M.Com IVth Semester **Course - MC 4.5**

E-COMMERCE

LESSONS 1- 10

By:-

Prof. Aman Kumar Sharma
Computer Science Department,
H.P. University, Shimla

(NAAC Accredited "A" Grade University)
INTERNATIONAL CENTRE FOR DISTANCE EDUCATION AND OPEN LEARNING
HIMACHAL PRADESH UNIVERSITY, SHIMLA.

INDEX

SYLLABUS
MC 4.5
E-COMMERCE
Course Contents

Max.Marks 80
Internal Assessment 20

Unit I

Introduction to E-Commerce: Meaning of electronic commerce, business applications of e-commerce, comparison with traditional commerce.

Business models in E-Commerce- e-shops, e-procurement, e-auctions, value chain integrators, information brokerage, telecommunication, collaboration platforms, etc, electronic payment system.

Unit II

E-Banking-concept, operations. Online fund transfer, RTGS, ATM etc, Online share market operations.

Online Marketing and web based advertising, - concept, and advantages. Types of online advertisements.

Unit III

Search Engine- as an advertising media, search engine optimization- concept and techniques, e-mail marketing, social networking and marketing- promotion, opinion etc. Viral Marketing, E-retailing concept, advantages, limitations. CRM and Information technology, Tools to conducting online research- secondary research, online focus groups web based surveys, data mining from social networking sites.

Unit IV

Enterprise resource planning –Security issues in e-commerce- online frauds, privacy issues, cyber laws including Information Technology Act.

Note: - There will be nine (9) questions in all. The first question is compulsory and consists of ten (10) short questions having two (2) marks each the candidate will be required to attempt one question from each unit and each question carries fifteen (15) marks.

For students of correspondence courses the paper will be of 100 marks spread as 20 marks including the compulsory question.

References

1. Bajaj, Kamlesh K and Debjani Nag: E-Commerce – The Cutting Edge Of Business, Tata McGraw Hill (P) Ltd. New Delhi.
2. Greenstein: Electronic Commerce, Tata McGraw Hill (P) Ltd. New Delhi.
3. Leon, Alexis: Fundamentals of Information Technology, Vikas Publication House (P) Ltd., New Delhi.
4. Mansfield, Ron: The Compact Guide to Microsoft Office, BPB Publication, Delhi.
5. Norton Peter: Introduction to Computer 4/E, Tata McGraw Hill (P) Ltd. New Delhi.

Saxena Sanjay: A First Course in Computer, Vikas Publication House (P) Ltd., New Delhi.

Chapter 1

INTRODUCTION TO E-COMMERCE

Objectives:

- Introduction
- Meaning of electronic commerce
- Business applications of e-commerce
- Benefits of e-commerce
- Limitations of e-commerce

1.1 Introduction

E-commerce is conducting business online. Selling goods and / or buying goods electronically using software programs. Web sites exist that run the main functions of an e-commerce web site, including product display, online ordering and inventory management. The software resides on a commerce server and works in conjunction with online payment systems to process payments. Since these servers and data lines make up the backbone of the internet, in a broad sense, e-commerce means doing business over interconnected networks.

E-Commerce or Electronics Commerce is a methodology of modern business which addresses the need of business organizations, vendors and customers to reduce cost and improve the quality of goods and services while increasing the speed of delivery. E-commerce refers to paperless exchange of business information using following ways.

- Electronic Data Exchange (EDI)
- Electronic Mail (e-mail)
- Electronic Bulletin Boards
- Electronic Fund Transfer (EFT)
- Other Network-based technologies

1.2 Electronic commerce

The definition of e-commerce includes business activities that are business-to-business (B2B), business-to-consumer (B2C), consumer-to-business (C2B), consumer-to-consumer (C2C), extended enterprise (also known as "newly emerging value chains"), digital commerce (d-commerce) and mobile commerce (m-commerce). E-commerce is a major factor in the U.S. economy because it assists computing companies with many levels of current business transactions, as well as creating new online business opportunities that are global in nature.

B2B (Business-to-Business): Companies doing business with each other such as manufacturers selling to distributors and wholesalers selling to retailers.

B2C (Business-to-Consumer): Interactions relating to the purchase and sale of goods and services between a business and consumer—retail transactions. Businesses selling to the general public typically through customized software.

C2B (Consumer-to-Business): A consumer attempts business transaction by selling a product to a business man. For example, a consumer posts his project with a set budget online and within hours companies review the consumer's requirements and bid on the project. The consumer reviews the bids and selects the company that will complete the project.

C2C (Consumer-to-Consumer): There are many sites offering free classifieds, auctions and forums where individuals can buy and sell thanks to online payment systems like PayPal where people can

send and receive money online with ease. eBay's auction service is a great example of where person-to-person transactions take place every day since 1995.

D-commerce is a type of e-commerce used by an organization that delivers and sells products online. D-commerce is used by companies that sell news, subscriptions, documents or any form of electronic content and the digital commerce company collects payments, handles customer refunds and billing and manages other accounting functions for online publisher clients. D-commerce is considered a form of e-commerce because it deals with the exchange of electronic goods. The pay-as-you-go model is applied to digital commerce. Customers start an account with a digital commerce company and can purchase text and content from publishers, but they only have to relay their financial information once. This makes for a more secure online environment. Publishers of books, news, magazines, white papers and academic research papers are big users of digital commerce. Some digital commerce companies resell publishers' content. This form of business can be very profitable for publishers and digital commerce companies.

M-Commerce, is about the explosion of applications and services that are becoming accessible from Internet-enabled mobile devices. It involves new technologies, services and business models. It is quite different from traditional e-commerce. Mobile phones impose very different constraints than desktop computers. They follow you wherever you go, making it possible to look for a nearby restaurant, stay in touch with colleagues, or pay for items at a store. M-commerce is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and Personal Digital Assistants (PDAs).

It can be summarized that business to business or B2B (vendor doing financial transaction with another vendor), business to consumer or B2C (consumer buying a product using internet) and consumer to consumer or C2C (consumer selling a product to another consumer) are different forms of ecommerce.

Few examples of e-commerce:

- accepting credit cards for commercial online sales
- generating online advertising revenue
- trading stock in an online brokerage account
- driving information through a company via its intranet
- driving manufacturing and distribution through a value chain with partners on an extranet
- selling to consumers on a pay-per-download basis, through a Web site

Rather, e-commerce is execution of any financial transaction with the use of electronic network. There are numerous ways of expressing the concept of e-commerce:

E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet.

In other words, the buying and selling of products and services in business by vendors and consumers through an electronic medium, without using any paper documents.

E-commerce is widely considered as buying and selling of products over the internet, further any transaction that is completed solely through electronic measures can be considered e-commerce.

Self-Check Exercise

Question I:

Is D-commerce a type of e-commerce used by an organization that delivers and sells products online? (True/False)

Question II:

eBay's auction service is a great example of _____.

Question III:

D-commerce is a form of e-commerce. (True/False)

1.3 Business applications of e-commerce

Various applications of e-commerce are continually affecting trends and prospects for business over the Internet, including e-banking, e-tailing and online publishing/online retailing. The most common e-commerce applications are as follows:

1. Manufacturing Sector
2. Wholesale Sector
3. Retail Sector
4. Service Sector
5. Marketing
6. Finance
7. Auctions
8. Banking
9. Electronic tickets

1. Manufacturing

Manufacturing can be defined as the process of collecting and then converting raw materials into finished, qualitative goods or products for the consumers. Manufacturing requires a web of various components, contracts personnel etc working intricately together and in synch in order to produce goods or services. Manufacturing requires components, assemblies, transportation, storages, paper works, etc. e-commerce applied to the supply chain management process helps in reducing the overall costs drastically and improves quality and efficiency by automating most of the supply chain. Hence, e-commerce is useful in the supply chain operations of a company. Some companies form an electronic exchange by providing together buy and sell goods, trade market information and run back office information such as inventory control. This speeds up the flow of raw material and finished goods among the members of the business community. Various issues related to the strategic and competitive issues limit the implementation of the business models. Companies may not trust their competitors and may fear that they will lose trade secrets if they participate in mass electronic exchanges.

2. Wholesale

Selling goods or products in large quantities to anyone other than the consumers, take for example the retailers, industrial/ commercial or other business users or even distributors are known as wholesalers.

Physical assembling, sorting & grading goods in large lots, breaking bulk, repacking and redistributing in smaller lots is all a part wholesale. E-Commerce benefits wholesalers in various ways such as:

- Reduced operating costs, access to accurate and correct information on time & quick responses helps in qualitative and efficient decision making.
- Ability of access to global marketing in less time and by consuming less effort.
- Gaining and catching up to the competitive edge held by foreign wholesalers such as MNC's.
- Offers a wide and extensive range of information, intermediary and business services.

3. Retail

Selling of goods and services to the consumers for their personal consumption and use is known as **retailing.** Retailers provide a link between the consumers and the manufacturers and add value to the product and service by making their sales easier. They even provide extra services from personal shopping to gift wrapping and home delivery.

E-Commerce has a number of applications in retail and wholesale. E-retailing or on-line retailing is the selling of goods from Business-to-Consumer through electronic stores that are designed using the electronic catalogue and shopping cart model. Cybermall is a single website that offers different products and services at one internet location. It attracts the customer and the seller into one virtual space through a web browser.

People can now sit at their computers, open the website they desire to do so and browse the catalogues put up by the company (retailer), choose their product and either pay for it online itself or on delivery. Having your store online helps drastically in cost cutting as companies don't need to purchase stores, they can cut down on staff, provide services to a much wider audience, etc.

4. Service sector

It involves basically the provision of all services such as distribution and sales of goods to other businesses and consumers such as pest control, entertainment and even services such as transportation. It also includes the public utilities and the soft parts of the economy such as insurance, banking, education, insurance, etc. The service sector focuses mainly on people to people services.

Services are intangible, it’s extremely difficult to make customer understand and aware about their benefits. Quality of services depends solely on the quality of the individual providing the services.

e-commerce helps in improving and increasing the speed of transactions, reduces management expenditure, increases efficiency and increases competitiveness.

It helps the insurance, banking and mainly all the financial sectors, real estate, telecommunications, tourism, logistics and postal services. E-commerce also helps services gain a competitive advantage by providing strategies for differentiation, cost leadership and customer satisfaction.

5. Marketing

Data collection about customer behaviour, preferences, needs and buying patterns is possible through web and e-commerce. This helps marketing activities such as price fixation, negotiation, product feature enhancement and relationship with the customer. Future prediction about the trend of sale can be estimated.

6. Finance

Financial companies are using e-commerce to a large extent. Customers can check the balances of their savings and loan accounts, transfer money to their other account and pay their bill through on-line banking or E-banking. Another application of E-Commerce is on-line stock trading. Shares can be sold or purchased online using websites designed for this purpose. Such web sites are linked to stock exchanges. Many Websites provide access to news, charts, information about company profile and analyst rating on the stocks.

7. Auctions

Customer-to-Customer E-Commerce is direct selling of goods and services among customers. It also includes electronic auctions that involve bidding. Bidding is a special type of auction that allows prospective buyers to bid for an item. For example, airline companies give the customer an opportunity to quote the price for a seat on a specific route on the specified date and time.

8. Banking

A more developed and mature e-banking environment plays an important role in e-commerce by encouraging a shift from traditional modes of payment (i.e. cash, cheques or any form of paper-based legal tender) to electronic alternatives (such as e-payment systems). E-banking provides better tracking mechanism of financial transactions. E-bank provides the facility of transferring money from an account to another electronically.

9. Electronic tickets

Tickets can be bought for trains, aeroplanes, movies, theatres, parks, auditions, games etc. by making payment using credit cards, debit cards and internet banking. The soft copy of the ticket is sent digitally in return and at times the ticket can even be sent by postage.

Thereby the applications of e-commerce are in the domain of any sale and purchase of goods and services for which the payment has been made electronically. Some more examples are, Document automation in supply chain and logistics, Domestic and international payment systems, Enterprise content management, Group buying, Print on demand, Automated online assistant, Newsgroups, Online shopping and order tracking, Online office suites, Shopping cart software, Teleconferencing, Social networking and Instant messaging.

Self-Check Exercise

Question IV:

Process of collecting and converting raw material into finished goods is known as _____.

Question V:

Selling goods and products in large quantities is called _____.

Question VI:

Selling of goods and services is known as Retailing. (True/False)

Question VII:

Data collection about customer behaviour is called _____.

Question VIII:

Tickets can be bought for trains, movies, buses etc. by making payment using Debit card / Credit card. (True/False)

1.4 Benefits of e-commerce

E-Commerce uses the technology of digital information processing and electronic communications through internet in business transactions that helps in facilitating and redefining the relationships between or among organizations and between organizations and individuals for value creation. Multiple benefits are provided by E-commerce to the consumers in form of availability of goods at lower cost, wider choice and saves time. Internet is treated as a functional and operational medium for consumers, business owners, information seekers and entrepreneurs. E-Commerce sales would rise in the years to come with the increasing availability of broadband internet services combined with new applications.

E-commerce has several advantages:

1. Conduct business 24 x 7

E-Commerce can operate all day every day. Physical shop does not need to be open for customers and suppliers for doing business electronically.

2. Reduce cost to buyers

Electronically open market places will increase competition and reduce buyers cost.

3. Reduced cost to the suppliers

The ability to access online databases of bid opportunities, to submit bids electronically and to review awards online will reduce supplier's costs

4. Create new markets

The ability to reach potential customers easily and cheaply will create new markets.

5. Easy market entry

Market entry will be easier when geographic limits are no longer relevant.

6. Increase in variety of goods

As the market will expand, the variety of goods available shall also expand.

7 Reduce inventories

Electronically linking the demand for goods and services through just-in-time inventory and integrated manufacturing techniques will allow companies to maintain reduce inventories.

8. No Middlemen

There is a direct contact with customers in e-commerce through internet without any intermediation. Companies can now focus more on specific customers by adopting different one-to-one marketing strategy.

9. Improved and better customer service

Since there is a direct contact with the customers, it is possible to solve their queries regarding price, quality and additional features of the product can be provided and thus resulting in a better improved customer service. Response time is reduced between the seller and the buyer. It also improves the loyalty among customers.

10. Teamwork

The output of the e-commerce is the teamwork that helps organizations work together. Email is one of the examples of how people collaborate to exchange information and work on solutions. It has changed the way organizations interact with the suppliers, vendors and customers.

11. Information sharing with the customers

It is possible for the buyers to keep in touch with the seller's web site, find the information and can make quick purchase decisions. Knowledge of the customer is increased about the product and its varied features. Thus web is a source of dissemination of information for the probable customers.

12. Customized products

On the basis of the demand from the customers for their requirements about the product, it is possible to differentiate the product for an individual. There are many websites that helps in reorganizing, revising or editing the digital products.

13. Swapping of goods and services

Swapping is to exchange or using a barter system for goods and services on the websites between the business firms. A firm offers something for a want of another service or product from another firm for its services. For example instead of accepting cash for a consultancy service from a firm, a person or another firm can buy products in exchange from that firm.

14. Information sharing

It takes only few seconds to share information over the internet. A firm can e-mail the required data to its customers and can solve their product related queries. This is a major advantage overcoming the limitation of traditional method of doing business.

15. Global reach

Creating a web site for a firm or set of products and uploading it on the server, enables it to reach millions of customer worldwide. E-Commerce creates the whole world as a global village from where anyone can buy anything at anytime from anywhere.

16. Expanded customer base

The websites have access to customers' world-wide. Restriction of regions or physical locations is over ruled in online shopping.

17. Search engine marketing

Customers have easy access to find a product or service using search engines. Data pertaining to prices, specifications of products, availability details, comparison with other similar products and other related data can be accessed using search engines.

18. Reduction of marketing and advertising Costs

The need of advertising is reduced to a great extent with the advent of e-commerce. The probable customer attempts to locate the product on its own. A business firm can easily promote its product on the website by giving the complete required information over the internet. One of the tools of e-commerce is sales promotion from where not only the firm gains but also the customers are benefited.

19. Widened size of market

Expands the size of the market from regional to national or national to international market, the product has a wider domain from which it can be accessed.

20. Higher profits

A great amount of reduction in cost is measured in e-commerce in transactions of commercial nature e.g. no manual handling of the transactions, paperless exchange, easy payments from customers, no transportation except in the case of tangible products and higher profit margins from higher sales volume. Also business over the internet attracts every customer from all over the world and exposure in the new markets enhances the profits of the business firm.

21. Equal access rights

Anyone can start up a company on the internet. Equal rights are given to the smaller organizations in comparison to multinational, large international firms.

E-commerce uses the technology of digital information processing and electronic communications through internet in business transactions that helps in facilitating and redefining the relationships between or among organizations and between organizations and individuals for value creation. Wider domain and less overhead is the key factor in e-commerce.

Self-Check Exercise

Question IX:

Does e-commerce help in reducing the product cost? (True/False)

Question X:

Is there any middleman in e-commerce? (True/False)

Question XI:

E-commerce uses _____ of digital information process.

Question XII:

Information sharing is a major advantage of e-commerce over traditional business. (True/False)

Question XIII:

Output of ecommerce is _____ that helps organisation to work together.

1.5 Limitations of e-commerce

The main disadvantage of E-commerce is the lack of a business model, lack of trust and key public infrastructure, slow navigation on the internet, the high risk of buying unsatisfactory products and most of all lack of security. Besides various advantages of e-commerce, there are limitations also that can be divided into two parts:-

Non Technical Limitations

These are limitations that are more difficult to change like people's attitude, lack of trust, resistance to change, faceless transactions, etc. They are not related to the technology.

