E-Commerce & Electronic Banking

Lecture 2

Assis Lec: Hadi Salah

Lecture Objectives

By the end of this lecture, students will be able to:

• Understand e-commerce concepts

• Define electronic banking

• Identify types of electronic banking services

• Understand advantages and challenges of e-banking

• Recognize security issues in online banking

What is E-Commerce?

Electronic Commerce (E-Commerce) refers to buying and selling goods and services over electronic networks, especially the Internet.

It includes online shopping, online payments, and digital services.
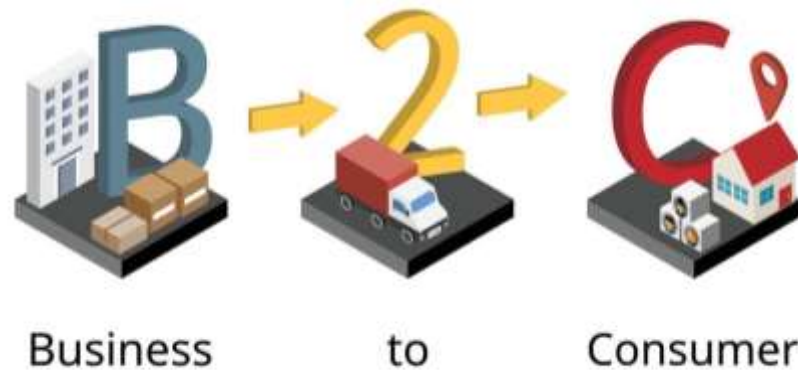
Types of E-Commerce

E-commerce can be classified into:

- B2C (Business to Consumer)

- B2B (Business to Business)

- C2C (Consumer to Consumer)

- C2B (Consumer to Business)

B2C – Business to Consumer

B2C refers to transactions where businesses sell products or services directly to consumers.
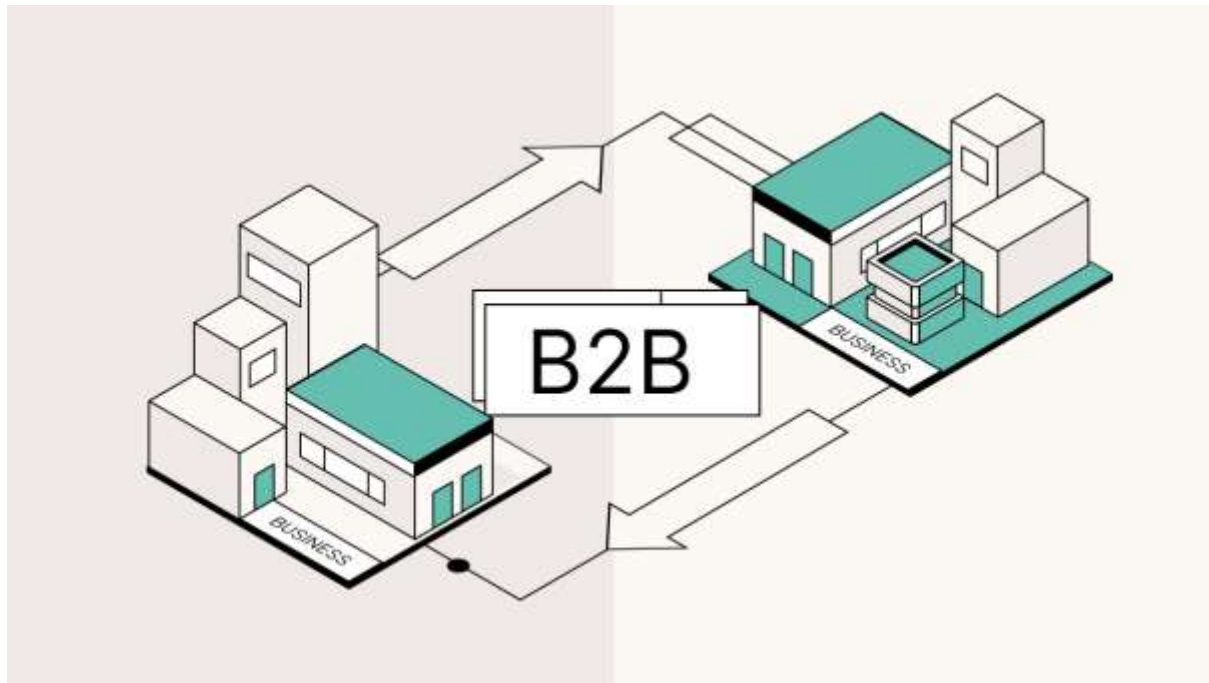
Examples include online shopping websites such as Amazon and online food delivery platforms.

