Unit – 4

E-Commerce

E-Commerce is a method of buying and selling goods and services online. E-commerce can be defined as- "**E-Commerce" or "electronic commerce**" is the trading of goods and services on the internet.

Components of E-Commerce

The main components of e-commerce include:

1) **Website**: A digital platform where transactions take place. This could be a standalone online store, a marketplace like Amazon or eBay, or even a social media platform with built-in shopping capabilities.
2) **Product Catalog**: An organized listing of the products or services available for purchase, including descriptions, images, prices, and any other relevant information.
3) **Shopping Cart**: A virtual cart that allows customers to select items they want to purchase and store them while they continue browsing. It also enables customers to review their selected items before proceeding to checkout.
4) **Payment Gateway**: A secure service that processes online payments, allowing customers to pay for their purchases using various methods such as credit/debit cards, digital wallets, or bank transfers.
5) **Order Management System**: Software that helps businesses manage orders received through the e-commerce platform, including order processing, inventory management, and shipping logistics.
6) **Customer Relationship Management (CRM)**: Tools and strategies for managing interactions with customers, such as email marketing, customer support, and loyalty programs, to foster long-term relationships and repeat business.
7) **Mobile Responsiveness**: With the increasing use of smartphones and tablets for online shopping, ensuring that the e-commerce platform is optimized for mobile devices is essential for reaching and engaging customers on-the-go.

Elements of E-Commerce security

E-commerce security is a set of guidelines that ensure safe online transactions. Just like physical stores invest in security guards or cameras to prevent theft, online stores need to defend against cyberattacks.

The elements of E-Commerce security are:

- **Privacy**: In the context of ecommerce security, privacy involves preventing unauthorized internal and external threats from accessing customer data. Disrupting customer privacy is considered a breach of confidentiality and could have devastating consequences for your customers' privacy and your reputation as a retailer. Privacy measures include antivirus software, firewalls, encryption, and other data protection measures.
- **Integrity**: Integrity refers to how accurate a company's customer data is. Maintaining a clean, curated customer dataset is critical to running a successful ecommerce business. Using incorrect customer's data — such as their phone number, address, or purchase history — causes people to lose confidence in your ability to protect their data and in your company.
- **Authentication**: Authentication proves that your business does what it claims and that customers are who they say they are.
- **Non-repudiation**: Non-repudiation means neither a company nor a customer can deny transactions they've participated in. Non-repudiation is somewhat implicit in physical stores but pertains to online purchases as well. Non-repudiation measures like digital signatures ensure that neither party can deny a purchase after it has been made.
- **Encryption**: Utilizing encryption protocols such as SSL/TLS to encrypt data transmitted between the customer's browser and the e-commerce server. This protects sensitive information like credit card numbers, passwords, and personal details from interception by unauthorized parties.
- **Secure Sockets Layer (SSL) Certificates**: SSL certificates verify the identity of the website and establish an encrypted connection. Websites with SSL certificates display a padlock icon in the browser's address bar and use "**https://**" in the URL, indicating a secure connection.

E-Commerce threats

With the growth of e-commerce comes a heightened level of risk regarding data security. Businesses must be aware of the common threats in the digital space and how to best protect their customer data.

COMMON E-COMMERCE SECURITY THREATS
PAYMENT SECURITY
• Credit Card Fraud
• Phishing
• Skimming
DATA SECURITY
• Hacking
• Malware
• Denial of Service (DoS) Attack
NETWORK SECURITY
• Unauthorized Access
• Insecure Network Infrastructure
• Poor Password Management

Data Security

Data security is one of the most important aspects of e-commerce safety and security. Data security includes protecting customer data from hackers, malware, and denial of service (DoS) attacks.

1) **Hacking**: Hacking is a type of cyberattack that involves gaining unauthorized access to a computer system or network. Hackers can use this access to steal customer data, modify or delete files, or take control of the system. Businesses should take steps to protect their systems from hacks, including implementing strong passwords and two-factor authentication, using a secure connection, and regularly patching software.
2) **Malware:** Malware is software that is intended to harm or disable computer systems. Malware commonly includes viruses, ransomware, and spyware. Businesses should use anti-malware software and scan their systems on a regular basis to protect themselves from malware.

3) **Denial of Service (DoS) Attacks:** DoS attacks are a type of cyberattack that seeks to make a computer system or network unavailable for use by flooding it with traffic or requests. DoS attacks can cause significant disruptions to an e-commerce store, including slowing down or crashing the website, preventing customers from accessing the site, and preventing orders from processing.