Technical Limitations

These are related to the technology and that can be solved (most of the time) by spending money. They are related to security, databases, standards, applications etc. These limitations are discussed below.

a) Costs

Expenses related to hardware/software, setup cost, connection cost, maintenance and enhancement cost of the website has to be borne in the initial stage. Such costs are besides the cost of the product.

b) Security

A primary concern without which it is difficult to sustain in e-market is e-security. It aims at preventing unauthorized access to the data/information travelling on the internet. The protection needs to be taken from the hacker, viruses, data transfer and transaction risk, client and server risk. Internet provides universal access but companies must protect their assets from accidental or malicious use. Customer information needs to be protected from internal and external misuse. Further sufficient security should be available for financial transactions. E-Payments are made without any loss of time but security is to be insured when using this system because customers are sending their personal detail related to credit card numbers.

Self-Check Exercise

Question XIV:

Lack of business model, lack of trust is main disadvantage of _____.

Question XV:

Cost and security comes under _____ limitations.

Summary

Buying and selling of product and services is termed as Ecommerce.

E-commerce is execution of any financial transaction with the use of network. B2B, B2C, C2C are different forms of E-commerce and also Known as different Business Models. Internet is treated as a functional and operational medium for consumers, business owners, information seekers and entrepreneurs. Besides various advantages of e-commerce, there are technical and non-technical limitations.

Glossary

- Electronic Commerce (E-Commerce)
- Electronic Data Exchange (EDI)
- Electronic Fund Transfer (EFD)
- Business to Business (B2B)
- Business to Consumer (B2C)
- Consumer to Business (C2B)
- Consumer to Consumer (C2C)
- Mobile Commerce (m-commerce)
- Digital Commerce (d-commerce)
- Personal Digital Assistants (PDA’s)

Questions

Q.1. Define e-commerce.

Q.2. Give examples of e-commerce in B2B, B2C and C2C scenario.

Q.3. Differentiate between d-commerce and m-commerce.

Q.4. Explain business applications of e-commerce.

Q.5. Discuss limitations of e-commerce.

Q.6. Describe the benefits of e-commerce.

Q.7. Mention how e-commerce is beneficial to the society.

Q.8. Give some examples of the use of e-commerce.

Q.9. What are the various e-commerce applications related to wholesale.

Q.10. List the ways of exchange of business information in e-commerce.

Answers to Self check exercise

Question I: True

Question II: Person to Person Transaction

Question III: True

Question IV: Manufacturing

Question V: Wholesale

Question VI: True

Question VII: Marketing

Question VIII: True

Question IX: True

Question X: False

Question XI: Technology

Question XII: True

Question XIII: Teamwork

Question XIV: Ecommerce

Question XV: Technical

Chapter 2

BUSINESS MODELS IN E-COMMERCE

Objectives:

- Introduction
- Comparison with traditional commerce
- Business models

2.1 Introduction

Nowadays ecommerce has become very popular among the people who want to buy and sell different things because of the convenience it offers and the cost benefits to retails and the cost saving to the customer and also the secrecy it offers.

First thing first, when you ask yourself, “What is e-commerce?” The best way to begin to describe different ecommerce businesses and the different types of ecommerce businesses is to break them down into the types of ecommerce business model that exist.

Ecommerce business models can be differentiated into **three** main categories:

- What type of product are sold
- Who the product are sold to
- Where the product are sold on

2.2 Comparison with traditional commerce

Due to the increased popularity and availability of internet access many traditional small business are considering e-commerce as a valid and profitable sales channel. However, e-commerce and traditional commerce are different from each other.

1. Direct interaction

Traditional commerce is often based around face to face interaction. The customer has a chance to ask questions and the sales staff can work with them to ensure a satisfactory transaction. Often this gives sales staff an opportunity for up selling, or encourages the client to buy a more expensive item or related items, increasing the shop profits. On the other hand, e-commerce doesn't offer this benefit unless features such as related items or live chats are implemented. Generally, in e-commerce the customer buys the product without any interaction with the seller. The product is selected based on the images and specifications displayed on the website.

2. Lower costs

E-Commerce is usually much cheaper than maintaining a physical store in an equally popular location. Compared with costs such as commercial space rent, opening an online store is much cheaper than the physical store. This can prove invaluable for small business owners who don't have the start up capital to rent prime retail space and staff it to be able to sell their goods.

3. Reach

With an online shop you can do business with anybody who has access to internet. In e-commerce the customers are those who are willing to access websites, send mail to place an order and make payment using e-banking facility leads to ecommerce. In traditional commerce the customers are limited to only those who visit the shop for the purpose of shopping. E-Commerce opens the door to many other forms of marketing that can be implemented entirely online, which often results in a much larger volume of sales. An online store has no capability limits and you can have as many clients as

your stock can serve. Whereas, in traditional commerce the seller has access to customers of nearby places.

4. Returns rate

In a traditional store, the customer will be purchasing the product in person, which has some benefits for both him and the store. The customer will be able to touch and check the items, to make sure they are suitable and even try them on, which reduces the number of returned items or complaints due to an item not being as advertised on a catalogue or promotional leaflet. Expect a significantly higher rate of returns if you start trading online, as many will just order and try the items at home and won't hesitate to return them as they can do it by post without having to talk with anybody in person.

5. Credit card fraud

The remote nature of e-commerce makes much more difficult to detect fraud, which means stores can lose money due to fraud. While traditional commerce is not totally secure, but it's easier for a sales attendant to verify that the person buying something is actually the owner of the credit card, by asking for photographic identity proof. However, the fight against card fraud is well underway. Banks and responsible e-commerce owners' are improving mechanisms to verify that all card use is legitimate.

6. Shopping time

In traditional shop the selling of product takes place during the period in which the shop is open. But in online shop the business timings are unlimited. The selling may take place 24/7 except the goods may at times be delivered in day time.

7. Research & Development

The seller in traditional shop spends most of its time in dealing with customers or waiting for the customers to walk in for purchases. On the contrary the seller may at times chat online with customers to handle their queries and finds no reason to waste time by waiting for the customers instead he may use ample time for research and development. The seller has time to focus on improving products and services.

8. Personnel

Traditional business needs to hire sales executive, sales managers, accountants and other staff for smooth functioning. However, in e-commerce personnel requirements are minimum. Web site managers, network administrators and system analyst are required by e-business.

9. Physical space

The traditional way requires location of shop either on rent or the shop has to be purchased. Further, the location of the shop needs to be in good locality. In newer mechanism only virtual cyber space is used for shopping. An office acting as a backup may be situated in a remote area.

10. Wider area of business

The traditional business acts in localized pools leading to no access of customers who need the product being sold by your organisation. The basis of a traditional business depends on the frequency of new and old customers buying from them to keep the business running. In modern business the customer and the seller may meet each other in a large cyber ocean.

11. Ordering of product

In e-commerce the stages of purchase are depicted as; it involves an agreement between the involved parties to continue with the succeeding phases. Order is made for the goods after an agreement is concluded. E-payment systems on the internet are used for receiving payments. Goods are delivered to the customers. If it is a tangible product, it is sent by transportation. However in traditional methodology, the product is selected and purchase of good involves giving cash and procuring the good.

12. Digital data

In e-commerce the order placed for the product is digital, the payment is made digitally and even the receipt is issued digitally. Hence, the data is digital.

13. Secure

Financial transactions on the internet can actually be more secure than in traditional retail environments.

14. Best deal

Consumers often associate online shopping with "deals" or lower prices, due to auction sites and easy cross-referencing via search engines. In addition, using the internet to purchase goods or services facilitates consumer competition because of greater accessibility. In other words, while consumers can visit only a few traditional outlets per day, they have access to countless web retailers in the same timeframe. Because of the ease of access to many retailers and greater opportunities for bargain-hunting, competition on the web is fierce. Price transparency is the rule. With shopping-comparison services, it is possible to check the price offered by hundreds of merchants with a couple of mouse clicks

15. Feedback

Online consumers have access to an unprecedented amount of product information, not just from manufacturers' websites but also from online reviews written by previous customers and employees.

16. Taxes

Differences also exist in terms of costs to consumers and retailers. For online consumers shipping is usually charged but not sales taxes but for the traditional consumers tax is levied based upon the state or whether a store front exists in the marketplace.

17. Pull & push methodology

Traditional commerce consists of marketing to reach potential customers, getting together with the customer in a place of business, agreeing on a sale and making the exchange of goods and money. Common marketing techniques used to reach potential customers include mailings, phone calls and advertisements. Then the buyer and/or the salesman are the active parties involved in a sale and exchange. In one case, the buyer initiates the purchase by either going to the store to buy or calling on the phone and making an order. In another situation, the salesman goes to the home or place of business to make the sale, or he calls on the phone to make the sale. A third method combines action from both parties. The business' sales department mails a catalogue or other material and the customer then makes a purchase from the catalogue.

These methods all apply to business-to-consumer (B2C) as well as business-to-business (B2B) sales.

In online commerce or the e-commerce, the seller uses e-marketing to reach potential customers. There are two forms of e-marketing: push-marketing and pull-marketing. Push marketing consists of sending out emails, as well as posting online advertisements on various websites. It is pushing information to the people. Pull-marketing is having a website where customers seek out information about your products. Social marketing is also used in pull-marketing.

The buying and selling is similar to the traditional mail order catalogue method, except that orders can be performed online from a website. The business' sales department posts a web site with an online catalogue. The buyer then selects items from the online catalogue and makes the purchase, either online or by phoning or mail order. A valid credit card is required to make a purchase. Although the buyer is really using an online catalogue, the metaphor of browsing a store with a shopping cart is often used in e-commerce. This allows the customer to put items in the shopping cart to hold until checkout or when the purchase is finally made.

These methods also apply to both B2C and B2B sales.

Self-check Exercise

Question I:

_____ is more secure than traditional retail environments.

Question II:

E-commerce offers face to face interaction. (True/False)

Question III:

E-commerce is much cheaper than traditional commerce. (True/False)

Question IV:

_____ has large reach in business.

Question V:

Is it difficult to detect fraud in E-commerce? (True/False)

Question VI:

We can shop anything anytime with online shop. (True/False)

Question VII:

In E-commerce the order placed for product is _____.

Question VIII:

Financial transaction on internet is more secure than in traditional retail environment. (True/False)

2.3 Business Models

For organisations to be a success, new innovative ideas and strategies need to be implemented. New business models are created to offer a new way to deliver value to customers in business models.

The definition for a business model comprises of architecture for the product, service and information flows, including a description of the various business actors and their roles and also a description of the potential benefits for the various business actors and description of the sources of revenues. Another definition of business model is "a unique configuration of elements comprising the organisation's goals, strategies, processes, technologies and structure, conceived to create value for the customers and thus compete successfully in a particular market."

Some of the business models are as follows:

1. E-shop

It is a business model according to which individual shops sell various goods online. This is web marketing of a company or a shop. In first instance this is done to promote the company and its goods or services. Increasingly added is the possibility to order and possibly to pay, often combined with traditional marketing channels. Benefits sought for the company are increased demand, a low-cost route to global presence and cost-reduction of promotion and sales. Benefits for the customers can be lower prices compared to the traditional offer, wider choice, better information and convenience of selecting, buying and delivery, including 24-hour availability. Where repeat visits to the e-shop are done, one-to-one marketing can increase those benefits for both seller and buyer. Seller revenues are from reduced cost, increased sales and possibly advertising. Most commercial Web sites are business-to-consumer electronic shops, selling for example flowers, electronic goods, garments, books, tickets and many more products for sale.

Website following B2C business model sells its product directly to a customer. A customer can view products shown on the website of business organization. The customer can choose a product and

order the same. Website will send a notification to the business organization via email and organization will dispatch the product/goods to the customer.

A collection of e-shops under a common umbrella giving entry to individual e-shop gives space to another business model called e-mall.

2. E-procurement

This is electronic tendering and procurement of goods and services. Large companies or public authorities implement some form of e-procurement on the web. Benefits sought are to have a wider choice of suppliers which is expected to lead to lower cost, better quality, improved delivery, reduced cost of procurement (e.g. tendering specifications are downloaded by suppliers rather than mailed by post). Electronic negotiation and contracting and possibly collaborative work in specification can further enhance time- and cost saving and convenience. For suppliers the benefits are in more tendering opportunities, possibly on a global scale, lower cost of submitting a tender and possibly tendering in parts which may be better suited for smaller enterprises, or collaborative tendering (if the e-procurement site supports forms of collaboration). The main source of income is reduction of cost (automated tender processing, more cost-effective offers).

Website following B2B business model sells its product to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to final customer who comes to buy the product at wholesaler's retail outlet.

3. E-auctions

Electronic auctions (on the Internet) offer an electronic implementation of the bidding mechanism also known from traditional auctions. This can be accompanied by multimedia presentation of the goods. Usually they are not restricted to this single function. They may also offer integration of the bidding process with contracting, payments and delivery. The sources of income for the auction provider are in selling the technology platform, in transaction fees and in advertising. Benefits for suppliers and buyers are increased efficiency and time-savings, no need for physical transport until the deal has been established, global sourcing. Because of the lower cost it becomes feasible to also offer for sale small quantities of low value, e.g. surplus goods. Sources of income for suppliers are in reduced surplus stock, better utilisation of production capacity, lower sales overheads. Sources of income for buyers are in reduced purchasing overhead cost and reduced cost of goods or services purchased. Hence, it automates the traditional bidding process over the internet. They can also additionally support contracting, payments and delivery processes.

4. Value-chain integrators

These focus on integrating multiple steps of the value chain, with the potential to exploit the information flow between those steps as further added value. Revenues are generated from consultancy fees or possibly transaction fees. Some of the 3rd party marketplace providers are moving into the direction of value chain integration.

Internet is used to improve communication and collaboration between all parties within a chain. Value chain integration is necessary if vendors are to coordinate between suppliers and customers effectively. A set or sequences of activities are performed to produce the product. The links between the activities provide a prime opportunity for competitive advantage, whether due to exceptional efficiency or some form of product differentiation. This chain of partners that work in collaboration to create market and move products and services are complex. Based on the sorts of intimate trading relationships central to the integrated value chain model, modern business partnerships are eradicating duplication, irrelevant hand offs and rework, ensuring that processes run smoothly and effectively.

5. Information brokerage and trust

A whole range of new information services are emerging, to add value to the huge amounts of data available on the open networks or coming from integrated business operations, such as information search, e.g. search engines, customer profiling, business opportunities brokerage, investment advice, etc. Usually information and consultancy have to be directly paid for either through subscription or on a pay-per-use basis, although advertising schemes are also conceivable. A special category is trust services, as provided by certification authorities and electronic notaries and other trusted third parties. Subscription fees combined with one-off service fees as well as software sales and consultancy are the sources of revenue. Many consultancy and market research companies are now offering commercial business information services via the internet. Search engines are a special category of information services, with the public internet facility (rather than intranet versions) usually based on advertising as a source of revenue.

6. Collaboration platforms

These provide a set of tools and an information environment for collaboration between enterprises. This can focus on specific functions, such as collaborative design and engineering, or in providing project support with a virtual team of consultants. Business opportunities are in managing the platform (membership/usage fees) and in selling the specialist tools (e.g. for design, workflow, document management).

7. Third-party marketplace

This is an emerging model that is suitable in case companies wish to leave the web marketing to a 3rd party (possibly as an add-on to their other channels). They all have in common that they offer at least a user interface to the suppliers' product catalogues. Several additional features like branding, payment, logistics, ordering and ultimately the full scale of secure transactions are added to 3rd party marketplaces. An example for business-to-consumers is to provide a common marketing for a special event profiled by well-known brand names. ISPs may be interested in this model for business-to-business, using their web builder expertise. However, it may equally appeal to banks or other value chain service providers. Revenues can be generated on the basis of one-off membership fee, service fees, transaction fee, or percentage on transaction value.

A classification was provided for business models in internet electronic commerce (business-to-business as well as business-to-consumer). Some of these models are essentially an electronic re-implementation of traditional forms of doing business, such as e-shops. Many others go far beyond traditional business such as value chain integration and seek innovative ways to add value through information management and a rich functionality. Creating these new business models is feasible only because of the openness and connectivity of the Internet

8. Telecommunications

Telecommunication is communication at a distance by technological means, particularly through electrical signals or electromagnetic waves. The network of telecommunications is used for sending and receiving data for the purpose of sale and purchase of goods. The telecommunication network is used by internet and fax for transmitting signals. Audio signals, video signals and text is sent on an established network. However, it is up to the user whether the transmitted data is for sale, query, order, quotation or payment details.

Self-check Exercise

Question IX:

Production of product is performed by_____.

Question X:

Lower cost of tendering is better suited for small enterprises? (True/False)

Summary

Business Model is the mechanism by which business will deliver and receive value from customers. The business model can form the basis of a business plan. The business model however is designed to be more fluid tool that mole and changes with the development of the business (more efficiently than a business plan).

Glossary

- Face to Face Interaction
- E-banking
- Photographic Identity Proof (PIP)
- Website Managers
- Network Administrators
- System Analyst
- Virtual Cyber Space
- Bargain Hunting
- Seller Revenue
- E-procurement
- E-shop
- Global Sourcing

Questions

Q.1 In a tabular form differentiate between traditional commerce and e-commerce.

Q.2 What do you understand by business model.

Q.3 How is e-shop different from a shop.

Q.4 Explain the e-procurement model.

Q.5 Give examples to describe e-auction.

Q.6 Write a note on collaboration platform.

Q.7 Why is information available in abundance in the digital world.

Q.8 Describe the model value chain integrator.

Q.9 Explain the concept of pull and push methodology.

Q.10. How come in e-commerce the customer is able to get the best deal.

Answers to Self check Exercise

Question I: Financial Transactions

Question II: False

Question III: True

Question IV: Ecommerce

Question V: True

Question VI: True

Question VII: Digital

Question VIII: True

Question IX: Sequence of activities

Question X: True

Chapter 3

ELECTRONIC PAYMENT SYSTEM

Objectives:

- Introduction
- Definition
- Entities
- Phases in e-payment
- Classification of Payment Systems
- Payment schemes
- Offline and Online

3.1 Introduction

The ease of purchasing and selling products over the internet has helped the growth of electronic commerce and electronic payments services are a convenient and efficient way to perform financial transactions. Current e-payment technologies depend on using traditional methods that are common to non-electronic systems. Due to the nature of internet, security and authenticity of payments and participants cannot be guaranteed with technologies that are not specifically designed for electronic commerce. We need an e-payment system that would not only provide secure payments but should also have properties like online customer and merchant authentication, un-forgeable proof of transaction authorisation by the customer both to the merchant and the bank, privacy of customer and transaction data. This chapter provides an overview of e-payment architecture and their functionalities, their requirements and verification of payment protocols.

