- Challenges: complex approval processes, integration with enterprise systems, negotiation and data confidentiality.
- Common processes: supplier registration, request for quotation, quotation comparison, purchase order, invoice and payment.

B2C model

In B2C, a business offers goods or services to final consumers. The customer usually searches a catalogue, compares products, places an order, pays and receives the product or digital service. The business must focus on usability, clear product information, delivery, customer service and returns.

- Advantages: broad reach, convenience, product variety and personalised promotion.
- Challenges: competition, customer acquisition cost, returns, delivery issues and online trust.
- Examples include online retail, food ordering, travel booking and digital subscriptions.

B2G model

B2G refers to business transactions with government organisations. Businesses may supply office equipment, construction services, software, consultancy or maintenance. Digital tendering and procurement portals can improve transparency and document management, but suppliers must follow eligibility, technical and financial conditions.

C2C model

C2C platforms enable individuals to sell, exchange or offer services to other individuals. The platform may provide listing, search, communication, payment support, ratings or dispute resolution. The quality of the transaction depends heavily on accurate descriptions, seller credibility and safe payment and delivery practices.

C2G and G2G models

C2G services make it easier for citizens to interact with public authorities through digital applications, portals and payment systems. G2G systems support coordination among government departments, such as secure information exchange, shared databases and administrative workflows. Both models can reduce paperwork and improve service delivery when systems are accessible and reliable.

3.4 Models based on the nature of transactions

The syllabus lists four transaction-oriented models: Manufacture Model, Advertising Model, Value Chain Model and Brokerage Model. These describe the way a digital business organises its activities and creates value.

A. Manufacture Model

In the Manufacture Model, a producer creates goods or services and makes them available to customers through digital channels. The internet may be used for product configuration, direct ordering, customer feedback, production planning and after-sales service. A manufacturer may sell directly to customers or use distributors.

- Value created: the product itself, customisation, quality and direct access to the producer.
- Revenue: sale of manufactured products, customised orders or related services.
- Benefits: direct customer feedback, better demand information and fewer communication layers.
- Challenges: production capacity, inventory, delivery, returns and service support.

Illustration: A furniture manufacturer displays designs online. A customer selects dimensions and finish, submits an order, pays an advance and receives delivery after production.

B. Advertising Model

In the Advertising Model, a digital platform provides content, information or services to attract an audience and earns revenue by displaying advertisements or promotional messages. Advertisers pay to reach users who may be interested in their products.

- Value created: audience access, useful content, search, entertainment or community services.
- Revenue: display advertising, sponsored listings, promoted content or campaign fees.
- Important factors: audience size, relevance, engagement, trust and measurement.
- Risks: intrusive advertisements, misleading promotions, privacy concerns and dependence on advertising income.

Illustration: A news website publishes articles without charging readers for every article and earns income from advertisements displayed on its pages.

C. Value Chain Model

A value chain is the sequence of activities through which an organisation creates and delivers value. In an E-Business Value Chain Model, digital technology improves the coordination and performance of activities such as procurement, operations, marketing, sales, delivery and after-sales service.

Supplier coordination and procurement
↓
Inbound logistics and receipt of materials
↓
Operations / production / service creation
↓
Digital marketing and sales
↓
Order processing and outbound delivery
↓
Customer service and after-sales support

The model helps identify where digital systems can reduce delay, improve quality, share information or lower cost. For example, a retailer can connect supplier stock information with its own inventory system and online store.

D. Brokerage Model

A broker or intermediary connects buyers and sellers and helps them find each other or complete a transaction. The broker may provide search, comparison, listing, negotiation, payment support or trust mechanisms. The broker generally earns a commission, listing fee, subscription or service charge.

- Value created: reducing search effort and connecting market participants.
- Revenue: commission per transaction, listing fees, subscription or premium services.
- Examples: travel booking intermediaries, property portals and online marketplaces.
- Challenges: maintaining trust, preventing fake listings, handling disputes and balancing the interests of both sides.