Payment Security

Payment security is critical for any e-commerce business, as customers trust their sensitive financial information to your website. Payment security threats come in many forms, including phishing, skimming, and credit card fraud.

1) **Credit Card Fraud**: Credit card fraud is one of the most common forms of payment security threat. Credit card fraudsters use stolen credit card numbers to make unauthorized purchases. It's important to ensure your website is PCI-compliant to prevent credit card fraud. This will include using SSL encryption, tokenization, and other security measures.
2) **Phishing**: Phishing is common tactic cybercriminals use to access sensitive information. Phishing involves sending out emails that appear from a legitimate source but are malicious. The emails often contain a malicious link or attachment that installs malware onto the user's computer.
3) **Skimming**: Skimming is another payment security threat when a malicious actor places a device on a payment terminal or ATM to capture credit card information. Skimmers are becoming increasingly sophisticated; some can even be used remotely via Bluetooth. To protect against skimming, it's important to ensure that all payment terminals and ATMs have up-to-date security protocols.

Network Security

Network security is one of the most essential parts of any e-commerce security strategy. It's important to ensure that your network is up to date with the latest security protocols and that you're using a secure network architecture. It's also important to regularly monitor your network to ensure its security. This can be done through network scanning and intrusion detection systems.

1) **Unauthorized Access:** Unauthorized access is a major security threat in the e-commerce world. This can be done through malicious software, phishing attacks, and other malicious

activities. It's important to ensure that all of your systems are secured and that you're using strong authentication methods to prevent unauthorized access.

2) **Insecure Network Infrastructure**: Insecure network infrastructure is another common security threat. It's important to make sure that your network is regularly updated and maintained to prevent any cyber-attacks. Additionally, you should make sure that your network is protected from the inside out, with firewalls, VPNs, and other security measures.
3) **Poor Password Management**: Poor password management is another common security threat in e-commerce. It's crucial to ensure that all your passwords are strong and that they're regularly changed. Additionally, you should also ensure that all your staff members have unique passwords and that they're not shared with anyone else.

E-Commerce security best practices

E-commerce security is crucial for building trust with your customers and protecting your business. Here are some key best practices to consider:

Protecting Customer Data

- Implement strong encryption: Use HTTPS with a valid SSL certificate to encrypt all communication between your website and users. This safeguards sensitive information like passwords and credit card data.
- Minimize data storage: Only store customer data that is absolutely necessary for your business operations. Avoid storing full credit card numbers if possible.
- Enforce strong passwords: Require customers to create strong passwords and encourage them to enable two-factor authentication (2FA) for additional security.
- Regularly update software: Maintain updated software for your e-commerce platform, plugins, and operating systems to patch known vulnerabilities.
- Regularly scan for vulnerabilities: Conduct regular security scans of your website to identify and address potential weaknesses before they are exploited.

Payment Security

- Use a reputable payment gateway: Partner with a PCI DSS compliant payment processor to handle financial transactions securely. These companies have robust security measures in place.

- Avoid storing sensitive payment information: If possible, use a payment gateway that tokenizes or otherwise obfuscates sensitive credit card data.
- Implement fraud prevention measures: Use address verification systems (AVS) and other fraud detection tools to minimize the risk of fraudulent transactions.

General Security

- Educate your staff: Train your employees on cybersecurity best practices to identify and avoid phishing attacks, social engineering scams, and other threats.
- Implement access controls: Grant access to sensitive data and systems on a need-to-know basis and regularly review user permissions.
- Back up your data: Regularly back up your website and databases to a secure location in case of data breaches or ransomware attacks.
- Have a security incident response plan: Develop a plan for responding to security incidents in a timely and effective manner.

Advantages of E-Commerce

The advantages of E-Commerce are as follows:

1) **Global Reach**: E-commerce allows businesses to reach a global audience without the constraints of geographical location. This opens new markets and opportunities for growth, enabling businesses to expand their customer base beyond traditional boundaries.
2) **24/7 Availability**: Unlike physical stores with fixed operating hours, e-commerce websites are accessible 24 hours a day, 7 days a week. This provides convenience for customers who can shop at their own pace and convenience, regardless of time zone differences or busy schedules.
3) **Lower Overhead Costs**: Operating an e-commerce business typically involves lower overhead costs compared to brick-and-mortar stores. E-commerce eliminates the need for expensive retail space, reduces staffing requirements, and lowers utilities and maintenance expenses.
4) **Increased Convenience**: E-commerce offers unparalleled convenience for consumers, allowing them to browse, compare, and purchase products or services from the comfort of their homes or on-the-go using mobile devices. This eliminates the need for physical travel and saves time and effort.