3.2 Definition

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

E-payment is a subset of an e-commerce transaction to include electronic payment for buying and selling goods or services offered through the internet. Generally we think of electronic payments as referring to online transactions on the internet, there are actually many forms of electronic payments. As technology developing, the range of devices and processes to transact electronically continues to increase while the percentage of cash and check transactions continues to decrease.

E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. It is user friendly and less time consuming than manual processing, helps business organization to expand its market reach / expansion.

Self-check Exercise

Question I:

Ecommerce payment system is also known as _____.

3.3. Entities

Electronic payments involve a payer and a payee. A payer (buyer or customer), is an entity who makes a payment. A payee (seller or merchant), is an entity who receives a payment. The main purpose of an electronic payment protocols is to transfer monetary value from the payer to the payee. The process

also involves a financial institution (bank). Typically, financial institution participates in payment protocols in two roles: as an issuer (interacting with the payer) and as an acquirer (interacting with the payee). The issuer is responsible for validating the payer during account registrations and holds the payer's account and assets. The acquirer holds the payee's account and assets. The payee deposits the payments received during a transaction with the acquirer. The acquirer and the issuer then proceed to perform an inter-banking transaction for clearance of funds. It is possible for the issuer and the acquirer to be from the same financial institution. Other parties that may be present in a payment protocol include a trustee (arbiter) who is an entity that is independent from all parties. All entities in a protocol unconditionally trust the Trustee who is called to adjudicate any disputes between the payer and the payee. Certain payment systems might involve more players like Payment Gateways (PG) who are entities that act as a medium for transaction processing between other entities (e.g. MasterCard, Visa) and Certification Authorities (CA). They issue public key certificates to entities involved in a payment protocol so that their authenticity can be publicly verified. Figure 1 illustrates the participating entities in an e-payment system.

Self-check Exercise

Question II:

Electronic payments involve _____ and _____.

3.4. Phases in E-Payment

An electronic payment typically involves the following phases:

1. Registration: This phase involves the registration of the payer and the payee with the issuer and acquirer respectively. Most electronic payments designed require registration of payers and payees with their corresponding banks so there is a link between their identities and their accounts held at the bank.

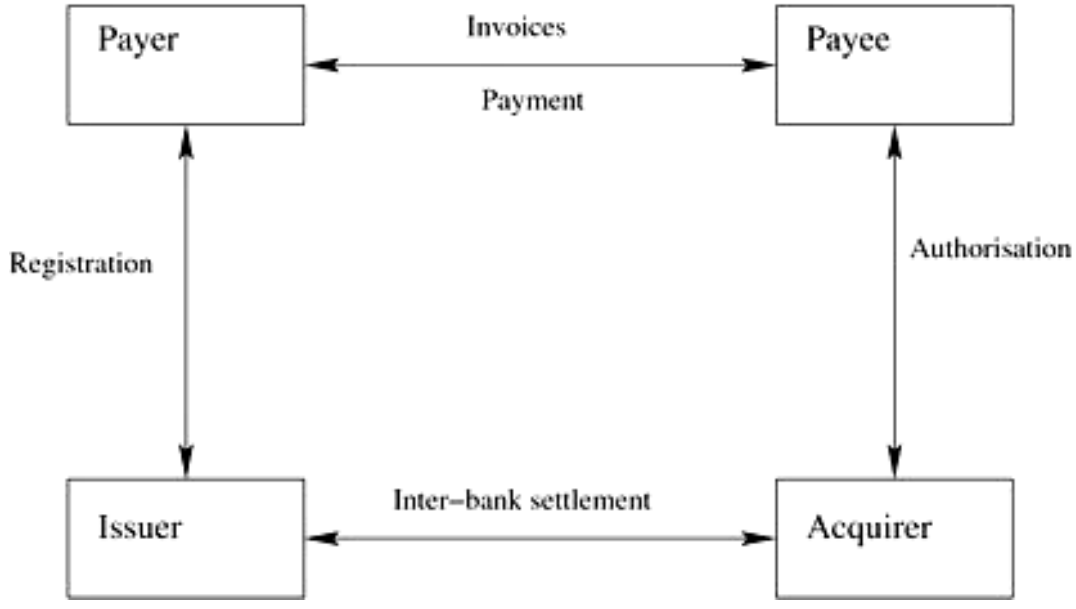

Figure 3.1: Generic E-payment Protocol

2. Invoicing: In this phase, the payee obtains an invoice for payment from the payee. This is accomplished by either browsing and selecting products for purchase from the merchant's (payee's) website in case of purchases made through the internet or obtaining an electronic invoice using other electronic communication medium like e-mail. This phase typically is performed in an unsecured environment and normally excluded while designing payment protocols. The importance of this phase is that, it sets the mandatory and optional data variables that should be included in a payment protocol.

3. Payment selection and processing: In this phase the payer selects type of payment, (card based, e-cash, e-cheque, etc.,) based on the type of payment the payee accepts. Based on the selection, the payer then sends the relevant payment details like account number, unique identifiers of the payer to the payee along with accepted amount based on the invoice. Certain protocols might also require the payer to obtain preauthorised token (like bank drafts) from the issuer before the payer sending the payment information to the payee.
4. Payment authorisation and confirmation: In this phase, the acquirer on receiving payment details from the payee authorises the payment and issues a receipt containing the success or failure of the payment to the payee. The payee based on the message may also issue a receipt of payment to the payer.

Self -Check Exercise

Question III:

An Electronic Payment typically involves _____ Phases.

Question IV:

_____ Phase is performed in an unsecured environment.

3.5. Classification of Payment Systems

Electronic commerce can be broadly categorised into groups, business-to-business (B2B), business to consumer (B2C) and consumer to consumer (C2C). B2B normally involve higher value transactions and predominant payment methods are electronic cheques and bank transfers, whereas, B2C and C2C payments are lower value transactions and payment methods used are cash and card based payment systems.

Payment instruments: There are three common electronic payment instruments, namely cash, cheque and card. Cash payment systems consist of self-authenticating divisible tokens that can be processed offline. Cheque payment system is typically linked to a payer's account and payment is indivisible. Card payment schemes provide a payment mechanism through the existing credit card payment infrastructure.

Self -Check Exercise

Question V:

B2B involves Lower Value Transaction whereas B2C and C2C payments involve Higher Value Transaction. (True/False)

3.6. Payment schemes.

The payment can be made based on different schemes namely pre-paid, pay-now and post-pay. In pre-paid system the payment is debited from the payer's account before a payment is processed and hence the term "pre-paid". Most cash-less systems such as an electronic-cash system fall in this category. In pay-now system, when an electronic transaction is processed, the payer's account is debited and the payee's account is credited with the payment amount. Even though availability of funds depends on the time when inter-bank settlements are carried out, the payer's and payee's account are updated to show the debited and credited balances immediately after an transaction is carried out. Credit card based system, like Secure Electronic Transaction (SET), Verified by Visa (VBV), MasterCard secure-code fall into this category. In post-pay systems the payer's account is debited only when the payee's makes a request for payment settlement with the acquirer. Most cheque based systems fall into this category.

Some of the modes of electronic payments are following.

- Credit Card
- Debit Card
- Smart Card

- E-Money
- Electronic Fund Transfer (EFT)
- Cyber wallet
- Prepaid - Cash like system
- Pay later or Cheque based system
- Micropayments
- Mobile Payments
- PayPal
- Google Wallet

Credit Card

The most common method for “on-line” payment is card-based systems. Most payment systems in this category are specifically designed for transaction conducted through the internet. Because of their convenience and omnipresent nature, credit cards in particular have become a popular method for conducting online payments over the internet, but they are insecure, offer no anonymity or protection of payer’s payment information like card details and account information. To overcome these drawbacks and make card payment more secure, the two leading credit card companies VISA and MasterCard have developed various protocols.

There are two major proposals for secure electronic payment over the internet. They are Visa 3-D Secure (Verified by Visa - VBV) and MasterCard SecureCode. Both protocols rely on SSL /TLS to encrypt communication over the internet. SSL is a client-server protocol that uses public key cryptography and has become the de facto standard for encrypted communication over the internet. In SSL, only servers (merchants) have public key certificates and clients (buyers) remain anonymous to the servers. SSL protocol, has implemented a standard that would allow merchant to incorporate the proposed security features into their payment acceptance structure.

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

- The card holder - Customer
- The merchant - seller of product who can accept credit card payments.
- The card issuer bank - card holder's bank
- The acquirer bank - the merchant's bank
- The card brand - for example , visa or mastercard.

Credit card payment process

Step	Description
Step 1	Bank issues and activates a credit card to customer on his/her request.
Step 2	Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service.

Step 3	Merchant validates customer's identity by asking for approval from card brand company.
Step 4	Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service chargers paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7	Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company.

Debit Card

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed. Whereas, in case of credit card there is no such compulsion of having a bank account or having balance in the account. Debit cards liberate customer to carry cash, cheques and even merchants accepts debit card. Having restriction on amount being in bank account also helps customer to keep a check on his/her expenses.

Smart Card

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage. Smart card can be accessed only using a Personal Identification Number (PIN) of customer. Smart cards are secure as they stores information in encrypted format and are less expensive/provide faster processing. Mondex and Visa Cash cards are examples of smart cards.

E-Money

E-Money transactions refer to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time.

Online payments done via credit card, debit card or smart card are examples of e-money transactions.

Electronic Fund Transfer

It is a popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer.

Internet based EFT is gaining popularity. It does not involve any sort of physical card. It is used by customers who have accounts enabled with internet banking feature. In this case, customer uses website provided by the bank. Customer logins to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers amount to other account if it is in same bank otherwise transfer request is forwarded to ACH (Automated Clearing House) to transfer amount to other account and amount is deducted from

customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank. It is also called as net banking.

Cyber Wallet

A cyber wallet in the form of stored and protected account information, which may be "carried" on a tamper resistant portable electronic storage medium such as a smartcard, or stored on the customer's computer (or personal digital assistant, PCMCIA card, or the like) together with the browser/mosaic software, is provide to a customer for the purpose of making electronic payments from the possessor of the wallet to a merchant at a remote site on the internet. Security of the information contained in the wallet is provided by a public key file containing public keys to be used for encrypting the payment information into an authorization ticket which is sent by the wallet to the merchant and then forwarded to the account servicer for decryption, the decryption key being in the form or a private key held only by the account servicer and to which the merchant and other parties have no access. The public key rile preferably contains a plurality or public keys selectable by an identifier associated with but not a part of the key itself, so that the account servicer can control, by having the merchant send an identifier to the wallet, the selection of uncompromised keys without anyone but the servicer having knowledge of which key is being selected.

Prepaid - Cash like system

The best-known subclass in pre-paid systems is the anonymous e-cash system.

Basic model of e-cash system: An anonymous off-line e-cash consists of three probabilistic, polynomially-bounded parties, a bank B, payer P and payee R and three main sub protocols: withdrawal, payment and deposit (refer Figure 2). Payer and payee maintain their accounts with the bank. The payer withdraws electronic coins from their account with the bank, by performing a withdrawal protocol over an authenticated channel. The payer spends coins by participating in a payment protocol with the payee over an anonymous channel. In effect, the payee performs a deposit protocol, to deposit the coins into their account. The e-cash system also includes setup protocols: system setup, payer setup and payee setup which performs system initialisation functions, namely creating and publishing public keys and opening payer and payee bank accounts.

Pay later or Cheque based system

Customers generally tend to use credit card payment methods for low and middle value payments, whereas, cheque is the preferred method for large value payments. Various electronic cheque (e-cheque) protocols have been proposed over the years. Systems like FSTC’s eCheck, NetCheque and MANDATE II are based on methods used in traditional paper based checking protocols. Systems like NetBill, ECheque and PayNow by CyberCash use a central server. Other e-cheque systems are based on modified versions of e-cash protocols. But most promising of all e-cheque system that has the support of major financial institutions and government agencies has been the FSTC’s e-cheque system.

Micropayments

One of the most promising payment methods is the use of micro payments: the ability to pay for data or services in small increments.

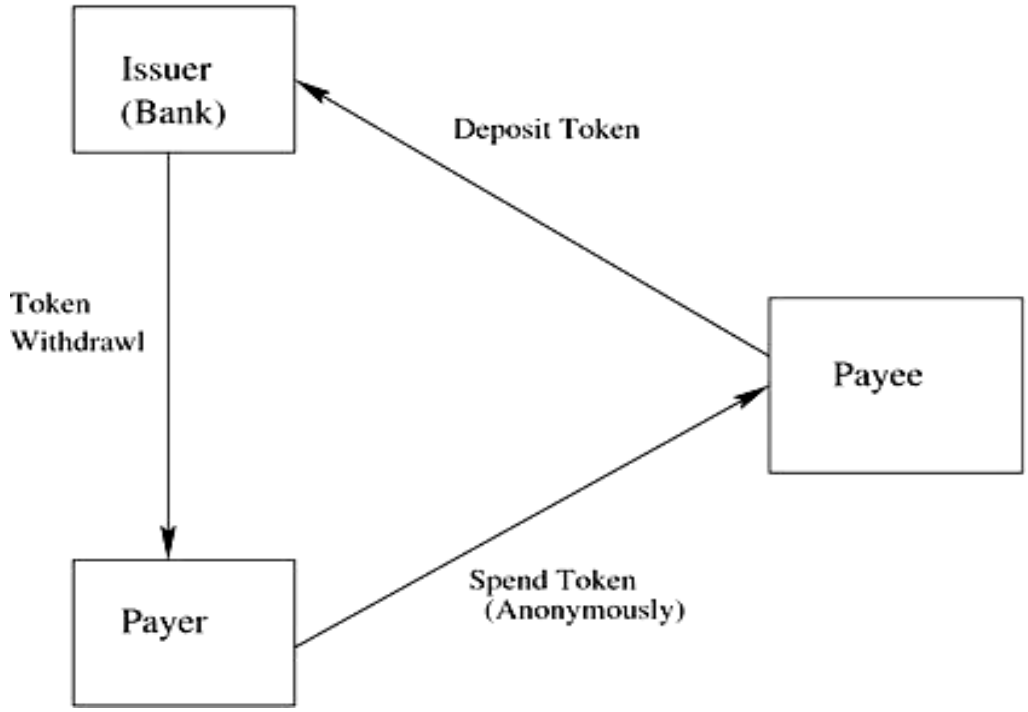

Figure 3.2: A Model E-cash system

Micro payments can be seen as a solution to allow low-value payments for purchasing news articles, stock quotes, index queries, per-click purchase and other services over the internet. The primary aim of micro payment system has been to handle arbitrarily small amounts of money and keep the cost for the individual transaction low along with generic e-payment security requirements like confidentiality, integrity, authentication and non-repudiation.

Mobile Payments

Due to the phenomenal success of mobile communicational devices, there has been increasing effort to used mobile devices as “electronic wallets” to store payment and account information. Currently two main wireless protocols are used for mobile commerce. WAP (Wireless Application Protocol) developed by WAP forum (consolidated into the Open Mobile Alliance) and i-Mode developed by NTT DoCoMo, Japan. WAP is an open and global specification that helps mobile devices with WAP enabled browsers to access information and services. WAP specifications include an XML-type markup language known as Wireless Markup Language (WML) for displaying information on to a mobile device browser. The WAP specifications also include a lightweight protocol stack to reduce bandwidth requirements. I-mode is a proprietary protocol developed by NTT DoCoMo and uses Personal Digital Cellular-Packet (PDC-P) to provide network services. I-mode allows efficient network usage by using packet switching technology for wireless communication and TCP/IP for wired communications. I-mode uses c-HTML (compact-HTML) to display content on mobile devices. I-mode enabled devices are also view HTML web pages as the structure of c-HTML is similar to HTML as compared to WAP where HTML needs to be converted to WML for display. Both WAP and I-mode provide security features that can be used to provide electronic commerce and electronic payment services.

PayPal

PayPal is a global e-commerce business allowing payments and money transfers to be made through the internet. Online money transfers serve as electronic alternatives to paying with traditional paper methods, such as cheque's and money orders. PayPal is an acquirer, a performing payment processing for online vendors, auction sites and other commercial users, for which it charges a fee. It may also charge a fee for receiving money, proportional to the amount received. The fees depend on the currency used, the payment option used, the country of the sender, the country of the recipient, the

amount sent and the recipient's account type. In addition, eBay purchases made by credit card through PayPal may incur extra fees if the buyer and seller use different currencies.

Google Wallet

Google Wallet was launched in 2011, serving a similar function as PayPal to facilitate payments and transfer money online. It provides the best feature of security and has the ability to send payments as attachments via email.

Self -Check Exercise

Question VI:

Electronic cash system falls in _____ category.

Question VII:

Credit/Debit cards are used for _____ payment.

Question VIII:

Fund transfer is done using _____ and _____.

Question IX:

Can we pay our money using mobile phone? (Yes/No)

Question X:

PayPal is _____.