Business   to   Consumer

B2B – Business to Business
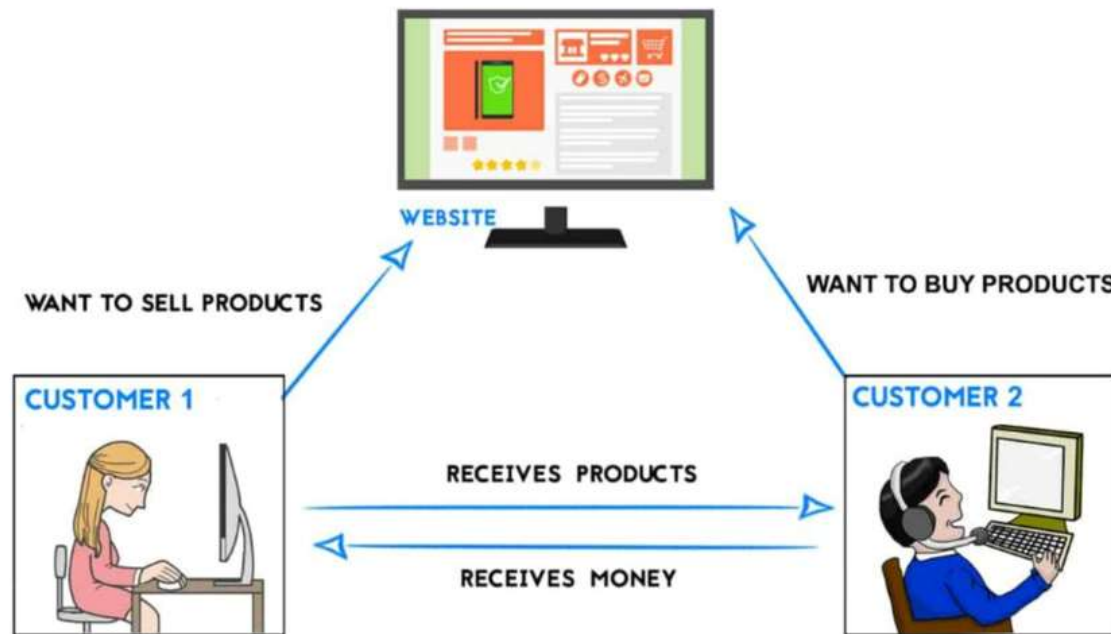
B2B involves transactions between businesses.

It is commonly used for wholesale, supply chains, and enterprise services.

C2C – Consumer to Consumer

C2C allows consumers to sell products or services directly to other consumers.

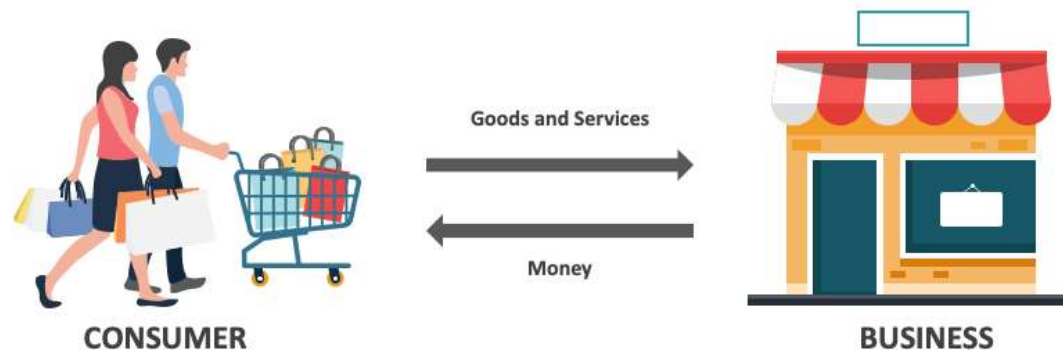Online marketplaces enable these transactions.

C2B – Consumer to Business

C2B occurs when individuals offer products or services to businesses.