3.5 Comparison of the four transaction models

Model	Core activity	Typical revenue / value capture	Illustration
Manufacture	Produce and sell goods or configured services.	Product sales and related service revenue.	Manufacturer's direct online store.
Advertising	Attract an audience and sell advertising access.	Advertising and sponsored placement fees.	Content or search platform.
Value Chain	Coordinate activities from sourcing to service.	Margin and efficiency across the chain.	Integrated retailer-manufacturer-distributor system.
Brokerage	Connect buyers and sellers.	Commission, listing or subscription fees.	Online travel or property intermediary.

3.6 Selecting an appropriate E-Business model

A business should select its model after studying customer needs, product characteristics, competition, resources, legal requirements and the cost of technology. A model suitable for a digital information service may not suit a business selling heavy physical equipment.

Decision factor	Question to consider
Customer	Who uses the product or service – business, consumer or government?
Value proposition	What problem does the digital offering solve?
Revenue	Who pays, how much and for what?
Cost structure	What are the costs of technology, staff, marketing, delivery and security?
Partners	Are suppliers, payment providers, logistics firms or platforms required?
Trust	How will identity, quality, payment and disputes be handled?
Scalability	Can the model serve more customers without costs increasing at the same rate?

UNIT 4 – E-PAYMENT SYSTEM

4.1 Meaning of an E-Payment System

An electronic payment system is a method through which payment information and payment instructions are transmitted and processed electronically. It allows customers, merchants, banks and payment service providers to complete or support payment transactions without relying entirely on physical cash or paper instruments.

4.2 Traditional payment system compared with modern payment system

Basis	Traditional payment methods	Modern / electronic payment methods
Form	Cash, paper cheque, demand draft and physical payment instrument.	Card, internet banking, mobile payment, e-cheque and electronic money arrangements.
Initiation	Often requires physical handover or visit to a bank or merchant.	Can be initiated through a website, app, card terminal or other electronic interface.
Processing	May involve manual handling, physical clearing and transport.	Uses electronic communication and payment-processing systems.
Speed	May take time depending on instrument and clearing process.	Many methods provide rapid authorisation; settlement timing varies.
Records	Paper receipts and bank records.	Electronic confirmations, statements and transaction references.
Convenience	Useful where digital access is limited.	Convenient for remote and cashless transactions.
Risk	Cash loss, counterfeit notes, cheque fraud or physical theft.	Phishing, card-not-present fraud, account compromise and data theft.
Accessibility	Can be used without internet or smartphone in many cases.	May require a device, network, bank account or supported payment service.

4.3 PC Banking

PC Banking refers to banking services accessed through a personal computer. A customer uses a bank's authorised internet banking website or computer-based banking facility to view account information and perform permitted transactions. Modern services may also be accessed through mobile devices, but the syllabus specifically mentions PC Banking.

Services available through PC Banking

- Balance enquiry and account statement viewing.
- Transfer of funds between eligible accounts.
- Payment of utility bills and other permitted dues.
- Viewing cheque status and transaction history.
- Requesting selected banking services or account documents.
- Managing beneficiaries and selected account preferences, subject to bank controls.

Basic PC Banking procedure

Open the bank's genuine official website
↓
Check the website address and secure connection

↓
Enter customer ID and authentication details
↓
Complete additional verification if requested
↓
Select the required banking service
↓
Review beneficiary, amount and transaction details
↓
Confirm the transaction using the bank's authorised method
↓
Save the reference number and log out

Safety note: Never share passwords, PINs, OTPs or confidential authentication codes with callers or through links received in unsolicited messages. Access banking only through official channels.

4.4 Credit Cards

A credit card is a payment card that allows an eligible cardholder to make purchases using a credit facility provided by the card issuer. The issuer pays or arranges payment to the merchant, and the cardholder must repay the amount according to the billing terms. Interest, fees and charges may apply when the outstanding amount is not paid as required.