3.7. Offline and Online

Based on communicational characteristics, electronic payments systems are classified as offline and online systems. In an offline system, the communication does not involve any third party, i.e., an electronic transaction takes place only between the payer and the payee. The advantages of offline payments are lower communication cost and less time-critical transaction handling at the banks. However, they suffer from one serious drawback, the problem of double spending. Double spending occurs when the payer spends the same electronic money multiple times. In a digital system the payer could make a backup of electronic money before each payment and reset his system to this backup after the payment. In this way, an arbitrary number of payments to different recipients are possible with the “same” money. Typically, double spending is prevented with the use of tamper-resistant hardware e.g. a smart card. In certain cases, the tamper-resistant hardware is issued by the bank containing a pre-authorised value of money. However tamper-resistant devices only offer limited protection as they are vulnerable to attacks. Another way to prevent double spending is pre-authorisation. The payer obtains pre-authorised secure digital money from its bank, thus the payee is assured of payment e.g. a bank cheque. However, this method can only be used if the payee is known to the payer before a payment. A weaker solution, rather than employing prevention techniques is to detect double spending when they occur and the dishonest payer can be held accountable. This solution is used in most e-cash implementations. Adequate security can be achieved by a combined approach that would involve both detection methods and tamper-resisted devices.

In an on-line system, the payee typically connects to the bank to obtain a payment authorisation, thus increasing the communication requirements for the payment system. The advantage is, the payee obtains a guarantee on the payment, as the bank is able to authorise and check for availability of funds in the payer’s account.

Self -Check Exercise

Question XI:

Does the payee obtain guarantee over payment? (True/False)

Summary

Electronic payment system: a means of making payments over electronic networks such as the Internet.

E-cash: Electronic financial transactions conducted in cyberspace via computer networks. Debit card: A payment card that deducts money directly from a consumer's checking account to pay directly for a purchase. Electronic Fund Transfer is a popular electronic payment method to transfer money from one bank account to another bank account. PayPal is a global e-commerce business allowing payments and money transfers to be made through the internet. Google Wallet provides the best feature of security and has the ability to send payments as attachments via email.

Glossary

- Security
- Authenticity
- Authorisation
- Monetary Transaction
- Certification Authority (CA)
- Invoicing
- Secure Electronic Transaction (SET)
- Public Key Cryptography
- SSL/TLS Protocols
- Personal Identification Number (PIN)
- Automated Clearing Housing (ACH)
- Personal Digital Cellular-Packet (PDC-P)

Questions

Q.1 Define electronic payment system.

Q.2 What do you understand by protocol, payee and payer.

Q.3 Discuss the different phases in e-payment.

Q.4 Explain the payments made by cards.

Q.5 Describe the electronic fund transfer.

Q.6 Define cyber wallet.

Q.7 Differentiate between offline and online payments.

Q.8 Explain the various pre paid and post paid payment schemes.

Q.9 Discuss the procedure of credit card usage.

Q.10 Which e-cheque system is supported by government agencies and why.

Answers to Self check Exercise

Question I: Electronic Data Interchange

Question II: Payee and Payer

Question III: 4

Question IV: Invoicing

Question V: False

Question VI: Cash-less system

Question VII: Online

Question VIII: ATM and Computer

Question IX: True

Question X: Ecommerce business

Question XI: True

Chapter 4

E-BANKING

Objectives:

- Introduction
- Concept
- Operations

4.1 Introduction

Electronic banking, also known as Electronic Funds Transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by cheque or cash.

4.2 Concept

E-Banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a Personal Computer (PC), Personal Digital Assistant (PDA), Automated Teller Machine (ATM), kiosk, or Touch Tone telephone. While the risks and controls are similar for the various e-banking access channels.

In other words, **Online banking** is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual ban, credit union or building society. Online banking is also referred as **internet banking**, **e-banking** and **virtual banking**.

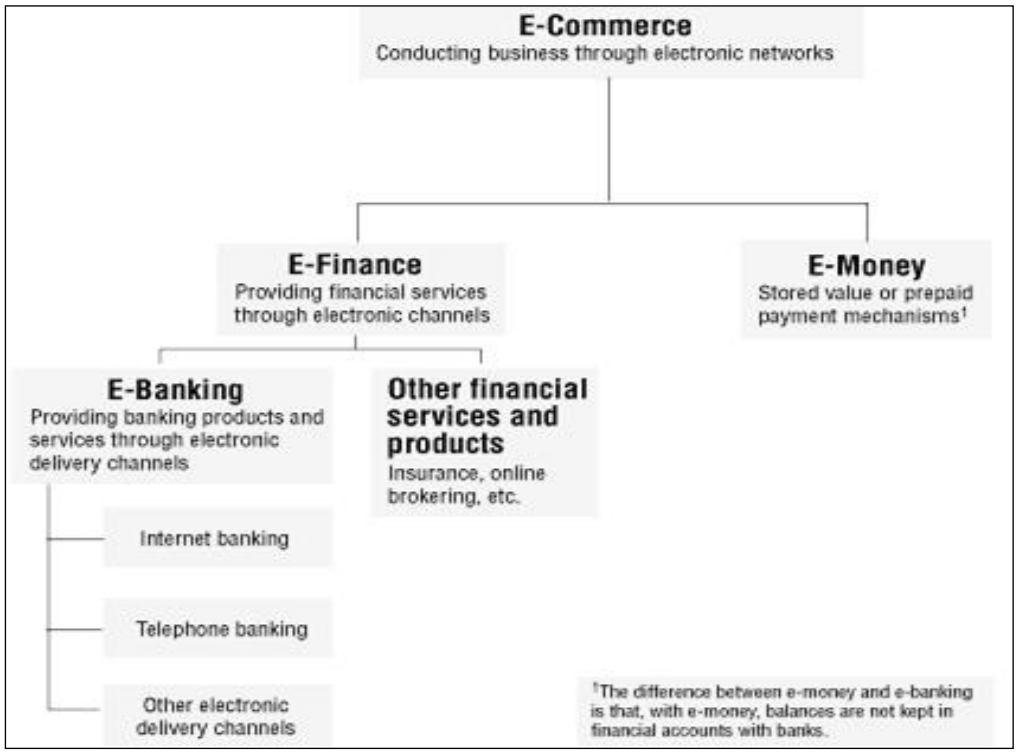

Figure 4.1: E-banking vs E-commerce.

Web Banking or Internet Banking is a term used to describe banking transactions that are performed via a secured internet application.

To access a financial institution's online banking facility, a customer with internet access would need to register with the institution for the service and set up some password for customer verification. The

password for online banking is normally not the same as for telephone banking. Customers' numbers are normally not the same as account numbers, because a number of customer accounts can be linked to one customer number. The customer can link to the customer number any account which the customer controls, which may be cheque, savings, loan, credit card and other accounts. Customer numbers will also not be the same as any debit or credit card issued by the financial institution to the customer. To access online banking, a customer would go to the financial institution's secured website and enter the online banking feature using the customer number and password previously setup. Some financial institutions have set up additional security steps for access to online banking, but there is no consistency to the approach adopted.

Electronic funds transfer can be used to:

- have pay cheque deposited directly into the bank
- withdraw money from bank account from an ATM machine with a Personal Identification Number (PIN), at any time.
- instruct bank to automatically pay certain monthly bills from bank account, such as auto loan or mortgage payment.
- have the bank transfer funds each month from bank account to the mutual fund account.
- have government social security benefits cheques or tax refund deposited directly into your bank account.
- buy groceries, gasoline and other purchases at the point-of-sale, using a card rather than cash, credit or a personal cheque.
- use a smart card with a prepaid amount of money embedded in it for use instead of cash at a pay phone, expressway road toll, or on college campuses at the library's photocopy machine or bookstores.
- use computer and personal finance software to coordinate your total personal financial management process, integrating data and activities related to income, spending, saving, investing, recordkeeping, bill-paying and taxes, along with basic financial analysis and decision making.

Thereby, e-banking transactions include paying bills, transferring funds, viewing account statements and paying down loans and mortgages. Hence, its popularity is expected to grow rapidly as internet usage grows internationally and people discover the many advantages that it provides.

Thus, electronic banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. Therefore transactions related to bank activities via Electronic Mean and medium is called electronic Banking.

A Virtual Bank is one that does business by phone and over the web but does not have a "brick and mortar" presence. Because virtual banks don't require high-end office towers in major cities or hundreds of bank branches in residential communities, they are able to pay their customers higher rates of return on deposits and provide mortgages and loans at highly competitive rates. Although most banking transactions occur electronically, there is always a need for customers to deposit cheques and obtain cash. Virtual banks leverage the existing banking network of ATM machines around the world to accept cheques and provide cash.

Self-Check Exercise

Question I:

Sometime Online Banking is also called_____.

Question II:

Password of telephone banking and online banking is same (True/False).

Question III:

A transaction related to banking via Electronic medium is called _____.

4.3 Operations

Operations of E-banking can be classified into numerous sections.

1. Telephone Banking
2. Online fund transfer or Internet Banking or Online Banking
3. RTGS
4. ATM

1. Telephone banking

Telephone banking is a service provided by a financial institution that enables customers of the financial institution to perform financial transactions over the telephone, without the need to visit a bank branch or automated teller machine. Telephone banking times can be longer than branch opening times and some financial institutions offer the service on a 24 hour basis. From the bank's point of view, telephone banking reduces the cost of handling transactions by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions.

Condition & Regulation: To use the benefits of telephone banking the common condition & Regulation are:

- Customer must first register with the institution for the service.
- Set up password for customer verification.

Process of Servicing: To access telephone banking

- The customer would call the special phone number set up by the financial institution
- Enter on the keypad the customer number and password.
- There could be more steps for security for automated systems to secure customer accounts or specific question to answer pre-determined by customer.
- If the customer is validated positive, then the customer requests for the transaction to teller.
- The request could be to enquire the balance amount in the account or it could be to know the details of the last few transactions or it could be to transfer the amount to another bank account or it could be to demand for a cheque book to be sent via post.
- The teller in response executes the request. However, the cash cannot be provided through telephone banking. But some banks provide cash at the door step of the customer for which the request was made through a telephone call. Though the cash requested for should be of at least some pre decided value.

2. Online fund transfer or Online banking or Internet banking allows customers of a financial institution to conduct financial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union or society. Online fund transfer was introduced in 1980's gradually it has become popular. Presently all standardised banks are providing the facility of internet banking to its customers. It may include any transactions related to online usage.

The Internet Banking Concept: There are two concepts of Internet banking: First, a bank that only exists on the internet and has no offices. In this case the operations are conducted exclusively over the Internet. Second, banks whose offices are physically present and have a distribution channel for products and services operating on the internet.

Condition & Regulation: To access a financial institution's online banking facility:

- Personal Computer or Online Banking Services Compatible Handset

- Personal Internet access
- Registration with the institution for the service
- Set up some password for customer verification

Process: To access online banking,

- Visit financial institution's website. It contains information about the main products and services being offered. A menu of options through links, which are sections of text or image are visible which when clicked by the user, transfers to new areas within the site.
- Enter the online banking facility using the customer number and password.
- There may be additional security steps for access like the customer answering to some pre defined questions. The answers are matched with the earlier stored responses for verification of the customer.
- The valid customer is to the area of transactions, secure site format, i.e. where the information is encrypted during transmission to prevent third party access. This is where the user may make inquiries to their accounts or perform any transactions.

The three broad facilities that e-banking offers are:

- Convenience- Complete your banking at your convenience in the comfort of your home.
- No more Qs- There are no queues at an online bank.
- 24x7 service- Bank online services is provided 24 hours a day, 7 days a week and 52 weeks a year.
- Later, on the completion of the transactions the user needs to log out. Logging out stops further financial transactions. In other words, it discontinues the access to the website.

Description of services: In the Internet banking services you can perform almost all operations can be done in a real office, except deposit or withdraw cash. However, some banks are already working on the design of alternatives, such as smart cards employing a microchip to recharge funds through special devices on the computer and could replace the use of small bills denomination through its acceptance in the trade.

Funds can be transferred from one account to another. Provided sufficient fund is available in the account before the transfer. The bank account number of the beneficiary should be known, as it is required to be specified during the course of the transaction. Also the IFSC code of the beneficiary's bank needs to be given. The beneficiary bank may or may not be of the same banking group. The fund transfer is immediate. Of course the amount of money to be transferred has to be mentioned. By logging into the online banking site the user can only send the fund and shall not be able to create a transaction for receiving the money.

Another activity which can be performed online is requesting for cheque book to be delivered in physical form via post or courier.

Log of the earlier executed transactions into the account can be seen or printed.

The password used to access the account can be changed. Some banks make it mandatory for the customer to change the password after every pre decided period which could be few months of time. The passwords are changed to reduce the chance of password hacking.

It provides enormous benefits to consumers in terms of the ease and cost of transactions. But it also poses new challenges for country authorities in regulating and supervising the financial system and in designing and implementing macroeconomic policy.

Challenges in adoption of E-banking: E-banking is facing following challenges banking industry:

- The most serious threat faced by e-banking is that it is not safe and secure all the time. There may be loss of data due to technical defaults.
- E-banks are facing business challenges. For the transactions made through internet, the service charges are very low. Unless a large number of transactions are routed over the web the e-banks cannot think of profit.
- There is lack of preparedness both on part of banks and customers in the adoption of new technological changes.
- There is lack of proper infrastructure for the installation of e-delivery channels

3. RTGS:

Real Time Gross Settlement systems (RTGS) are specialist funds transfer systems where transfer of money or securities takes place from one bank to another on a "real time" and on "gross" basis. Settlement in "real time" means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. "Gross settlement" means the transaction is settled on one to one basis without bundling or netting with any other transaction. Once processed, payments are final and irrevocable.

RTGS systems are typically used for high-value transactions that require immediate clearing. In some countries the RTGS systems may be the only way to get same day cleared funds and so may be used when payments need to be settled urgently such as when purchasing a house. However most regular payments would not use a RTGS system, but instead would use a national payment system or network that allows participants to batch and net payments. The RTGS system is primarily meant for large value transactions. Banks generally fix some range of value for RTGS transfer amount. Also some banks levy RTGS charges. The RTGS transactions can even be scheduled in advance. RTGS transactions can be as cash management transfer, hedging, interest, loan, securities, supplier payment, tax payment, trade, trade settlement payment, value added tax payment etc.

In RTGS system, transactions are settled across accounts held at a central bank on a continuous gross basis. Settlement is immediate, final and irrevocable. Credit risks due to settlement lags are eliminated.

However RTGS is different from NEFT. NEFT is an electronic fund transfer system that operates on a Deferred Net Settlement (DNS) basis which settles transactions in batches. In DNS, the settlement takes place with all transactions received till the particular cut-off time. These transactions are netted (payable and receivables) in NEFT whereas in RTGS the transactions are settled individually. Any transaction initiated after a designated settlement time would have to wait till the next designated settlement time. Contrary to this, in the RTGS transactions are processed continuously throughout the RTGS business hours.

Transactions through Retail Electronic Payment Systems: - The electronic payment systems such as Electronic Clearing Service (ECS) credit and debit and National Electronic Fund Transfer (NEFT) have improved the speed of financial transactions across the country. Electronic Clearing Service (ECS) is one of the new electronic banking services. ECS is a non-paper based movement of funds which is encouraged by the RBI on a wide scale. ECS consists of- Electronic Credit Clearing Service & Electronic Debit Clearing Service. ECS brings down administration cost and ensures profitability and productivity to the banks. National Electronic Fund Transaction (NEFT) is a deferred net settlement system and is an improvement over other modes in terms of security and processing efficiency. Growth rate in case of ECS has increased. Volume of NEFT has also increased

4. Automated Teller Machines (ATMs)

ATM is a modern device introduced by the banks to enable the customers to have access to money day in day out without visiting the bank branches in person. ATM also called 24-hour tellers are electronic terminals which give consumers the opportunity to bank at almost any time. The system is known as “Any Time Money” because it enables the customers to withdraw money from the bank from

any of its ATMs round the clock installed at various places. ATM has become the most popular and convenient delivery channel throughout entire country. Some ATMs charge a usage fee for this service, with a higher fee for consumers who do not have an account at their institution. If a fee is charged, it must be revealed on the terminal screen or on a sign next to the screen.

The banking transactions from home represent the biggest change in financial institutions since the introduction of ATMs. Automated Teller Machines (ATMs) are used to withdraw cash, make deposits or transfer funds between accounts; a consumer needs an ATM card and a personal identification number. Common operations that are offered are: New accounts opened; Check balance and recent account statements; Balance inquiries and recent movements in credit cards; Bank Transfers; Consultation rates; Refers to monetary exchange; Consultation stock index (stock market); Requests for cheque books; Report stolen / lost card; Payments by electronic transfer (credit card payments, bill payment business by special agreements); Advisers and virtual simulators (calculation of monthly loans, calculation of return on investments); Stop payment on cheques. These are just some of the most common services offered today; the range of possibilities continues to grow. The operation of the service is quite simple. Usually requires an initial contact between the customer and the bank that can be personal or through the site itself or website and usually involves the execution of a contract or agreement regulating the use of the service. The bank gives away a card bearing a unique card number which is assigned to the customer and is linked to the bank account. The bank also provides the customer with a personal password of a confidential nature, which allows its identification in the system and should be used whenever it wants to access the account or transactions through the service. The card is swiped and the password is presented to the machine for verification and for further access to the transaction to be made by the customer.

Self-Check Exercise

Question IV:

Cost of handling transaction is reduced by _____.

Question V:

Is Online Fund Transfer uses conditions and regulations (True/False)?

Question VI:

Settlement of transactions on one to one basic is called _____.

Question VII:

High value transaction is required for immediate clearing in _____ system.

Summary

Electronic Banking (E banking/e-Banking) is a modern banking system. It is the accessibility of banking services in electronic form which are traditionally available only at bank. E-Banking is changing the ways of doing banking businesses with modern technologies (Internet) and techniques.

Glossary

- Automated
- Personal Computer
- Touch Tone Telephone
- Virtual Banking
- E-Delivery
- Indian Financial System Code (IFSC)
- Real Time Gross Settlement (RTGS)
- Deferred Net Settlement (DNS)

- Electronic Clearing Service (ECS)
- National Electronic Fund Transfer (NEFT)

Questions

Q.1 Define online banking.

Q.2 Discuss the applications of electronic fund transfer.