5) **Wider Product Selection**: E-commerce platforms can offer a wider selection of products and services compared to traditional retail stores, as they are not limited by physical space constraints. This provides consumers with more choices and enables businesses to cater to niche markets.
6) **Personalized Shopping Experience**: E-commerce platforms can leverage data analytics and customer profiling techniques to offer personalized shopping experiences. By analyzing customer preferences and behavior, businesses can recommend relevant products, send targeted promotions, and tailor the shopping journey to individual preferences.
7) **Cost-Effective Marketing**: E-commerce allows businesses to leverage digital marketing channels such as social media, search engine optimization (SEO), and email marketing to reach and engage customers cost-effectively. Digital marketing campaigns can be highly targeted and offer measurable results, allowing businesses to optimize their marketing efforts for maximum return on investment (ROI).

Survey of popular e-commerce sites

Some of the most popular e-commerce sites globally include:

1) **Amazon**: Amazon is the largest online retailer in the world, offering a vast selection of products across various categories, including electronics, books, clothing, and household goods. It also provides services such as Amazon Prime for fast shipping and streaming content.
2) **Alibaba**: Alibaba is a Chinese e-commerce giant known for its diverse range of platforms, including Alibaba.com for wholesale trade, Taobao for consumer-to-consumer (C2C) sales, and Tmall for business-to-consumer (B2C) sales. It dominates the e-commerce market in China and serves customers worldwide.
3) **JD.com**: JD.com, also known as Jindong, is one of the largest B2C online retailers in China, offering a wide range of products, including electronics, apparel, and fresh groceries. It operates its own logistics network and focuses on providing high-quality, authentic products to customers.
4) **eBay**: eBay is a global online marketplace that facilitates consumer-to-consumer and business-to-consumer sales. It offers auctions and fixed-price listings for a wide variety of products, including collectibles, electronics, and used goods.

5) **Walmart**: Walmart is a multinational retail corporation that operates both physical stores and an e-commerce platform. Walmart.com offers a wide selection of products, including groceries, electronics, clothing, and home goods, with options for in-store pickup and delivery.

6) **AliExpress**: AliExpress is a subsidiary of Alibaba Group that caters to international consumers, offering a wide range of products at competitive prices. It primarily focuses on small to medium-sized businesses selling directly to consumers.

7) **Flipkart**: Flipkart is one of the largest e-commerce platforms in India, offering a diverse range of products, including electronics, fashion, and home goods. It was acquired by Walmart in 2018 and competes with Amazon in the Indian market.

8) **Rakuten**: Rakuten is a Japanese e-commerce company that operates a diverse range of services, including an online marketplace, travel booking, and financial services. It offers a loyalty program that rewards customers with cashback and discounts.

9) **Taobao**: Taobao is a Chinese online shopping website owned by Alibaba Group, specializing in consumer-to-consumer (C2C) sales. It offers a wide range of products, including clothing, electronics, and accessories, often at discounted prices.

10) **Etsy**: Etsy is an online marketplace focused on handmade, vintage, and unique goods. It connects independent sellers with buyers looking for artisanal products, crafts, and personalized items.

Introduction to Digital payments:

Digital payments are a way to exchange money electronically, without using physical cash or checks. Instead of handing over cash or coins, you can use your computer, smartphone, or other electronic devices to transfer money from one account to another.

Here's how it works:

1)	**Setting Up an account**: To make digital payments, you first need to have an account with a digital payment service provider. This could be a bank, a mobile payment app like Paytm or Google pay, You link your bank account, credit card, or debit card to this digital account.

2)	**Making a payment**: When you want to pay for something digitally, you provide the necessary information such as the recipient's account details or their phone number or email address associated with their digital wallet. Then you specify the amount you want to transfer.
3)	**Processing the payment**: The digital payment service securely processes your request, verifies your identity, and checks if you have sufficient funds in your account to cover the payment.
4)	**Confirmation**: Once the payment is processed successfully, you receive a confirmation, usually via email or notification on your device. The recipient also gets notified of the incoming payment.
5)	**Completion**: The recipient now has the money in their digital account, which they can leave there or transfer to their bank account.