Credit card transaction process

Customer presents card or enters card details through a permitted checkout
↓
Merchant sends transaction request to payment processor / acquiring side
↓
Card network routes request to issuer for authorisation
↓
Issuer checks account status, available credit and risk signals
↓
Approval or decline response returns to merchant
↓
Transaction is captured and later settled through the payment system
↓
Cardholder receives statement and repays issuer

Advantages and limitations of credit cards

Advantages	Limitations / risks
Convenient for online and physical purchases.	Overspending may lead to debt.
May provide a short interest-free period when terms are met.	Interest and fees may be high on unpaid balances.
Useful for emergencies and travel when managed responsibly.	Stolen details or account compromise can cause fraud.

May provide transaction records and dispute mechanisms.	Eligibility and credit limits depend on issuer assessment.

4.5 Debit Cards

A debit card is linked to a bank account. When the cardholder makes a purchase or cash withdrawal, the amount is generally deducted from the available account balance, subject to bank rules and transaction limits. Unlike a credit card, it normally does not provide a revolving credit facility.

Credit card	Debit card
Payment is made using a credit facility.	Payment is made from available funds in a linked account.
Cardholder repays the issuer as per the statement.	Amount is normally debited from the account.
Interest may apply to unpaid balances.	No credit-card interest on an ordinary purchase because it uses the account balance; other bank charges may still apply.
Can help build a credit history when used responsibly.	Use does not normally create a credit balance.

4.6 Smart Cards

A smart card is a plastic or other form-factor card containing an embedded integrated circuit chip. The chip can store data and may perform processing or cryptographic functions. Smart cards can be contact-based, where the card is inserted into a reader, or contactless, where it communicates over a short distance.

- Applications: payment cards, identity systems, access control, transport and healthcare administration.
- Features: chip-based storage, authentication capability and controlled data access.
- Benefits: can support stronger security than simple magnetic-stripe storage when properly designed and managed.
- Limitations: requires compatible readers and secure card issuance, personalisation and lifecycle management.

4.7 E-Cheques / Internet Cheques

An e-cheque or internet cheque is an electronic form of a cheque-based payment instruction. It represents a payer's instruction to transfer funds to a payee through an electronic process. The exact format and legal recognition depend on the applicable banking arrangement and law. It should not be confused with simply scanning a paper cheque and emailing the image.

General e-cheque process

Payer prepares an electronic payment instruction
↓
Payer authenticates and applies the required electronic authorisation
↓
Instruction is transmitted through the authorised channel
↓
Bank or service provider validates the instruction
↓
Funds and account details are checked
↓
Payment is processed, cleared or rejected
↓

Payer and payee receive transaction status

4.8 Micro-payments

Micro-payments are very small-value payments made electronically. They are useful when the price of an individual digital item or service is low. Examples may include a small digital content purchase, a low-value service charge or a small in-app transaction. The payment provider's minimum value, charges and rules determine whether a micro-payment is commercially practical.

- Suitable for low-priced digital content or services.
- Can support pay-per-use business models.
- May be aggregated into a periodic bill to reduce processing overhead.
- Must balance transaction convenience, processing fees, fraud controls and user consent.

4.9 E-Cash

E-Cash is a broad term used for electronic representations of monetary value used to make payments. In some systems, value is stored in an account or wallet; in others, a prepaid instrument represents value. The term should be understood according to the particular system being discussed. It is not automatically the same as cryptocurrency.

Feature	Explanation
Digital value	Value is represented and managed electronically.
Convenience	Can support remote or quick payment, depending on the system.
Storage	May be account-based, wallet-based or stored-value based.
Acceptance	Depends on participating merchants and service providers.
Security	Requires authentication, access control and protection against unauthorised use.
Regulation	Applicable regulatory treatment depends on the type of instrument and jurisdiction.

4.10 Digital Signature

A digital signature is a cryptographic technique used to help establish the authenticity and integrity of an electronic record and to provide evidence that the record was signed using the corresponding private key. It is based on public-key cryptography. A digital signature is not simply a scanned handwritten signature pasted into a document.