Q.3 What is an virtual bank.

Q.4 List the operations of e-banking.

Q.5 Describe the process of telephone banking services.

Q.6 What are the facilities that e-banking offers.

Q.7 Explain the challenges of e-banking.

Q.8 How is RTGS different from NEFT.

Q.9 Describe the working of ATMs.

Q.10 Explain the transaction process of ECS.

Answers to self-check Exercise

Question I: Internet Banking

Question II: False

Question III: E-Banking

Question IV: Telephone Banking

Question V: True

Question VI: Gross Settlement

Question VII: RTGS

Chapter 5

MARKETING

Objectives:

- Introduction
- Online advertising
- Benefits of online advertising
- Disadvantages of online advertisements
- Types of Online Advertising

5.1 Introduction

In early years, marketing peoples used to depend upon traditional media such as television, radio, newspapers, magazines etc.

Today, the internet has become main source for promoting businesses. There has been a rapid increase in number of users since last few years.

Online marketing is advertising and marketing the products over internet. Online marketing totally relies upon websites or e-emails to reach to the users.

5.2 Online advertising

Online advertising is a form of marketing and advertising which uses the Internet to deliver promotional marketing messages to consumers. It includes email marketing, search engine marketing (SEM), social media marketing, many types of display advertising (including web banner advertising) and mobile advertising. Like other advertising media, online advertising frequently involves both a publisher, who integrates advertisements into its online content, and an advertiser, who provides the advertisements to be displayed on the publisher's content. It is also known as online marketing or Internet advertising.

Email marketing

Email marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing. It usually involves using email to send advertisements, request business, or solicit sales or donations, and is meant to build loyalty, trust, or brand awareness.

Search engine marketing

Search engine marketing (SEM) is a form of internet marketing that involves the promotion of websites by increasing their visibility in search engine results pages (SERPs) through optimization and advertising.

Display advertising

Display advertising is a type of advertising that is located on websites. It can be seen in a wide range of different formats and contains items such as texts, images, flash, video and audio. The main purpose is to deliver general advertisements and brand messages to the million people connected to the internet each month.

Mobile advertising

Mobile advertising is a form of advertising via mobile (wireless) phones or other mobile devices. It is a subset of mobile marketing.

Self-check Exercise

Question I:

SEM is used in _____.

Question II:

Internet advertising involves both publisher and an advertiser (True/False).

Question III:

Through optimization _____ involves promotion of a website increasing their visibility in SERPS.

5.3 Benefits of online advertising

- **Cost:** The low costs of electronic communication reduce the cost of displaying online advertisements compared to offline ads. Online advertising, and in particular social media, provides a low-cost means for advertisers to engage with large established communities. Advertising online offers better returns than in other media.
- **Measurability:** Online advertisers can collect data on their ads' effectiveness, such as the size of the potential audience or actual audience response, how a visitor reached their advertisement, whether the advertisement resulted in a sale, and whether an ad actually loaded within a visitor's view. This helps online advertisers improve their ad campaigns over time.
- **Formatting:** Advertisers have a wide variety of ways of presenting their promotional messages, including the ability to convey images, video, audio, and links. Unlike many offline ads, online ads also can be interactive. For example, some ads let users input queries or let users follow the advertiser on social media. Online ads can even incorporate games.
- **Targeting:** Publishers can offer advertisers the ability to reach customizable and narrow market segments for targeted advertising. Online advertising may use geo-targeting to display relevant advertisements to the user's geography. Advertisers can customize each individual ad to a particular user based on the user's previous preferences. Advertisers can also track whether a visitor has already seen a particular ad in order to reduce unwanted repetitious exposures and provide adequate time gaps between exposures.
- **Coverage:** Online advertising can reach nearly every global market, and online advertising influences offline sales.
- **Speed:** Once advertisement design is complete, online advertisements can be deployed immediately. The delivery of online ads does not need to be linked to the publisher's publication schedule. Furthermore, online advertisers can modify or replace ad copy more rapidly than their offline counterparts.

Self-check Exercise

Question IV:

Online advertising increases the cost of electronic communication. (True/False)

Question V:

Speed of deployment of online advertisement is very slow. (True/False)

5.4 Disadvantages of online advertisements

- **Banner blindness:** Eye-tracking studies have shown that Internet users often ignore web page zones likely to contain display ads (sometimes called "banner blindness"), and this problem is worse online than in offline media. On the other hand, studies suggest that even those ads "ignored" by the users may influence the user subconsciously.
- **Fraud on the advertiser:** There are numerous ways that advertisers can be overcharged for their advertising. For example, click fraud occurs when a publisher or third parties click (manually or through automated means) on a CPC ad with no legitimate buying intent. For

example, click fraud can occur when a competitor clicks on ads to deplete its rival's advertising budget, or when publishers attempt to manufacture revenue.

Click fraud is especially associated with pornography sites. Certain scamming websites launches dozens of hidden pages on each visitor's computer, forcing the visitor's computer to click on hundreds of paid links without the visitor's knowledge. As with offline publications, online impression fraud can occur when publishers overstate the number of advertisement impressions they have delivered to their advertisers. To combat impression fraud, several publishing and advertising industry associations are developing ways to count online impressions credibly.

- **Heterogeneous clients:** Because users have different operating systems, web browsers and computer hardware (including mobile devices and different screen sizes), online ads may appear to users differently from how the advertiser intended, or the ads may not display properly at all. Furthermore, advertisers may encounter legal problems if legally required information doesn't actually display to users, even if that failure is due to technological heterogeneity.
- **Ad-blocking:** Ad-blocking, or ad filtering, means the ads do not appear to the user because the user uses technology to screen out ads. Many browsers block unsolicited pop-up ads by default. Other software programs or browser add-ons may also block the loading of ads, or block elements on a page with behaviours characteristic of ads (e.g. HTML auto play of both audio and video).
- **Anti-targeting technologies:** Some web browsers offer privacy modes where users can hide information about themselves from publishers and advertisers. Among other consequences, advertisers can't use cookies to serve targeted ads to private browsers.
- **Privacy concerns:** The collection of user information by publishers and advertisers has raised consumer concerns about their privacy. Sixty percent of Internet users would use “Do Not Track” technology to block all collection of information if given an opportunity. Many consumers have reservations about by online behavioural targeting. By tracking users' online activities, advertisers are able to understand consumers quite well. Advertisers often use technology, such as web bugs and respawning cookies, to maximizing their abilities to track consumers.
- **Trustworthiness of advertisers:** Scammers can take advantage of consumers' difficulties verifying an online persona's identity, leading to artifices like phishing (where scam emails look identical to those from a well-known brand owner) and confidence schemes. Consumers also face malware risks, i.e. malvertising, when interacting with online advertising
- **Spam:** The Internet's low cost of disseminating advertising contributes to spam, especially by large-scale spammers. Numerous efforts have been undertaken to combat spam, ranging from blacklists to regulatory-required labelling to content filters, but most of those efforts have adverse collateral effects, such as mistaken filtering.

Self-check Exercise

Question VI:

Does online advertisement have any disadvantages? (Yes/No)

5.5 Types of Online Advertising:

The types of online advertising methods in use are as follows.

- **Banner Advertising**

This form of online advertising is even older than the search engines themselves, and the concept is pretty simple. You simply put some sort of banner (usually with a catchy image and headline) on a

relevant website. Users who choose to click the banners will end up on your website and hopefully will make a purchase. The problem is that these days, web users have developed “banner blindness” so only a small percentage will actually click on your ad. With this in mind, you need to make sure that you’re not paying very much for your advertising, especially if you are paying a certain amount per impressions (impressions means that your ad would show up a certain number of times and you will get charged regardless of whether anyone actually clicks on your advertisement).

- **Newsletter Advertising**

You can contact webmasters and email programs to ask them if they are willing to sell ad space in their newsletter or e-magazine. This way you will have access to their subscribers and be able to reach them with a simple low cost advertisement. The ad can be something as simple as a text link that states your website is a sponsor of that publication. Generous newsletters publishers may allow you to have an entire page space on their sent publications to give you maximize exposure. This makes it much simpler to reach an audience that wants to read the email with your website content information included.

- **Affiliate Marketing**

Whether you specialize in physical products or in digital information products like e-books and other courses, affiliate marketing is a great form of online advertising. The major advantage is that you don’t actually have to pay your affiliates a commission until the sale is made. If you do a good job of promoting your affiliate program in the appropriate marketplaces, then these affiliates can do most of the legwork for you like writing articles, using pay per click advertising themselves, and ultimately driving traffic to your product in any number of ways.

Unfortunately, there are still many website owners outside of traditional Internet marketing who are not familiar with the concept of affiliate commissions and may think there is something shady going on. So you simply have to be a salesperson and convince people that your affiliate program is legitimate and profitable. You also have to make sure to choose an excellent network such as Clickbank or Paydotcom.

- **Social Media**

The social media can be used as a form of online advertising, and Facebook ads are excellent examples. At the same time, however, you have to realize that most people are simply using these social networks to hang out with their friends and engaging in entertainment and conversations. Major companies are already expressing doubts about the efficacy of social media marketing campaigns. There are now entire books being written about social media ROI (return on investment), so this tells you that you need to be careful not to waste a lot of time in busy work without evaluating the results.

However Facebook does have its advantages as it uses an advertising system that is very simple to implement and offers a wide scope of coverage in the Facebook website. Only Facebook users that are within the specific demographic you choose will be able to see the advertising. This helps to narrow down who sees advertising so you are not wasting your money on people who are not going to be interested in what your website has to offer.

- **Google AdWords (Pay-per-click Advertising)**

Pay per click advertising is an excellent alternative for companies who have the financial resources and can make an investment in order to bring targeted traffic to their websites. Like SEO traffic, AdWords is considered targeted because people are actually typing in keyword phrases that are relevant to your products and services before clicking on your advertisement. This can bring a flood of traffic to your online business very quickly, and this is an excellent choice as long as you’re able to turn a profit.

That’s where the problem usually lies for small companies who are inexperienced with this form of advertising. There is a lot of competition in pay per click campaigns these days, and it is very easy to

waste a great deal of money if you don't have the experience. Many e-commerce stores get wrapped up in bidding wars that cost product margins to drop substantially. Therefore, if you're going to give this form of advertising a try, just make sure that you take an excellent training course and be ready to invest some money in the beginning while you figure out the entire process.

- **Pop-Up Ads**

According to many webmasters, pop-up ads are the most annoying type of advertisement, although there is little evidence this sentiment is shared by the larger Web community.

Pop-up ads consist of a small window that "pops up" over the main browser window when you enter a site (and sometimes when you leave it, a favourite tactic of adult sites). The pop-up windows can contain anything: text, graphics, a form to collect information or email addresses, even a little game.

There are two downsides to pop-up ads, one for webmasters, one for advertisers. From a webmaster's point of view, pop-up ads wrench control of the browser away from their own page, and some badly-written pop-up ads may also crash certain browsers, leaving a permanently bad impression in a visitor's mind. From an advertiser's point of view, most pop-up windows can be minimized (hidden behind the other windows) with relative ease, so if the pop-up window is being used to rotate ads on a time basis, your advertisement may not even be visible but you'll still be charged for it.

- **Rich Media Ads**

Rich media ads make use of multimedia elements such as sound, animation (often using plugins such as Shockwave or Flash) and Java/JavaScript to drive the message home. Great for advertisers, less good for webmasters since the premium for rich-media ads is not particularly high, but the extra load time and annoyance can be considerable (you'll lose your audience of visitors surfing from work on audio-equipped PCs for a start if your site suddenly blares out music!).

- **Pre-Roll Video Ads**

Pre-roll ads are fantastic for branding, since the users are forced to sit through at least five to 10 seconds of advertising before they see their desired video. They're also an acceptable option for direct response, although usually less effective than banners.

Because most users will click through using the 'skip' button after watching the first few seconds of your video, it's important to get your message through quickly when using pre-roll advertising to market your business.

- **Video Overlay Ads**

There's more to video advertising than just the pre-roll. Video overlay ads are text or banner ads that are displayed on top of a YouTube video. Like pre-roll ads, they can be purchased, designed and targeted using the Ad words Display Network.

Video overlay ads can be targeted using a variety of variables. You can select target keywords and display your ads on related videos, use placement targeting or select a retargeting audience to reach an audience that's already visited your website. While pre-roll video ads are ideal for branding, video overlay ads are generally the best choice for direct response. The key to an effective video overlay ad campaign is twofold: great targeting and even better copywriting.

- **Contextual Ads**

Contextual advertising is not an advertising example itself. It is technically a form of targeting for other advertising formats. Contextual advertisements can be banners, as in the example above, video overlay ads, social media ads and much more.

Although contextual ads can seem a little creepy at times, they're beneficial for both users and advertisers. Users get to see ads that are actually of interest to them, while advertisers benefit from a more motivated and enthusiastic marketing audience.

Self-check Exercise

Question VII:

Banner advertising, Affiliate Marketing, Google Ad words, popup-ads is not a type of online advertising. (True/False)

Summary

- Online advertising is a form of marketing and advertising which uses the Internet to deliver promotional marketing messages to consumers.
- Email marketing is directly marketing a commercial message to a group of people using email.
- Search engine marketing (SEM) is a form of internet marketing that involves the promotion of websites by increasing their visibility in search engine results pages (SERPs) through optimization and advertising.
- Display advertising is a type of advertising that is located on websites. It can be seen in a wide range of different formats and contains items such as texts, images, flash, video and audio.
- Mobile advertising is a form of advertising via mobile (wireless) phones or other mobile devices. It is a subset of mobile marketing.
- Ad-blocking, or ad filtering, means the ads do not appear to the user because the user uses technology to screen out ads.
- Pay per click advertising is an excellent alternative for companies who have the financial resources and can make an investment in order to bring targeted traffic to their websites.
- Rich media ads make use of multimedia elements such as sound, animation (often using plugins such as Shockwave or Flash) and Java/JavaScript to drive the message home.

Glossary

- Email Marketing
- Search Engine Marketing (SEM)
- Search Engine Result Pages (SERPs)
- Spam
- E-Magazine
- E-Book
- ClickBank
- PaydotCom
- Return on Investment (ROI)
- Adwords Display Network

Questions

Q.1 Explain online advertising. What are its advantages and disadvantages?

Q.2 Explain Email marketing.

Q.3 Explain Display advertising.

Q.4 Explain Search engine marketing.

Q.5 Explain Mobile advertising.

Q.6 Explain Benefits of online advertising

Q.7 Define Ad-blocking.

Q.8 Describe various examples of online advertising.

Q.9 What is the difference between pre-roll video Ads and video overlay Ads?

Q.10 Explain Pay-per-click Advertising.

Answers to Self-Check Exercise

Question I: Online Advertising

Question II: True

Question III: SEM

Question IV: False

Question V: False

Question VI: Yes

Question VII: False

Chapter 6

SEARCH ENGINE

Objectives:

- Introduction
- Search Engine as an advertising media
- Working of search engine
- Search engine marketing
- Tools for search engine advertising
- Search engine optimisation
- SEO concept & techniques

6.1 Introduction

It helps to locate Information on World Wide Web. Search engines are computer system which stores information, categorize it, and show it to user. Search engines are used as tools by large number of people throughout the world.

Main components of search engines are listed below:

- Web crawler
- Database
- Search interfaces

Main search engines are:

- Google
- Bing
- Yahoo
- Yandez
- Baido

6.2 Search Engine as an Advertising Media

Search engine as an advertising media refers to the short text advertisements which generally appear at the top or down the right hand side of search engine results. These are often labelled as "sponsored Links" or "sponsored results".

These advertisements are generally purchased from Google (the Google Adwords product), or Yahoo! Search Marketing. It is also known as search engine marketing (SEM).

Search engine advertising includes sponsorships, pay-for-placement (PFP) advertising and maybe contextual advertising.

Self-check Exercise

Question I:

Search Engine advertising includes _____and _____.

Question II:

Advertisements appear at the top or down the left hand side of search engine results. (True/False)

6.3 Working of search engine

Search engines have one objective to provide the user with the most relevant results possible in relation to your search query. If the search

engine is successful in providing you with information that meets your needs, then you are a happy searcher. And happy searchers are more likely to come back to the same search engine time and time again because they are getting the results they need.

In order for a search engine to be able to display results when a user types in a query, they need to have an archive of available information to choose from. Every search engine has proprietary methods for gathering and prioritizing website content. Regardless of the specific tactics or methods used, this process is called indexing. Search engines actually attempt to scan the entire online universe and index all the information so they can show it to you when you enter a search query.

Every search engine has what are referred to as bots, or crawlers, that constantly scan the web, indexing websites for content and following links on each webpage to other web pages. If your website has not been indexed, it is impossible for your website to appear in the search results as shown in figure 6.1. Unless you are running a shady online business or trying to cheat your way to the top of the search engine results page (SERP), chances are your website has already been indexed.

So, big search engines like Google, Bing, and Yahoo are constantly indexing hundreds of millions, if not billions, of web pages. How do they know what to show on the SERP when you enter a search query? The search engines consider two main areas when determining what your website is about and how to prioritize it.

1. **Type of content on the website:** When indexing pages, the search engine bots scan each page of your website, looking for clues about what topics your website covers and scanning your website's back-end code for certain tags, descriptions, and instructions.
2. **Links to other web pages:** As the search engine bots scan web pages for indexing, they also look for links from other websites. The more inbound links a website has, the more influence or authority it has. Essentially, every inbound link counts as a vote for that website's content. Also, each inbound link holds different weight. For instance, a link from a highly authoritative website like The New York Times (nytimes.com) will give a website a bigger boost than a link from a small blog site. This boost is sometimes referred to as link juice.

When a search query is entered, the search engine looks in its index for the most relevant information and displays the results on the SERP.