Examples include freelancing platforms and influencer marketing.
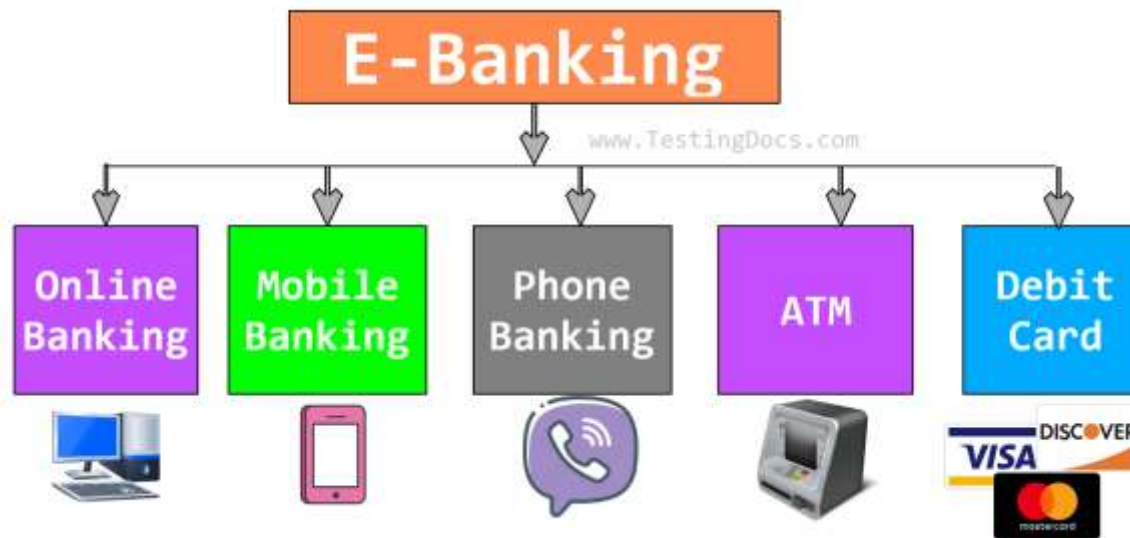
CONSUMER TO BUSINESS (C2B)

Goods and Services

Money

CONSUMER

BUSINESS

Electronic Banking (E-Banking)

Electronic banking refers to the use of electronic channels to deliver banking services.

It allows customers to perform banking transactions without visiting a physical bank branch.

Online Banking

Online banking allows customers to access their bank accounts through the internet.

Customers can check balances, transfer money, and pay bills online.

ATM Services

Automated Teller Machines (ATM) allow customers to withdraw cash anytime.

ATMs also support balance inquiry, fund transfer, and mini statements.

Debit Card Services

Debit cards are used for electronic payments directly from a bank account.

They are commonly used in shops, online purchases, and ATMs.

Phone Banking

Phone banking allows customers to perform banking operations via phone calls.
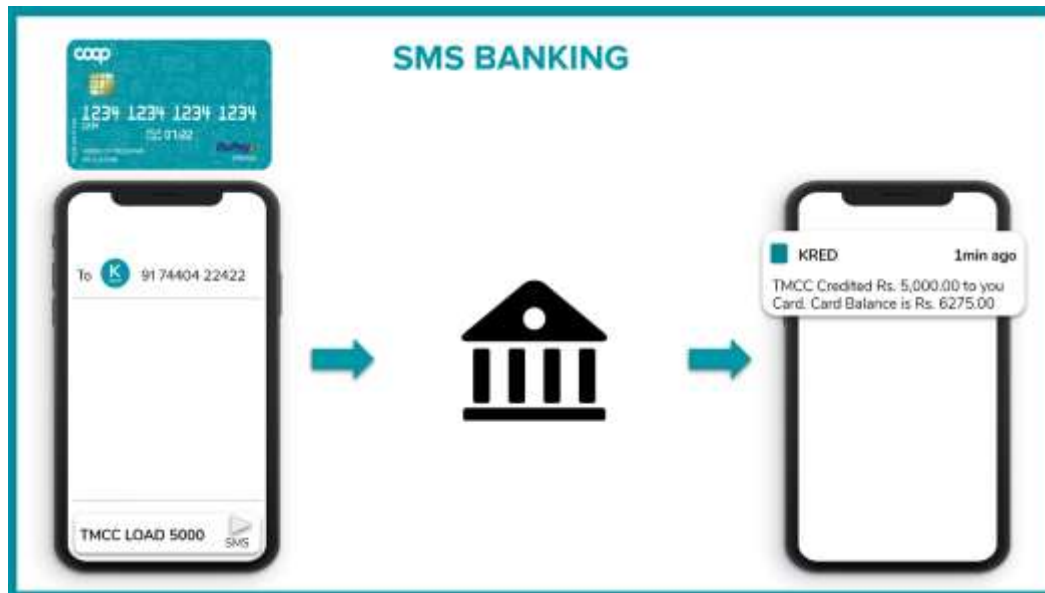
It provides services such as balance inquiry and transaction confirmation.