How digital signature technology works

Signer prepares the electronic document
↓
Software calculates a hash (digital fingerprint) of the document
↓
Signer uses the private key to sign the hash
↓
The digital signature is attached to or associated with the document
↓
Recipient obtains the signer's public key / digital certificate

↓
Recipient verifies the signature against the document hash
↓
A successful verification supports integrity and signer authentication

Important concepts in digital signatures

Concept	Meaning
Hash function	Creates a fixed-length digest from the electronic document; a changed document normally produces a different digest.
Private key	Secret key controlled by the signer and used to create the digital signature.
Public key	Corresponding key used to verify a signature.
Digital certificate	Electronic credential that links an identity to a public key, issued by a trusted certifying authority under the relevant framework.
Authentication	Helps establish that the signature was created using the private key associated with the certificate.
Integrity	Helps detect whether the signed content has been altered after signing.
Non-repudiation support	Can provide evidence relevant to disputes, subject to key control, identity verification and legal rules.

4.11 Legal position of digital signatures in India

The Information Technology Act, 2000 provides the principal statutory framework for electronic records and electronic authentication in India. The Act recognises electronic records and provides for legal recognition of electronic signatures in accordance with its provisions. Digital signatures based on asymmetric cryptosystems and hash functions are specifically addressed in the statutory framework. The exact legal effect of a signature depends on compliance with applicable provisions, rules, certificate requirements and the nature of the document or transaction.

For academic purposes, students should remember that legal recognition does not mean every document or every type of transaction can automatically be completed through any electronic signature. Certain documents and transactions may be excluded or governed by special requirements. The current Act, rules and official government guidance should be consulted for legal advice or operational decisions.

4.12 Procedure and working of digital signature technology

1. The signer obtains an appropriate digital signature certificate from a recognised certifying authority through the prescribed identity-verification process.
2. The signer securely controls the private key, often using a secure cryptographic device or approved signing application.
3. The electronic document is finalised and a hash value is generated.
4. The signing application uses the private key to create the digital signature for the hash.
5. The signed document and signature are sent to the recipient.
6. The recipient's software validates the certificate and uses the public key to verify the signature.
7. The software checks whether the document content has changed and reports the verification result.
8. The recipient retains the signed electronic record and verification information as required.

4.13 Comparison of listed payment methods

Method	Source of funds / basis	Typical use
PC Banking	Bank account accessed through a	Transfers, bill payment and account

	computer and bank service.	management.
Credit card	Credit facility provided by issuer.	Purchases and online checkout.
Debit card	Available balance in linked account.	Purchases and cash withdrawal.
Smart card	Chip-based data / payment credentials.	Payments, access and identification.
E-cheque	Electronic cheque-like payment instruction.	Electronic transfer under supported arrangement.
Micro-payment	Very small-value electronic payment.	Low-priced digital services.
E-cash	Electronic stored or account-based monetary value.	Digital payments within an accepted system.

UNIT 5 – E-SECURITY

5.1 Meaning of E-Security

E-Security refers to the policies, technologies, procedures and practices used to protect electronic information, computer systems, networks, applications and digital transactions from unauthorised access, misuse, alteration, disruption or destruction. In E-Business, security protects customer confidence, business continuity, financial resources and confidential information.

5.2 Objectives of E-Business security

Objective	Meaning	Example
Confidentiality	Information is accessible only to authorised persons.	Encrypting customer payment information.
Integrity	Information remains accurate and is not changed without authorisation.	Using hashes and access controls to detect unauthorised alteration.
Availability	Systems and information are available when needed.	Backups, redundancy and protection against denial-of-service attacks.
Authentication	Verifies the identity of a user, device or service.	Password plus one-time verification or security key.
Authorisation	Determines what an authenticated user is allowed to do.	A sales employee can view orders but cannot change payroll.
Accountability	Actions can be traced to responsible accounts or processes.	Audit logs record administrative changes.
Non-repudiation support	Provides evidence about an action or transaction.	A valid digital signature and reliable audit trail.

5.3 Cyber Crimes

Cybercrime refers to unlawful activity in which computers, networks, digital devices or electronic data are the target, tool or environment of the offence. Cybercrime can affect individuals, businesses, banks and government organisations.