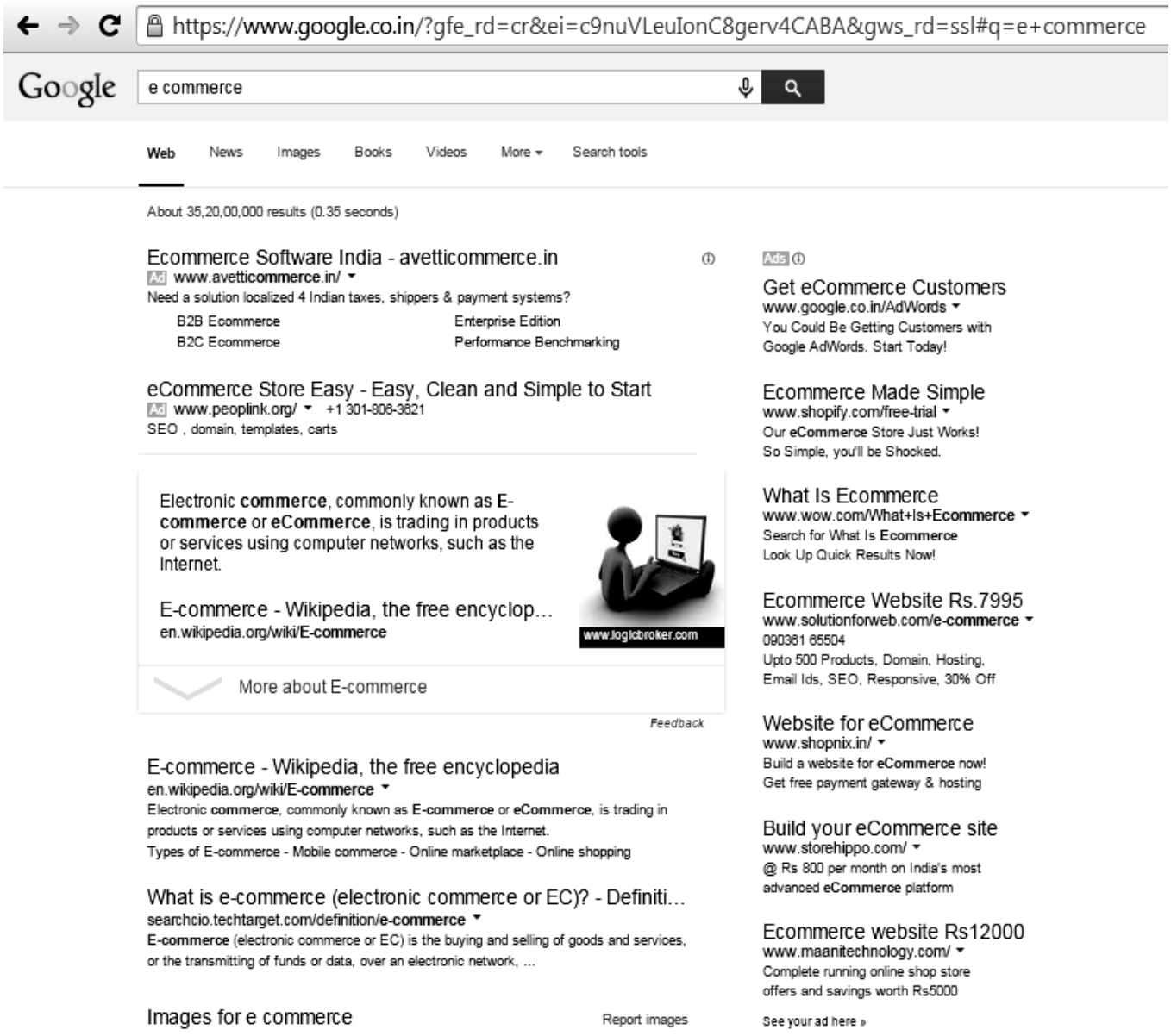

Figure 6.1: Search Engine

The results are then listed in order of most relevant and authoritative.

If you conduct the same search on different search engines, chances are you will see different results on the SERP. This is because each search engine uses a proprietary algorithm that considers multiple factors in order to determine what results to show in the SERP when a search query is entered as shown in Figure 6.2 (a) and Figure 6.2(b).

Figure 6.2 (a): Different Results In Different Search Engines

Figure 6.2 (b) Different Results In Different Search Engines

Self-Check Exercise

Question III:

Search Engine uses _____ methods for gathering and prioritizing website content.

Question IV:

Bots are used for scanning webs (True/False).

6.4 Search Engine Marketing

Search engine marketing is a form of Internet marketing that involves the promotion of websites by increasing their visibility in search engine results pages. SEM may use search engine optimization (SEO). Search Engine Optimisation is defined as the process of building pages in a manner which enables the pages to rank highly in algorithmically determined search results, which are generally displayed on the left hand side of the page. The algorithmic results are independently determined by the search engine's own mathematical algorithm, and are based on relevance to the search phrase. Search engines use complex mathematical algorithms to determine the relevance of indexed pages for a particular search phrase.

As an Internet marketing strategy, SEO considers how search engines work, what people search for, the actual search terms or keywords typed into search engines and which search engines are preferred by their targeted audience. Optimizing a website may involve editing its content, HTML and associated coding to both increase its relevance to specific keywords and to remove barriers to the indexing activities of search engines.

Self-Check Exercise

Question V:

SEM uses _____.

6.5 Tools for Search engine advertising

There are four categories of methods and metrics used to optimize websites through search engine marketing.

1. **Keyword research and analysis**: It involves ensuring the site can be indexed in the search engines, finding the most relevant and popular keywords for the site and its products, and using those keywords on the site in a way that will generate and convert traffic. A follow-on effect of keyword analysis and research is the search perception impact. Search perception impact describes the identified impact of a brand's search results on consumer perception, including title and meta tags, site indexing, and keyword focus. As online searching is often the first step for potential consumers/customers, the search perception impact shapes the brand impression for each individual.
2. **Website saturation and popularity**: It is used to know how much presence a website has on search engines, can be analyzed through the number of pages of the site that are indexed on search engines (saturation) and how many back links the site has (popularity). It requires pages to contain keywords people are looking for and ensure that they rank high enough in search engine rankings. Most search engines include some form of link popularity in their ranking algorithms.
3. **Back end tools**: It includes Web analytic tools and HTML validators, provide data on a website and its visitors and allow the success of a website to be measured. They range from simple traffic counters to tools that work with log files and to more sophisticated tools that are based on page tagging (putting JavaScript or an image on a page to track actions). These tools can deliver conversion-related information.
4. **Who is tools:** These tools reveal the owners of various websites, and can provide valuable information relating to copyright and trademark issues.

Self-Check Exercise

Question VI:

Can we index our website in search engine? (True/False)

Question VII:

Number of pages of website that are indexed on Search Engine is called _____.

Question VIII:

Popularity is number of _____ the website has.

6.6 Search Engine Optimisation

Search engine optimization (SEO) refers to techniques that help your website rank higher in organic (or "natural") search results, thus making your website more visible to people who are looking for your product or service via search engines.

SEO is part of the broader topic of Search Engine Marketing (SEM), a term used to describe all marketing strategies for search. SEM entails both organic and paid search. With paid search, you can pay to list your website on a search engine so that your website shows up when someone types in a specific keyword or phrase. Organic and paid listings both appear on the search engine, but they are displayed in different locations on the page.

Self-Check Exercise

Question IX:

Search Engine Marketing involves _____ and _____.

6.7 SEO Concept & Techniques

Search engine optimisation can be done using following two main strategies:

1. Off-page SEO
2. On-page SEO

Off-page SEO

On-page SEO covers everything you can control on each specific webpage and across your website to make it easy for the search engines to find, index, and understand the topical nature of your content.

On-page SEO

Off-page SEO covers all aspects of SEO that happen off your website to garner quality inbound links. Compared to on-page SEO, off-page SEO can certainly be more difficult to execute. Off-page SEO entails building relationships with other websites through the creation of attractive content, or reaching out to the people who run the websites. This process of building relationships is called link building. Who is linking to you, how they are linking to you, and how your content is shared in social networks and across the web are all factors that can have a significant impact on your ability to rank on the SERP.

Search Engine Optimization Techniques

SEO techniques are used to get more visibility for the websites in search engine results pages.

SEO techniques are classified into two broad categories:

- **White Hat SEO** - Techniques that search engines recommend as part of a good design.
- **Black Hat SEO** - Techniques that search engines do not approve and attempt to minimize the effect of. These techniques are also known as spamdexing.

White Hat SEO

An SEO tactic is considered as White Hat if it has the following features:

- It conforms to the search engine's guidelines.
- It does not involve in any deception.

- It ensures that the content a search engine indexes, and subsequently ranks, is the same content a user will see.
- It ensures that web page content should have been created for the users and not just for the search engines.
- It ensures good quality of the web pages.
- It ensures availability of useful content on the web pages.

Black Hat SEO

An SEO tactic is considered as Black Hat or Spamdexing if it has the following features:

- Attempting ranking improvements that are disapproved by the search engines and/or involve deception.
- Redirecting users from a page that is built for search engines to one that is more human friendly.
- Redirecting users to a page that was different from the page the search engine ranked.
- Serving one version of a page to search engine spiders/bots and another version to human visitors. This is called Cloaking SEO tactic.
- Using hidden or invisible text or with the page background color, using a tiny font size or hiding them within the HTML code such as "no frame" sections.
- Repeating keywords in the meta tags, and using keywords that are unrelated to the website content. This is called meta tag stuffing.
- Calculated placement of keywords within a page to raise the keyword count, variety, and density of the page. This is called keyword stuffing.
- Creating low-quality web pages that contain very little content but are instead stuffed with very similar keywords and phrases. These pages are called Doorway or Gateway Pages.
- Mirror websites by hosting multiple websites all with conceptually similar content but using different URLs.
- Creating a rogue copy of a popular website which shows contents similar to the original to a web crawler, but redirects web surfers to unrelated or malicious websites. This is called page hijacking.

Self-check Exercise

Question X:

Spamdexing is also known as _____.

Question XI:

All aspects of SEO are covered by _____.

Question XII:

Page Hijacking is a feature of Black hat SEO (True/False).

Summary

- Search engine as an advertising media refers to the short text advertisements which generally appear at the top or down the right hand side of search engine results.
- Every search engine has what are referred to as bots, or crawlers, that constantly scan the web, indexing websites for content and following links on each webpage to other web pages.

- On-page SEO covers everything you can control on each specific webpage and across your website to make it easy for the search engines to find, index, and understand the topical nature of your content.
- Off-page SEO covers all aspects of SEO that happen off your website to garner quality inbound links.
- Every search engine has proprietary methods for gathering and prioritizing website content.
- Search engines actually attempt to scan the entire online universe and index all the information so they can show it to you when you enter a search query.

Glossary

- Query
- Indexing
- Crawler
- Search Engine Optimization (SEO)
- Spamdexing
- Proprietary Algorithm
- Uniform Resource Locator (URLs)
- Meta tags

Questions

Q.1 What is search engine? Explain its role in advertising media.

Q.2 What is Search engine optimisation?

Q.3 What are the various methods and techniques for search engine optimisation?

Q.4 What are various SEO tools?

Q.5 Which are important factors for a search engine algorithm?

Q.6 Differentiate between on-page SEO and off-page SEO.

Q.7 What is white hat search engine optimization technique?

Q.8 What is black hat search engine optimization technique?

Q.9 What are various tools for search engine advertising?

Q.10 What is the role of web crawlers in search engine?

Answers to Self-check Exercise

Question I: Sponsorship and pay for placement

Question II: False

Question III: Proprietary

Question IV: True

Question V: SEO

Question VI: True

Question VII: Saturation

Question VIII: Links

Question IX: Organic and paid search

Question X: Black Hat SEO

Question XI: Off page SEO

Question XII: True

Chapter 7

EMAIL MARKETING

Objectives:

- Introduction
- Email Marketing
- Social Networking and Marketing
- Promotion & Opinion
- Viral marketing
- E-retailing
- Methods for E-retailing in Global Online Market
- Advantages of E-retailing
- Limitations of E-retailing

7.1 Introduction

Email marketing is one the most traditional form of digital marketing. Promoting a business by sending emails and newsletter to users is called as email marketing. The idea is to gather to a database of email addresses of customers and then send those peoples emails to keep them engaged with company's news and offerings.

It is most appealing and least expensive means of marketing.

7.2 Email Marketing

Email marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing. It usually involves using email to send ads, request business, or solicit sales or donations, and is meant to build loyalty, trust, or brand awareness. Email marketing can be done to either sold lists or a current customer database. Broadly, the term is usually used to refer to sending email messages with the purpose of enhancing the relationship of a merchant with its current or previous customers, to encourage customer loyalty and repeat business, acquiring new customers or convincing current customers to purchase something immediately, and adding advertisements to email messages sent by other companies to their customers.

Types of Email Marketing

Email marketing can be carried out through two types of emails:

1. Transactional emails

Transactional emails are usually triggered based on a customer's action with a company. To be qualified as transactional or relationship messages, these communications' primary purpose must be to facilitate, complete or confirm a commercial transactions that the recipient has previously agreed to enter into with the sender, along with a few other narrow definitions of transactional messaging. Triggered transactional messages include dropped basket messages, password reset emails, purchase or order confirmation emails, order status emails, reorder emails and email receipts.

Many email newsletter software vendors offer transactional email support, which gives companies the ability to include promotional messages within the body of transactional emails. There are also software vendors that offer specialized transactional email marketing services, which include providing targeted and personalized transactional email messages and running specific marketing campaigns such as customer referral programs.

2. Direct emails

Direct email or interruption based marketing involves sending an email solely to communicate a promotional message, for example, an announcement of a special offer or a catalogue of products. Companies usually collect a list of customer or prospect email addresses to send direct promotional messages to, or they can also rent a list of email addresses from service companies, but safe mail marketing is also used.

Advantages of Email Marketing

- An exact return on investment can be tracked and has proven to be high when done properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
- Advertisers can reach substantial numbers of email subscribers who have opted in to receive email communications on subjects of interest to them.
- If compared to standard email, direct email marketing produces higher response rate and higher average order value for e-commerce businesses.

Self-check Exercise

Question I:

We can communicate our commercial message to a group of people using emails. (True/False)

Question II:

Email marketing uses _____ type of emails.

Question III:

Traditional emails are based on _____.

Question IV:

Direct email is also known as _____.

7.3 Social Networking and Marketing

The most well-known social software applications are weblogs, wikis, social networking sites and instant messaging. Social networking at a high level is described as the convergence of technologies that make it possible for individuals to easily communicate, share information, and form new communities online. But the big question today is not what social networking is, but rather what it means for businesses.

During the fast growth of social media and software, social networks are forcing companies to increase activities in their traditional CRM systems. These popular websites could be a great approach for companies and customers to improve their communications by applying them in computers and mobile devices. Through the social networks the way, which the company uses in its marketing, is changed. Business can take benefit through applying Social network marketing in order to cooperate with companies to achieve their goals. One of the most important advantages of Internet based application is creating an interactive contact between stakeholders that enable businesses to get feedback directly from their customers.

In parallel companies can gain benefits through social marketing: they can achieve a better understanding of the customer needs and then they can build effective relationships with customers. Although social marketing is a common concept in business, there is a few numbers of people aware of its effective role in marketing. Social Marketing is a known term but not all the people know what it is exactly and what are the opportunities and risks from it. Social network marketing can be very advantageous for businesses.

Social Media Marketing

Marketing is the process, which is used to determine what products or services can be of interest to customer. Social networks help in improving the marketing of organizations to new insights about the brand, which offers innovative ways to implement the basic marketing programs, as well as new methods to win in online discussions of important business. So they can use these new opportunities, they need the tools that their companies can monitor conversations across the Internet effectively and participate. The goal is to link the success of activities in social networks with marketing programs and processes.

Social Networking Sites

Social networking sites are the source of almost inexhaustible views of clients and situations, and the challenge is to control this information in an appropriate manner and in a meaningful way for the company and that brings real benefits for them. Social networking is also a suitable framework for core activities in marketing on the Internet. Social networks provide the opportunity to talk with customers on a personal level, which is usually difficult to achieve or impossible through traditional channels. Marketing on social networking sites is not a substitute for traditional marketing. It should be treated as an additional channel with unique characteristics that can complement other marketing activities. With this approach, we can increase the effectiveness of each channel.

Self-Check Exercise

Question V:

Social networks are forcing companies to increase activities in _____.

Question VI:

Social networks do not help in improving the marketing of organizations (True/False).

7.4 Promotion & Opinion

The promotion of social media is very crucial in social marketing. The reason for a company or brand's social media participation, the audience they're trying to reach, budget/resources and the actual social platforms being used will all flavor how a social media program can and should be promoted.

As an example, let's say a fan page has been created on facebook to promote a specific brand/product. The promotion of that fan page could be accomplished through:

On – Facebook

- Facebook advertising.
- Contest or giveaway promotions that encourage fans to share links back to the fan page.
- Participation in groups and other fan pages that reach the audience being targeted.
- Leverage mailing lists of other group or fan pages for the same brand.
- Creation of a widget that provides the ability to interact with users, offer value and invite users back to the fan page.

Off – Facebook:

- SEO and link building to landing pages
- Press release optimization & promotion
- Email promotions to segmented lists
- Cross promotion to facebook fan page from other social media properties

Another example might involve a newly launched company blog. A blog should have content when it goes live, so anywhere from 5-15 posts can provide a good start for promotion.

Self-check Exercise

Question VII:

Promotion of social media is very crucial in _____.

7.5 Viral Marketing

"Viral marketing" is an advertising strategy in which people pass on a marketing message to others. For example, when hotmail first began to offer free email addresses, the following message was included at the bottom of every message: "Get your private, free email at http://www.hotmail.com". When people received emails from friends and family that were already using hotmail, many of them would sign up for their own accounts. Later on, these new hotmail users would send out their own emails, thereby continuing the cycle.