Digital payments offer several advantages over traditional cash transactions, such as convenience, speed, and security

Components of Digital payments & stakeholders

Components of Digital Payments:

1) **Payment Gateway**: This is like a digital bridge between the buyer and seller. It securely authorizes and processes the payment transaction. Think of it as the cashier at a digital store.
2) **Merchant Account**: This is where the money from your purchases goes. It's a special kind of bank account that allows businesses to accept digital payments.
3) **Digital Wallets**: These are apps or platforms where you store your payment information, like credit card details or bank account numbers, to make purchases online or in stores without needing to enter your information every time.
4) **Payment Processor**: This is the behind-the-scenes technology that securely moves money from the buyer's account to the seller's account. It's like the middleman that ensures the transaction happens smoothly.
5) **Security Measures**: These are the tools and protocols that protect your financial information from being stolen or misused. Examples include encryption, two-factor authentication, and fraud detection systems.

Stakeholders in Digital Payments

1) **Consumers**: These are the people like you and me who use digital payments to buy goods and services, send money to friends, and manage our finances online.
2) **Merchants**: These are the businesses that accept digital payments from customers in exchange for goods or services. They rely on digital payments to facilitate transactions and grow their businesses.
3) **Banks and Financial Institutions**: These organizations provide the infrastructure and services that enable digital payments to happen, such as issuing credit and debit cards, managing accounts, and processing transactions.
4) **Payment Service Provider**: These companies offer platforms and technologies that facilitate digital payments, such as payment gateways, digital wallets, and payment processing services.
5) **Regulatory Bodies**: These are government agencies or industry associations that set rules and standards for digital payments to ensure they are safe, fair, and compliant with laws and regulations.

Each of these stakeholders plays a crucial role in the digital payment ecosystem, working together to enable seamless and secure transactions for consumers and businesses alike.

Mode of digital payments

Banking Card (Debit/Credit Card)

- **What it is**: A banking card, whether debit or credit, is a physical card issued by your bank that allows you to make purchases or withdraw cash electronically.
- **How it works**: You use your card to swipe, insert, or tap at a point-of-sale (POS) terminal in a store. The terminal reads the information on your card's magnetic stripe or chip, and you usually input a PIN or sign a receipt to confirm the transaction. For online purchases, you enter your card details on the website's payment page.
- **Key features**: Convenience, widespread acceptance, ability to make both online and offline payments.

Unified Payments Interface (UPI)

- **What it is**: UPI is a real-time payment system developed by the National Payments Corporation of India (NPCI) that allows you to instantly transfer money between bank accounts through a smartphone app.
- **How it works**: You link your bank account to a UPI-enabled mobile app provided by your bank or a third-party app like Google Pay, PhonePe, or Paytm. To send money, you enter the recipient's UPI ID (e.g., phone number@upi) and the amount, and authenticate the transaction using a PIN or biometric authentication.
- **Key features**: Instant transfers 24/7, no need to remember or share bank details, interoperability between different banks and apps.

E-Wallets

- **What they are**: E-wallets, or digital wallets, are mobile apps or online platforms that allow you to store money and make payments electronically.
- **How they work**: You create an account with the e-wallet provider and link it to your bank account or card. You can then add funds to your e-wallet and use the balance to pay for goods and services online or in stores. Some e-wallets also offer features like bill payments, mobile recharges, and peer-to-peer transfers.
- **Key features**: Convenience, faster checkout, security features like encryption and biometric authentication.

Each mode of digital payment has its own advantages and use cases, and you may choose the one that best suits your needs based on factors like convenience, security, and acceptance.

Unstructured Supplementary Service Data(USSD)

USSD, or Unstructured Supplementary Service Data, is a communication protocol used by GSM (Global System for Mobile Communications) cellular telephones to communicate with the mobile network operator's computers.

- It allows users to access various services and interact with applications using short codes, typically starting with * and ending with #.
- USSD messages are usually displayed in real-time and enable instant communication between the mobile device and the network.

- They are commonly used for services such as balance inquiries, mobile banking, prepaid mobile recharge, and accessing menu-based services.
- Unlike SMS, USSD sessions are session-based, meaning the interaction occurs in real-time, and the session terminates once the user ends the session or the network does not receive any input for a certain period.
- USSD is widely used globally, particularly in developing countries, due to its simplicity and accessibility, even on basic mobile phones.