Major types of cybercrime

Cybercrime	Meaning	E-Business impact
Phishing	Fraudulent messages or websites trick users into revealing credentials or sensitive information.	Account takeover, payment fraud and customer data loss.
Identity theft	Unauthorised use of another person's identity information.	Fraudulent accounts, orders or financial activity.
Malware	Malicious software designed to damage, spy on or control systems.	Data theft, disruption and unauthorised access.
Ransomware	Malware that blocks access to data or	Business interruption and possible data

	systems and demands payment.	exposure.
Hacking / unauthorised access	Accessing a system or account without permission.	Theft, alteration or misuse of business information.
Denial-of-Service (DoS / DDoS)	Flooding a service with traffic so legitimate users cannot access it.	Website or payment service outage.
Card and payment fraud	Unauthorised use of card or payment credentials.	Financial loss, chargebacks and loss of trust.
Spoofing	Faking an email address, website, caller identity or network source.	Users may trust a fake communication or destination.
Data breach	Unauthorised access to or disclosure of protected information.	Privacy harm, legal exposure and reputational damage.
Social engineering	Manipulating people into revealing information or performing unsafe actions.	Employees may disclose passwords or approve fraudulent requests.
Website defacement	Unauthorised modification of a website's appearance or content.	Reputation damage and misinformation.
Insider threat	A person with legitimate access misuses it intentionally or accidentally.	Leakage, fraud or disruption.

5.4 Common methods used by cybercriminals

- Sending fake bank, courier or marketplace messages containing malicious links.
- Creating imitation login pages to collect passwords and one-time codes.
- Exploiting outdated software or weak configurations.
- Using infected attachments or downloads to install malware.
- Guessing weak or reused passwords.
- Misusing stolen session cookies or credentials.
- Manipulating employees through urgent calls or messages.
- Abusing excessive user permissions or poorly protected databases.

5.5 E-Business Security Solutions

Security requires multiple layers. No single product can eliminate every risk. An organisation should identify important assets, assess threats, apply preventive controls, detect suspicious activity, respond to incidents and recover services.

Security solution	Purpose / application
Strong authentication	Uses robust passwords and additional factors to reduce account compromise.
Access control	Gives users only the permissions needed for their work.
Encryption	Protects information at rest and in transit from unauthorised reading.
Firewall	Controls network traffic according to defined security rules.
Anti-malware / endpoint protection	Detects or blocks malicious software on devices and servers.
Secure software development	Reduces coding weaknesses through review, testing and secure design.
Patch management	Updates operating systems and applications to address known vulnerabilities.
Backup and recovery	Allows restoration of data and services after failure or attack.
Intrusion detection / prevention	Monitors systems and network activity for suspicious patterns.
Security monitoring and logs	Supports investigation and early detection of unusual activity.
Employee awareness	Teaches staff to recognise phishing, social engineering and unsafe practices.
Incident response plan	Defines roles and steps for containment, communication and recovery.

Vendor and cloud security review	Assesses risks created by third-party services and integrations.

5.6 Basic security process for an online business

Identify information assets and business-critical services
↓
Assess threats, vulnerabilities and business impact
↓
Select preventive controls and assign responsibilities
↓
Monitor systems, transactions and user activity
↓
Detect and report suspicious events
↓
Contain and investigate the incident
↓
Restore services and recover data safely
↓
Review lessons and improve controls

5.7 E-Locking Techniques

The syllabus uses the term “e-locking techniques”. In these notes, e-locking is explained as electronic methods used to restrict access to devices, systems, information or digital transactions to authorised users. The term can cover several access-control and encryption techniques; the exact meaning may vary by textbook or institutional teaching reference.

Technique	How it works	Example
Password / PIN lock	Requires a secret code before access is granted.	Login password or ATM PIN.
Multi-factor authentication	Requires two or more different types of proof.	Password plus authenticator approval.
Biometric lock	Uses a physical or behavioural characteristic for verification.	Fingerprint or face authentication on a device.
Smart-card / token lock	Requires a physical token or card, sometimes with a PIN.	Employee access card.
Encryption-based locking	Data is unreadable without the correct cryptographic key.	Encrypted files or storage.
Role-based access control	Access is assigned according to job role.	Only authorised finance staff can approve refunds.
Session lock / timeout	Automatically locks a session after inactivity.	Banking website logs out after inactivity.
Digital certificate-based access	Uses a trusted certificate to authenticate a user or device.	Certificate-based access to a business portal.