To create and promote an ad that you want to "go viral", you have to show it to several focus groups. Based on their responses, you estimate that the average viewer will send your ad to three other people the next day. If you send the ad to five people on the first day, how many new people do you expect will see the ad each day for the first week? How many people in total will see the ad each day for the first week?

Hence viral marketing refers to marketing techniques that use pre-existing social networking services and other technologies to try to produce increases in brand awareness or to achieve other marketing objectives (such as product sales) through self-replicating viral processes, analogous to the spread of viruses or computer viruses. It can be delivered by word of mouth or enhanced by the network effects of the Internet and mobile networks. Viral advertising is personal and, while coming from an identified sponsor, it does not mean businesses pay for its distribution. Most of the well-known viral ads circulating online are ads paid by a sponsor company, launched either on their own platform i.e. company webpage or social media profile or on social media websites such as youtube. Consumers receive the page link from a social media network or copy the entire ad from a website and pass it along through e-mail or posting it on a blog, webpage or social media profile. Viral marketing may take the form of video clips, interactive flash games, e-books, software, images, text messages, email messages or web pages.

Self-Check Exercise

Question VIII:

_____ refers to marketing techniques that use pre-existing social networking services.

Question IX:

To promote and create an ad about any product you have to do _____.

7.6 E-retailing

E-Retailing is the use of technology such as computers and the internet to sell a range of products and services online to the world.

7.7 Methods for E-retailing in Global Online Market

The following methods can be used to make products and service be available to the global market:

- Using banners on others sites to advertise
- Using word of mouth
- Using social networking sites to advertise such as twitter to alert people when a new product is available
- Use of existing contacts with customers to invite them through email.
- If the funds are available use television advertisement and radio advertisement.

Self-Check Exercise

Question X:

Can we make our product available to global market by using banner and social networking? (Yes/No)

7.8 Advantages of E-retailing

- E-Retailing opens up many doors for companies.
- E-Retailing provides a greater range of people to whom the products can be sold.
- This can lead to increase in profits and a decrease in costs.
- The web site can also lead to opportunities of better and cheaper products to sell thought globalization.

7.9 Limitations of E-retailing

- Privacy: Some consumers are reluctant to embrace e-retailing because of privacy issues. Making an online purchase often requires disclosing personal information such as an address, telephone number and banking or credit card account information. While many people feel making an online purchase does not compromise their personal information, some still prefer not to take a chance of having their account information accessed by a third party, and will only make their purchases at a storefront operation.
- Unfamiliarity: There are always going to be people who prefer to do their shopping at a brick and mortar location. Some people are resistant to change and may not want to embrace e-retailing due to a lack or knowledge about the process or a general reluctance to purchase an item they cannot physically examine. If the product does not meet the customer's expectations in some way, such as being the wrong size or defective, he must then spend time sending it back and waiting for the replacement product to arrive.
- Lack of consumer trust and security: People may have more trust and confidence in dealing with a physical retail store than with an online e-retailer. They know that the store is there, and if they have a problem they know where to go. In contrast, a website might look very impressive, yet the business might simply be a person working part-time with a laptop computer on a kitchen table, which could close the business at any time or simply decide to ignore customers who have complaints. Some consumers might not only be leery of the solidness of an e-retailer but also be hesitant to share credit card and other personal information over the internet to someone they can’t see.
- Hard to build customer relations: The friendly smile of an employee greeting you as you walk into a retail store can go a long way in building customer relations, helping ensure repeat business. Helpful and knowledgeable interaction with store employees creates confidence with customers. E-tailing lacks the opportunity for face-to-face contact and must try other means to establish long-term relationships with customers.
- Additional costs: E-retailing involves additional costs for purchased items compared to purchases made at brick and mortar stores. Items must be mailed or shipped, incurring not only the additional cost of postage but also for packing materials, which can be significant if items are large or fragile. When items have to be returned, even more postage may be required by the e-retailer for return shipping costs.
- Can't feel products: Just looking at a photograph and reading a description of a product may give enough information for a consumer to make a purchase online. Some products, however, need to be held, smelled, touched and listened to in person, making them poor candidates for e-tailing. Musicians, for example, will typically want to play an acoustic guitar before making a purchase, since every guitar has its own unique feel and sound. A person interested in buying speakers for his home stereo may want to listen to them, which can be demonstrated in a retail store but not through an online e-retailer.

Self-Check Exercise

Question XI:

Can user faces privacy issues while purchasing something online? (Yes/No)

Summary

- Email marketing is directly marketing a commercial message to a group of people using email.
- Marketing is the process, which is used to determine what products or services can be of interest to customer.
- Social networking is also a suitable framework for core activities in marketing on the Internet.
- Viral marketing is an advertising strategy in which people pass on a marketing message to others.
- E-Retailing is the use of technology such as computers and the internet to sell a range of products and services online to the world.
- Some consumers are reluctant to embrace e-retailing because of privacy issues.
- People may have more trust and confidence in dealing with a physical retail store than with an online e-retailer.

Glossary

- Web-Blogs
- Wiki's
- Social Network
- Instant Messaging
- Viral Marketing
- E-retailing
- Electronic Customer Relationship Management (E-CRM)
- E-tailing
- Advertisement
- Social Marketing

Questions

Q.1 Define email marketing. What are its features?

Q.2 Explain briefly various types of email marketing.

Q.3 What is social media networking and social media marketing.

Q.4 Explain the role of social media in marketing. How it is promoted?

Q.5 Define viral marketing. What are its features?

Q.6 Define e-retailing. What are various advantages of e-retailing?

Q.7 Explain the limitations of e-retailing.

Q.8 Differentiate between transactional email and direct email.

Q.9 What are privacy issues in e-retailing?

Q.10 What kind of additional costs occur in e-retailing?

Answers to Self-check Exercise

Question I: True

Question II: Two

Question III: Customer action

Question IV: Interruption based Marketing

Question V: CRM System

Question VI: False

Question VII: Social Networking

Question VIII: Viral Marketing

Question IX: Viral Marketing

Question X: Yes

Question XI: Yes

Chapter 8

CRM AND INFORMATION TECHNOLOGY

Objectives:

- Introduction
- CRM software
- Role of information technology in CRM
- Tools to conducting online research
- Secondary research
- Online focus groups
- Web based surveys
- Design Guidelines for Web-Based Surveys
- Data mining from social networking sites

8.1 Introduction

Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers, assisting in customer retention and driving sales growth. CRM systems are designed to compile information on customers across different channels -- or points of contact between the customer and the company -- which could include the company's website, telephone, live chat, direct mail, marketing materials and social media. CRM systems can also give customer-facing staff detailed information on customers' personal information, purchase history, buying preferences and concerns.

8.2 CRM Software

CRM software consolidates customer information and documents into a single CRM database so business users can more easily access and manage it. The other main functions of this software include recording various customer interactions (over email, phone calls, social media or other channels, depending on system capabilities), automating various workflow processes such as tasks, calendars and alerts, and giving managers the ability to track performance and productivity based on information logged within the system.

Features of CRM software

- Marketing automation: CRM tools with marketing automation capabilities can automate repetitive tasks to enhance marketing efforts to customers at different points in the lifecycle. For example, as sales prospects come into the system, the system might automatically send them marketing materials, typically via email or social media, with the goal of turning a sales lead into a full-fledged customer.
- Sales force automation: Also known as sales force management, sales force automation is meant to prevent duplicate efforts between a salesperson and a customer. A CRM system can help achieve this by automatically tracking all contact and follow-ups between both sides.
- Contact centre automation: Designed to reduce tedious aspects of a contact centre agent's job, contact centre automation might include pre-recorded audio that assists in customer problem-solving and information dissemination. Various software tools that integrate with the agent's desktop tools can handle customer requests in order to cut down the time of calls and simplify customer service processes.

- Geolocation technology or location-based services: Some CRM systems include technology that can create geographic marketing campaigns based on customers' physical locations, sometimes integrating with popular location-based GPS apps. Geolocation technology can also be used as a networking or contact management tool in order to find sales prospects based on location.

Self-Check Exercise

Question I:

Main function of CRM software includes _____ and _____.

Question II:

CRM system automatically tracks all contacts. (True/False)

8.3 Role of information technology in CRM

Technology and customer relationship management (CRM) software go hand and hand. CRM is software. CRM software extents across the organizational structure beginning with a web-based, user-friendly interface for sales executives and customer service personnel and ending with massive databases and knowledge management systems. In some applications, the web-based interface extends to the customer as well. The primary objective of any company or corporation is the get and keep a customer. Customer relationship management (CRM) is an information technology-driven strategy companies use to get and keep a customer.

Everything about CRM is information technology-driven. Technology is pervasive from the basic user-friendly interface to complex back-end database and knowledge management systems. Massive databases are the heart of any CRM system. Data is collected from multiple sources ranging from data entry from customer service personnel to online data collection forms made available to the customer via a web browser. Sales executives or customer service personnel can access this data via the worldwide web, an extranet relationship with a corporate partners or an internal corporate intranet. Given the rise of PDAs and smartphones, many companies offer CRM mobile applications to sales executives in the field.

CRM technology components

CRM applications has three primary technology components that are referred to as customer touch points, applications, and data stores.

Customer touch points: Customer touch points are the primary human interface with customers. This is the beginning of the sales process. Sales people or customer service personnel communicate with the customer and input data into the system. Or, with the web, this interface could be through an online form where the customer is asking for more information.

Applications: Applications is the software interface between the customer touch points and corporate databases.

Data stores: Data stores represent the data stored in the databases as well as the knowledge management systems designed to interpret the data and map out customer buying habits or buying behavior patterns.

Advantages of IT in CRM

- Using CRM & internet, one not only achieve support for online customer but also improve relationship with traditional customer.
- It facilitates global reach of services through internet.
- IT enables both customer & employees to be more effective in getting & providing services.
- IT helps in providing complete product information.

- IT helps in providing an easy ordering and billing process.
- IT plays pivotal role to play in enabling companies to maximize profitability through more precise targeting of market segment & micro segment within.
- IT assist in managing the data required to understand customer so that appropriate CRM strategies can be adopted.

Disadvantages of IT in CRM

- Loss of human contacts & personal interaction
- There are tremendous investment cost in it for fine, often with uncertain payback.
- It may not understand the marketing objective & analysis effectively and sometimes work on wrong data results in wastage of time & money.
- It threatens privacy of customers in many ways, e.g. hacking, stealing data over the internet etc.

Self-Check Exercise

Question III:

_____Strategy is used by companies to get and keep their customers.

Question IV:

_____ are the heart of CRM system.

Question V:

Most of the sales executives use CRM Mobile application (True/False).

8.4 Tools to conduct online research

Using the Internet to conduct quantitative research presents challenges not found in conventional research. Some of our knowledge concerning the effective design and use of paper-based surveys does translate into electronic formats. However, electronic surveys have distinctive technological, demographic and response characteristics that affect how they should be designed, when they can be used and how they can be implemented. Survey design, subject privacy and confidentiality, sampling and subject solicitation, distribution methods and response rates and survey piloting are critical methodological components that must be addressed in order to conduct sound online research.

Tools

The following techniques can be used to gather market information with the help of a few mouse clicks and keystrokes:

- **Keyword Search:** One must know how to do a simple Web search using search engines such as Google and Yahoo. Take that a step farther by searching for "keywords" that people would use to find your type of products or services on the Internet. Analyse how much interest there is in these keywords -- and how many competitors you have in this market. Keyword searches can also help remind you of product niches that you might not have considered.
- **Competitor Links:** A traditional search engine can also help you check out your competitors, their prices, and their offerings. Try typing 'link:www.[competitor's name].com' into Google to find out how many other sites link to your competitor's website. It is a great way to see a competitor's link development and strategies.
- **Read Blogs:** Blogs are updated much more regularly than traditional websites and, therefore, they can be another gauge of public opinion.
- **Conduct Online Surveys:** Another way to gauge public opinion is through online surveys. While not as scientific as in-person or phone surveys that use a random sampling of the

population, online surveys are a low-cost way to do market research about whether an idea or a product will be appealing to consumers.

Features of questionnaire in conducting online research

Following features must be incorporated in the survey design while conducting online research:

- Respondent can designate conditions of release, use, retention and disposal of personal data.
- Send invitations and surveys separately.
- Offer e-incentives.
- Collect data through web pages.
- Provide multiple response options.
- Use “remailers” to ensure anonymity.
- Do not troll through observation.
- Do not use “cookies”.
- Do not use links from personalized sites.
- Provide disclosures.
- Provide 3rd party privacy certification.
- Use credible domains.
- Use encryption for sensitive material.
- Use hypertext links for long disclosures.
- Disclose sampling procedures.
- Community leader consent for member email addresses can be obtained.
- Provide survey results to respondents.
- Use self-selected user ids, passwords.
- Provide “rather not say” response option for sensitive questions.

Self-Check Exercise

Question VI:

We can gather market information with the help of internet. (True/False)

Question VII:

Blogs/Online surveys are tools to conduct online Research. (Yes/No)

Question VIII:

Traditional websites are updated more regularly than blogs. (True/False)

8.5 Secondary research

Secondary sources consist of data that has already been produced and can be contemporary or historical, qualitative or quantitative. Secondary research involves the summary, collation and synthesis of existing research rather than primary research, where data is collected from, for example, research subjects or experiments. It is also known as desk research.

Secondary sources include:

- Documents
- Letters

- Diaries
- Autobiographies
- Referencing other forms of research and using quotes

Benefits of secondary research

The benefits of the use of secondary sources include:

- Save time and money
- May provide information and access to historical data.
- May be used to prove or disprove an argument or theory.
- May be used to offer general background information.
- Can be used to set the scene of the research and its findings.
- May be useful for putting the research into context.

Self-Check Exercise

Question IX:

In Secondary Research data is collected from _____ and _____.

8.6 Online focus groups

An online focus group is one type of focus group, and is a sub-set of online research methods. They are typically an appropriate research method for consumer research, business-to-business research and political research.

Advantages

Advantages of on-line focus groups include congruence with the environment being studied, increased ease of communication between participants, greater equality of participation in the discussion, anonymity of participants, reduction in bias, ability to recruit diverse populations, and the ability to address more controversial topics.

Disadvantages

Disadvantages associated with on-line focus groups include under representation of the overall population because only internet users are included, loss of verbal cues during communication, potential problem of privacy of discussion, a high no-show rate among participants agreeing but failing to take part in the online focus groups

Self-Check Exercise

Question X:

_____ is the subset of Online Research Method.

8.7 Web based surveys

A Web-based survey is the collection of data through a self-administered electronic set of questions on the Web. With Web-based surveys, the manager has control over the physical appearance and can create attractive and inviting forms. Web-based surveys can include radio buttons and drop-down lists that permit only one choice for the response. Check boxes allow multiple answers. Text boxes can be one line with a limited number of characters, or they may permit unlimited text entry.

Advantages of conducting web based surveys

- Paper, postage, mail out, and data entry costs are almost completely eliminated.
- Time required for implementation can be reduced. Once electronic data collection system is developed, cost of surveying additional respondents is much lower.

- Display of response data can be simultaneous with completion of surveys. Often, data from Web-based surveys are available in real time in graphic and numerical format.
- Reminders and follow-up on non-respondents are relatively easy.
- Data from Web-based surveys can be easily imported into data analysis programs.

Disadvantages of conducting web based surveys

- Not everyone is connected, so the web survey method will not work with all populations.
- Even if connected, not all potential respondents are equally computer literate.
- Screen configurations may appear significantly different from one respondent to another, depending on settings of individual computers.
- Sampling of e-mail addresses is difficult. There are no directories. Sometimes there is more than one e-mail address per respondent. Addresses are not standardized.
- The decision not to respond is likely to be made more quickly.

Self-Check Exercise

Question XI:

Checkboxes doesn't allow multiple answers. (True/False)

8.8 Design Guidelines for Web-Based Surveys

- Utilize a multiple contact strategy much like that used for regular mail surveys.
- Personalize contacts through e-mail if possible.
- Keep the invitation brief.
- Begin with an interesting, but simple to answer, question.
- Introduce a Web survey with a welcome screen that is motivational, emphasizes the ease of response, and instructs about how to proceed to the survey.
- Present each question in a conventional format similar to that normally used on paper, self-administered surveys.
- Do not require respondents to provide an answer to each question before being allowed to answer subsequent questions.
- Make it possible for each question, and corresponding potential responses to that question to be visible on the screen at one time.

Self-Check Exercise

Question XII:

Multiple contact strategy is similar as _____ survey.

8.9 Data mining from social networking sites

Social networking site is a term used to describe web-based services that allow individuals to create a public or semi-public profile within a domain such that they can communicatively connect with other users within the network.

Social networks are considered to be important sources of online interactions and contents sharing, subjectivity, assessments, approaches, evaluation, influences, observations, feelings, opinions and sentiments expressions borne out in text, reviews, blogs, discussions, news, remarks, reactions or some other documents.

Data mining is the process of analyzing data from different perspectives and summarizing it into useful information, information that can be used to increase revenue, cuts costs or both. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships

identified. Technically data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.

Mining social media is a new plan to boom business. The Social media houses vast amount of user generated data which can be used for data mining. Marketing enthusiasts are searching for means to utilize these mined business information for the intake of their sales or marketing and advertising teams. The mined information from social platforms can considerably impact business strategy of any business enterprise.

Social media has vast amount of user-generated data which can be utilized for data mining. Data mining of social media can amplify use of social media and perk up commercial intelligence to transport enhanced services. For example, data mining techniques can identify user sentiments for anticipatory preparation to develop suggestion systems for business of specific products and even to build new friendships or connect certain interest groups. Marketing experts are searching for means to utilize them for their sales and advertising teams.