SMS Banking

SMS banking enables customers to receive account information via text messages.
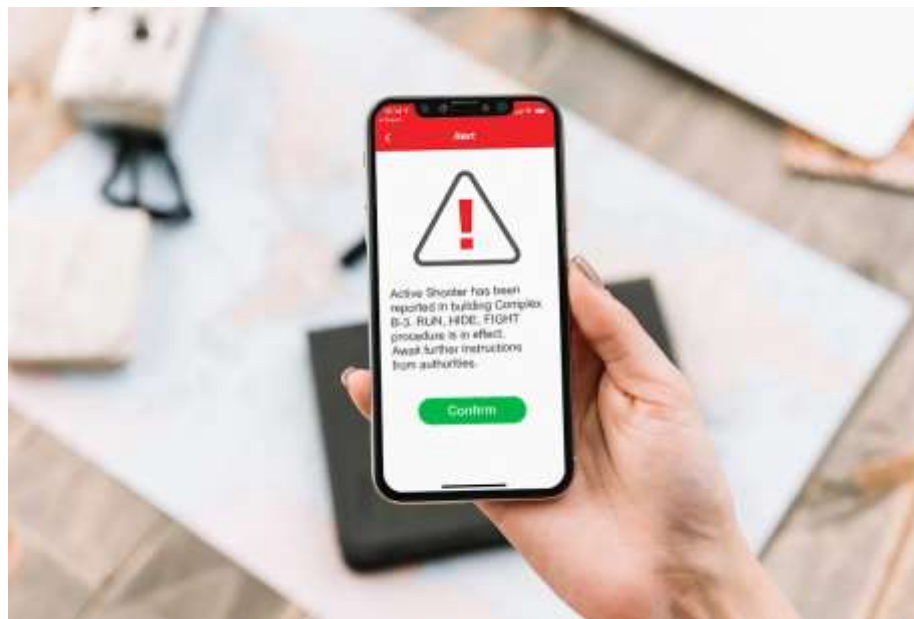
It is used for balance alerts, transaction alerts, and reminders.

Electronic Alerts

Electronic alerts notify customers about account activities.

Alerts help detect unauthorized transactions and improve security.

Mobile Banking

Mobile banking uses smartphone applications to provide banking services.

It supports transfers, bill payments, and account management anytime, anywhere.

Advantages of Electronic Banking

- Convenience and time saving

- 24/7 access to services

- Faster transactions

- Reduced operational cost

Challenges of Electronic Banking

- Security risks

- Internet dependency

- Technical issues

- Lack of user awareness

Security in Electronic Banking

Security is critical in e-banking systems.

It includes authentication, encryption, and fraud detection mechanisms.

Why Security is Critical in E-Banking

Banks deal with **highly sensitive data and money**, therefore security is essential to:

• Protect customer financial information

• Prevent fraud and identity theft

• Maintain trust between banks and customers

• Ensure legal and regulatory compliance

Main Security Objectives

Electronic banking security focuses on the following principles:

- **Confidentiality** – Protecting data from unauthorized access

- **Integrity** – Ensuring data is not altered during transmission

- **Availability** – Banking services must be accessible when needed

- **Authentication** – Verifying user identity

- **Non-repudiation** – Preventing denial of performed transactions

Common Security Threats

- Phishing attacks

- Malware

- Identity theft

- Unauthorized access

Phishing Attacks

Phishing is a type of cyber attack where attackers send fake emails, messages, or websites pretending to be trusted organizations.

The goal is to trick users into revealing sensitive information such as usernames, passwords, or bank details.

Malware

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.

Common types of malware include viruses, worms, trojans, spyware, and ransomware.

Malware

1- Viruses
Malicious programs that attach themselves to legitimate files or programs. They spread when the infected file is executed and can damage data or disrupt system operations.

2- Worms
Self-replicating malware that spreads automatically across networks without user interaction, often causing network congestion and system slowdowns.

3- Trojans (Trojan Horses)
Malware disguised as legitimate software. Once installed, they create backdoors, steal data, or allow attackers to control the system.

4- Spyware
Software that secretly monitors user activities, collects sensitive information such as passwords or banking details, and sends it to attackers.

5- Ransomware
Malware that encrypts files or locks systems and demands a ransom payment to restore access.

Identity Theft

Identity theft occurs when an attacker steals personal information such as national ID numbers, credit card details, or login credentials.

The stolen identity is then used to commit fraud or other illegal activities.

Unauthorized Access

Unauthorized access happens when a person gains access to a system, network, or data without permission.

This can occur due to weak passwords, hacking techniques, or insider misuse.

Conclusion

E-commerce and electronic banking play a major role in modern digital economies.

Understanding electronic banking services helps users and organizations operate safely and efficiently.