5.8 E-Locking Products

E-locking products are physical or software-based tools that implement electronic access restriction or protection. Product examples should be understood by function rather than as an endorsement of a particular brand.

Product category	Purpose	Example
Electronic door lock	Controls physical entry using electronic credentials.	PIN or card-based office door lock.
Biometric access device	Verifies a fingerprint or other biometric characteristic.	Fingerprint attendance/access terminal.
Hardware security token	Stores or generates authentication credentials.	Security key or one-time-code token.
Smart card and reader	Provides card-based identity or access verification.	Employee smart-card access system.
Encryption software	Protects stored or transmitted information.	File or disk encryption tool.
Endpoint security product	Protects computers and mobile devices.	Anti-malware and endpoint detection software.
Firewall appliance / software	Filters network connections.	Network firewall.

5.9 E-Locking Services

E-locking services are externally provided or centrally managed facilities that help an organisation enforce electronic access controls. They may include identity management, authentication, certificate management, cloud access control, managed security monitoring and secure key management.

- Identity and Access Management (IAM): creates, manages and removes user identities and permissions.
- Multi-factor authentication service: verifies users using more than one factor.
- Certificate management: issues, renews and revokes digital certificates.
- Managed security service: monitors systems and alerts the organisation to suspicious events.
- Cloud access security: applies policies to users accessing cloud applications and data.
- Key management service: protects cryptographic keys and controls their use.
- Secure backup service: maintains protected copies of important business information.

5.10 Netscape Security Solutions

The supplied syllabus specifically lists “Net-scape Security Solutions”. This appears to refer to Netscape-related web security technologies, particularly the historical role of Netscape in the development and use of Secure Sockets Layer (SSL) for protecting communication between a browser and a web server. SSL is a historical protocol family; modern websites use Transport Layer Security (TLS), the successor to SSL. SSL versions are obsolete and should not be used for current security deployments.

SSL / TLS – basic purpose

SSL was designed to provide a secure communication channel over a network. TLS performs the modern equivalent role. A secure web connection helps protect information exchanged between a browser and a website against interception and unauthorised modification. It also helps the browser verify the website's identity through a digital certificate.

Simplified secure web connection process

User opens a website using HTTPS
↓

Browser and server negotiate supported security parameters
↓
Server presents its digital certificate
↓
Browser checks certificate validity and identity
↓
Session keys are established through the secure handshake
↓
Encrypted communication begins
↓
Browser and server exchange protected application data

Security benefits of HTTPS / TLS

- Confidentiality: helps prevent outsiders from reading transmitted data.
- Integrity: helps detect unauthorised modification of data in transit.
- Server authentication: certificate checks help confirm the website's identity.
- Trust: browser security indicators help users identify a protected connection, although users must still verify the domain and avoid phishing sites.

Limitations and safe use

HTTPS does not prove that a website is honest, that a seller will deliver goods, or that a device is free from malware. A fraudulent website can also obtain a valid certificate for its own domain. Users should check the domain name, avoid unexpected links, keep software updated and never share authentication codes. For current deployments, organisations should use supported TLS versions and secure configurations rather than obsolete SSL.

5.11 Security responsibilities of an E-Business organisation

Management responsibility	Practical action
Policy	Create clear policies for acceptable use, passwords, data handling and remote access.
People	Train employees and test awareness of phishing and social engineering.
Technology	Maintain secure systems, encryption, access controls and updates.
Data	Classify information, limit collection and retain it only as required.
Monitoring	Review logs, unusual transactions and access attempts.
Response	Maintain a written incident response and communication plan.
Continuity	Test backups and recovery arrangements.
Third parties	Assess service providers, platforms and outsourced technology.