Some examples for USSD

1) Checking your prepaid mobile balance: Dialling *123# and pressing call to see your current balance.
2) Mobile banking: Using USSD to transfer funds between accounts by dialling a specific code and following the prompts.
3) Recharging your mobile data: Dialling *141# to recharge your data plan with a prepaid voucher.
4) Checking bank account balance: Dialling *99# to access basic banking services like balance inquiry and mini statement.

Aadhaar Enabled Payment System(AePS)

Aadhaar Enabled Payment System(AePS) is a payment service developed by the National Payments Corporation of India (NPCI) that allows Aadhaar-linked bank account holders to conduct financial transactions through micro-ATMs.

Here's some key information about AePS:

1) **Authentication**: AePS uses Aadhaar biometric authentication (fingerprint or iris scan) for user identification, eliminating the need for ATM cards or PINs.
2) **Financial Transactions**: Users can perform various financial transactions such as cash withdrawals, balance inquiries, fund transfers, and bill payments using AePS.
3) **Banking Inclusion**: AePS aims to promote financial inclusion by providing basic banking services to individuals who may not have easy access to traditional banking infrastructure.
4) **Micro-ATMs**: AePS transactions are facilitated through micro-ATMs, which are essentially modified point-of-sale (POS) terminals equipped with fingerprint scanners and a GPRS connection.

5) **Participating Institutions**: AePS is available through banks and financial institutions that are authorized to provide Aadhaar-based services.
6) **Security**: Aadhaar biometric authentication adds an extra layer of security to transactions, reducing the risk of fraud and unauthorized access.
7) **Availability**: AePS services are available 24/7, enabling users to conduct transactions at their convenience, even in remote areas with limited banking facilities.
8) **Government Schemes**: AePS is often used to facilitate government subsidy payments, welfare benefits, and other social security payments directly into beneficiaries' bank accounts linked to Aadhaar.

Overall, Aadhaar Enabled Payment System plays a crucial role in promoting digital financial inclusion and facilitating secure, convenient transactions for Aadhaar-linked bank account holders across India.

Digital payments related common frauds and preventive measures

Common digital payment frauds include phishing scams, identity theft, account takeover, and unauthorized transactions. Here are some preventive measures to safeguard against these frauds:

1) **Phishing Awareness**: Be cautious of unsolicited emails, messages, or phone calls asking for personal or financial information. Verify the authenticity of the sender before responding or clicking on any links.
2) **Secure Passwords**: Use strong, unique passwords for your online accounts and update them regularly. Avoid using easily guessable information such as birthdays or pet names. Enable two-factor authentication (2FA) whenever possible.
3) **Secure Networks**: Avoid using public Wi-Fi networks for conducting financial transactions, as they may be insecure. Use a secure and trusted network connection, such as your home Wi-Fi or mobile data.
4) **Verify Transactions**: Regularly review your bank and credit card statements to detect any unauthorized transactions. Report any discrepancies or suspicious activities to your bank or financial institution immediately.
5) **Secure Websites**: Ensure that you are using secure websites for online transactions by looking for "https://" and a padlock icon in the address bar. Avoid entering sensitive information on unsecured websites.

6) **Update Software**: Keep your devices, operating systems, and antivirus software up to date with the latest security patches and updates to protect against vulnerabilities.
7) **Use Trusted Apps**: Only download and use official and trusted payment apps from reputable sources such as the Google Play Store or Apple App Store. Avoid downloading apps from unknown sources or third-party app stores.
8) **Educate Yourself**: Stay informed about the latest fraud trends and scams in the digital payment space. Educate yourself and your family members about common fraud tactics and how to recognize and avoid them.

By following these preventive measures and exercising vigilance while conducting digital transactions, you can reduce the risk of falling victim to common payment frauds.

RBI Guidelines on digital payments and customer protection in unauthorized banking transactions.

1) The RBI has issued guidelines to ensure customer protection in digital payments and unauthorized banking transactions.
2) These guidelines aim to enhance the security of digital transactions and protect customers from fraudulent activities.
3) They include measures such as two-factor authentication, limits on transaction amounts, and real-time alerts for transactions.
4) They include measures such as two-factor authentication, limits on transaction amounts, and real-time alerts for transactions.
5) The RBI also provides a grievance redressal mechanism to address customer complaints related to digital payments.

Relevant provision of payment settlement act 2007

- **Payment and Settlement Systems Act, 2007** provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India (Reserve Bank) as the authority for that purpose and all related matters.
- The PSS Act, 2007 received the assent of the president on 20th December 2007 and it came into force with effect from 12th August 2008.
- The Act also provides the legal basis for "netting" and "settlement finality".