Self-Check Exercise

Question XIII:

Data Mining does not allows users to analyse data from different dimensions or angles. (True/False)

Question XIV:

Can we use social media data for Data Mining? (True/False)

Summary

- Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers, assisting in customer retention and driving sales growth.
- CRM software consolidates customer information and documents into a single CRM database so business users can more easily access and manage it.
- Using the Internet to conduct quantitative research presents challenges not found in conventional research.
- Secondary sources consist of data that has already been produced and can be contemporary or historical, qualitative or quantitative.
- An online focus group is one type of focus group, and is a sub-set of online research methods.
- A Web-based survey is the collection of data through a self-administered electronic set of questions on the Web.
- Social networking site is a term used to describe web-based services that allow individuals to create a public or semi-public profile within a domain such that they can communicatively connect with other users within the network.
- Data mining is the process of analyzing data from different perspectives and summarizing it into useful information, information that can be used to increase revenue, cuts costs or both.

Glossary

- GeoLocation Technology
- Database
- Hacking
- Steeling data
- Electronic survey

- Keywords
- Data Mining
- Auto biography
- Research
- Review

Questions

Q.1 What is CRM? What are its features?

Q.2 Explain the role of information technology in CRM.

Q.3 What are the various tools for conducting online research?

Q.4 What is CRM software? What are its features?

Q.5 What are advantages and disadvantages of using information technology in CRM?

Q.6 Write down the features of questionnaire in conducting an online research survey.

Q.7 Define secondary research. Explain its advantages and disadvantages.

Q.8 What are online focus groups? What are the advantages and disadvantages of online focus groups?

Q.9 Explain web based surveys. Also describe its advantages and disadvantages.

Q.10 Describe briefly the design guidelines for web based surveys.

Q.11 Define data mining. How is it useful in social networking sites?

Answers to Self-check Exercise

Question I: Recording various customer information and auto mailing

Question II: Yes

Question III: CRM

Question IV: Massive Databases

Question V: True

Question VI: True

Question VII: Yes

Question VIII: False

Question IX: Research and Experiment

Question X: Online Focus Group

Question XI: True

Question XII: Regular mail surveys

Question XIII: True

Question XIV: True

Chapter 9

ENTERPRISE RESOURCE PLANNING AND SECURITY ISSUES

Objectives

- Introduction
- Characteristics of ERP System
- Functional Areas of ERP
- Security Issues in e-commerce
- Tools to provide secure e-commerce
- Cyber Law
- Need for cyber law
- Cyber Crimes / Cyber Frauds
- Definition of cyber crime
- Types of cyber frauds

9.1 Introduction

Enterprise resource planning (ERP) is business management software—usually a suite of integrated applications—that a company can use to collect, store, manage and interpret data from many business activities, including:

- Product planning, cost
- Manufacturing or service delivery
- Marketing and sales
- Inventory management
- Shipping and payment

ERP provides an integrated view of core business processes, often in real-time, using common databases maintained by a database management system. ERP systems track business resources—cash, raw materials, production capacity—and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across the various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data. ERP facilitates information flow between all business functions, and manages connections to outside stakeholders.

Enterprise system software is a multi-billion dollar industry that produces components that support a variety of business functions. IT investments have become the largest category of capital expenditure in United States-based businesses over the past decade. Though early ERP systems focused on large enterprises, smaller enterprises increasingly use ERP systems.

The ERP system is considered a vital organizational tool because it integrates varied organizational systems and facilitates error-free transactions and production. However, ERP system development is different from traditional systems development. ERP systems run on a variety of computer hardware and network configurations, typically using a database as an information repository.

9.2 Characteristics of ERP System:-

ERP (Enterprise Resource Planning) systems typically include the following characteristics:

- An integrated system that operates in (or near) real time without relying on periodic updates a common database that supports all applications
- A consistent look and feel across modules
- Installation of the system with elaborate application/data integration by the Information Technology (IT) department provided the implementation is not done in small steps.

Self-Check Exercise

Question I:

ERP stands for _____.

Question II:

We can implement ERP system with small steps. (True/False)

9.3 Functional Areas of ERP:-

An ERP system covers the following common functional areas. In many ERP systems these are called and grouped together as *ERP modules*:

- Financial accounting: General ledger, fixed asset, payables including vouchering, matching and payment, receivables cash application and collections, management, financial
- Management accounting: Budgeting, costing, cost management, activity based costing
- Human resources: Recruiting, training, payroll, benefits, diversity management, retirement, separation
- Manufacturing: Engineering, bill of materials, work orders, scheduling, capacity, workflow management, quality control, manufacturing process, manufacturing projects, manufacturing flow, product life cycle management
- Order Processing: Order to cash, order entry, credit checking, pricing, available to promise, inventory, shipping, sales analysis and reporting, sales commissioning.
- Supply chain management: Supply chain planning, supplier scheduling, order to cash, purchasing, inventory, claim processing, warehousing (receiving, put away, picking and packing).
- Project management: Project planning, resource planning, project costing, work breakdown structure, billing, time and expense, performance units, activity management
- Customer relationship management: Sales and marketing, commissions, service, customer contact, call centre support - CRM systems are not always considered part of ERP systems but rather Business Support systems (BSS).
- Data services : Various "self–service" interfaces for customers, suppliers and/or employees

Self-Check Exercise

Question III:

Functional areas of ERP are also called _____.

9.4 Security Issues in e-commerce:-

The massive increase in the uptake of ecommerce has led to a new generation of associated security threats, but any ecommerce system must meet four integral requirements:

a) Privacy – information exchanged must be kept from unauthorized parties

b) Integrity – the exchanged information must not be altered or tampered

c) Authentication – both sender and recipient must prove their identities to each other and

d) Non-repudiation – proof is required that the exchanged information was indeed received.

These basic maxims of ecommerce are fundamental to the conduct of secure business online.

1. Privacy:-

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for ecommerce providers. According to Consumer Reports Money Adviser, the US Attorney General has announced multiple indictments relating to a massive international security breach involving nine major retailers and more than 40 million credit- and debit-card numbers. US attorneys think that this may be the largest hacking and identity-theft case ever prosecuted by the justice department. Both EU and US legislation at both the federal and state levels mandates certain organizations to inform customers about information uses and disclosures. Such disclosures are typically accomplished through privacy policies, both online and offline

2. Integrity, Authentication & Non-Repudiation:-

In any e-commence system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business. Data integrity is the assurance that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during transmission. Authentication is a means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place. Proof of data integrity is typically the easiest of these factors to successfully accomplish.

3. Technical Attacks:-

Technical attacks are one of the most challenging types of security compromise an e-commerce provider must face. Perpetrators of technical attacks, and in particular Denial-of-Service attacks, typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, large online retailers and popular social networking sites.

Denial of Service Attacks

Denial of Service (DoS) attacks consists of overwhelming a server, a network or a website in order to paralyze its normal activity. Defending against DoS attacks is one of the most challenging security problems on the Internet today. A major difficulty in thwarting these attacks is to trace the source of the attack, as they often use incorrect or spoofed IP source addresses to disguise the true origin of the attack.

The United States Computer Emergency Readiness Team defines symptoms of denial-of-service attacks to include:

- Unusually slow network performance
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received

5. Non-Technical Attacks:-

Phishing Attacks

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing scams generally are carried out by emailing the victim with a ‘fraudulent’ email from what purports to be a legitimate organization requesting sensitive information. When the victim follows the link embedded within the email they are brought to an elaborate and sophisticated duplicate of the legitimate organizations website. Phishing attacks generally target bank customers,

online auction sites (such as eBay), online retailers (such as Amazon) and services providers (such as PayPal).

Self-Check Exercise

Question IV:

Can we maintain the integrity of data after it has been altered? (True/False)

Question V:

_____, _____ and _____ are critical factor of any successful online business.

Question VI:

Denial of Service (DoS) is _____.

Question VII:

Major difficulty in preventing technical attacks is to trace _____.

Question VIII:

IP spoofing is the main reason behind inevitableness of DoS attack. (True/False)

Question IX:

Phishing attacks are generally target _____ and _____.

9.5 Tools to provide secure e-commerce services:-

Different initiatives in the area of providing secure e-commerce fall under the different banners of privacy, identification, authentication and authorization. Let's examine a few of these initiatives.

- Secure Sockets Layer (SSL): Netscape Communications Corporation developed this security protocol, designed to reduce the chances that information being sent through the Internet would be intercepted. It does not offer a means to confirm the customer, merchant or financial institution involved in a given transaction.
- Platform for Privacy Principles**:** Known as P3, it supported by the World Wide Web Consortium, the Direct Marketing Association and, in the beginning, Microsoft. This developing standard tries to define and describe limits on the culling and use of users private information garnered from Web sites.
- Tokens: Small devices, usually the size of a credit card or calculator that the remote users physically carry with them. Based on a challenge-response system, when the remote user tries to log on a given authentication server a challenge is issued. The user keys the challenge into the device which then generates the correct reply. The user then sends this response to the remote server to gain access.
- Secure Electronic Transaction (SET): Developed by MasterCard and Visa, working in conjunction with partners including IBM, Microsoft, GTE, Netscape and others. It is an open, multi-party protocol, transmitting bank card payments via open networks like the Internet. SET allows the parties to a transaction to confirm each other's identity. Employing digital certificates, SET allows a purchaser to confirm that the merchant is legitimate and conversely allows the merchant to verify that the credit card is being used by its owner. It also requires that each purchase request include a digital signature, further identifying the cardholder to the retailer. The digital signature and the merchant's digital certificate provide a certain level of trust. SET is important because it offers protection from repudiation and unauthorized payments.
- Digital Certificates: Purchasers and retailers generate these certificates through the bilateral use of secret keys that authenticate the legitimacy of each party to the transaction. The majority of digital certificates conform to the CCITT (ITU) standard X.509v3. Many major companies that

develop GroupWare products, such as Lotus, Novell and Microsoft, have decided that the X.509 standard is the best choice for the securing of information on the Internet. Also employed by GTE Service Corporation and VeriSign, digital certificates that are X.509 compliant are thought to strengthen both simplicity and interoperability.

- Open Profiling Standard for Authorization and Single Sign-On (OPS): Supported by Firefly, Netscape and VeriSign, it obviates the necessity for customers to reenter information that identifies them more than once at a Web site.

Self-Check Exercise

Question X:

P3 is also known as _____.

Question XI:

SSL is developed by _____.

Question XII:

Can tokens provide secure ecommerce service? (Yes/No)

Question XIII:

Digital certificates are used for _____.

9.6 Cyber Law

Cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

Self-Check Exercise

Question XIV:

Main purpose of cyber law is _____.

Question XV:

Information Technology Act, 2000 is also known as _____ or _____.

9.7 Need for cyber law:-

Firstly, India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. However the arrival of Internet signalled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. Despite the brilliant acumen of our master draftsmen, the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws. Secondly, the existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects

relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, there is a need for enactment of relevant cyber laws. Thirdly, none of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law. Fourthly, Internet requires an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth. All these and other varied considerations created a conducive atmosphere for the need for enacting relevant cyber laws in India.

Self-Check Exercise

Question XVI:

Arrival of internet signalled the beginning of rise of _____ and _____ legal issues.

9.8 Cyber Crimes / Cyber Frauds:-

The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life. Fraud is the intentional deception of a person or group for the purpose of stealing property or money. Internet fraud includes any scheme using Web sites, chat rooms, and email to offer nonexistent goods and services to consumers or to communicate false information to consumers. Customers then pay for the fraudulent goods over the Internet with their credit cards. Internet fraud involves a wide variety of schemes limited only by the imagination and creativity of a seller intent on deceiving a buyer. A few general characteristics one can find in all cyber scams. Most scams are done by e-mail. They entice users to give them critical information like usernames, passwords, credit card information, or other types of account information. Cyber fraud has the potential of hindering the economic and social development of any nation. This is because among other dire consequences, foreign investment is seriously discouraged. Cyber fraud can also destroy our good and morally sound culture. This is because the youth will no longer work but resort to that means to earn their living.

Self-Check Exercise

Question XVII:

Most scams are done through emails. (Yes/No)

Question XVIII:

Can cyber fraud destroy goods and culture? (True/False)

9.9 Definition of cybercrime:-

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

The OECD Recommendations of 1986 included a working definition as a basis for the study: Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

Self-Check Exercise

Question XIX:

Cybercrime is also called as _____ crime.

Question XX:

Illegal transmission of data also comes under category of _____.

9.10 Types of cyber frauds:-

A wide variety of scams operate in the online environment, ranging from fraudulent lottery schemes, travel and credit-related ploys, modem and web page hijacking, and identity theft (ID theft) to name but a few. Many of these scams, such as pyramid selling, are simply online variants of fraudulent practices that have long existed offline. However, the Internet has given criminals access to a worldwide base of consumer targets as well as more opportunities to elude enforcement as they need not be in the same country, or even in the same hemisphere, as their victims. The Internet allows fraudsters to masquerade as legitimate traders behind professional-looking websites or on virtual auction sites to advertise “free” or “bargain” prices, “miracle” products, and “exciting” investment and business opportunities. These deceptive and misleading offers trick unsuspecting consumers into buying goods and services on line which turn out to be far less than promised or even non-existent. Many online scams originate in spam messages – usually through e-mail, but sometimes through text messages (SMS), voice messages delivered by Internet (Voice-over Internet Protocol or – VoIP) or other electronic channels. Spam has evolved into a vehicle for the spread of fraud and other online abuses. Many email users will have received a message from a person claiming to be a government official or member of the royal family of a foreign country (usually in Africa), promising substantial sums of money in return for assistance in transferring money out of the country. Commonly known as the “Nigerian”, “West African” or “419” scam, once it has sucked in victims it convinces them to make small advance payments for various reasons, such as banking transaction fees. Needless to say, the victim never receives the promised substantial sums in return. Many pyramid and work-at-home schemes are also distributed through spam and follow the “advance fee fraud” format of requiring up-front payment or investment on the promise of high returns that are never forthcoming.

Spam is a key tool for the spread of ID theft, luring people into disclosing sensitive information such as credit card numbers or passwords. For example, phishing spams falsely claim to come from legitimate and well-known financial institutions or merchants. They ask recipients to click through on hyperlinks in order to verify or update their online accounts. These hyperlinks direct users to fake “look alike” websites where users are tricked into divulging personal information which can be used to access and illegally transfer money out of the victim’s bank account(s), open new bank or credit card accounts in the victim’s name, make unlawful online purchases, etc.

These attacks are continually becoming more sophisticated. The past year has seen the growth of a new practice known as spear-phishing where accurate information about the recipient, such as the full name and home address, is included in the phishing e-mail making it even more convincing. Another

new phenomenon known as phishing tricks people into making phone calls rather than clicking on links to websites. The number given is to a VoIP phone which records digits (such as account numbers) entered into the telephone, again enabling crooks to steal and use the information.

Other variants of fraud rely on the use of identity stolen through technological methods. For example, harming interferes with the domain name system (DNS) look up process and redirects users attempting to reach a particular website to a “spoofed” one where they divulge personal information to the crooks. Malware (or malicious software), can be downloaded unwittingly by consumers from spam attachments or as they surf on line. Such malicious code, which increasingly targets mobile phones and other portable devices in addition to computers, can install “key stroke” loggers and other programs to steal information stored on, entered into, or received by these devices. The information collected through these kinds of technological attacks, such as passwords and other sensitive data, can then be used to perpetrate fraud.

Following are some types of cyber crimes:

1. Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). (Delhi Public School case)

2. Sale of illegal articles:-

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of ‘honey’.

3. Online gambling:-

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported. Whether these sites have any relationship with drug trafficking is yet to be explored. Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound. After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

4. Intellectual Property crimes:-

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cyber squatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name ‘Yahooindia.Com’ deceptively similar to its ‘Yahoo.com’. As this case was governed by the Trade Marks Act, 1958, the additional defense taken against Yahoo’s legal action for the interim order was that the Trade Marks Act was applicable only to goods.

5. Email spoofing:-

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs

her e-mail and sends obscene messages to all her acquaintances. Since the e-mails A pear to have originated from Gauri, her friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money. Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days.

But the best example of the email spoofing can be given by an Executive's case, where he pretended to be a girl and cheated an Abu Dhabi based NRI for crores by blackmailing tactics.

6. Forgery:-

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates. Some of the students are caught but this is very rare phenomenon.

7. Cyber Defamation:-

This occurs when defamation takes place with the help of computers and/ or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company. The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

8. Cyber stalking:-

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

9. Unauthorized access to computer systems or networks:-

This activity is commonly referred to as hacking. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". However, as per Indian law, unauthorized access does occur, if hacking has taken place. An active hackers' group, led by one "Dr. Nuker", who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

10. Theft of information contained in electronic form:-

This includes information stored in computer hard disks, removable storage media etc.

11. Email bombing:-

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

12. Data diddling:-

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in his bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

13. Salami attacks:-

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month. To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems. Logic bombs are programmes, which get activated on the occurrence of a particular predefined event. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizeable amount of money being transferred into his account every Saturday. Being an honest person, he reported the "mistake" to the bank authorities and the entire scheme was revealed.

14. Denial of Service attack:-

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

15. Virus / worm attacks:-

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a

computer's memory. The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion. VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail which was sent out had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". People weary of opening email attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me". Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

16. Logic bombs:-

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

17. Trojan attacks:-

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. There are many simple ways of installing a Trojan in someone's computer. To cite an example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the 14th of February, he sent Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

18. Internet time theft:-

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa's login name and password from various places causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time. On further inquiry in the case, it was found that Krishan Kumar, son of an ex army officer, working as senior executive in M/s Highpoint Tours & Travels had used Col Bajwa's login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested Krishan Kumar under sections 379, 411, 34 of IPC and section 25 of the Indian Telegraph Act. In another case, the Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the

password of an Internet user, accessed the computer and stole 107 hours of Internet time from the other person's account. He was booked for the crime by a Delhi court during May 2000.

19. Web jacking:-

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website. In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

20. Theft of computer system:-

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system:-

This crime is committed by physically damaging a computer or its peripherals. This is just a list of the known crimes in the cyber world. The unknown crimes might be far ahead of these, since the lawbreakers are always one-step ahead of lawmakers.

Self-Check Exercise

Question XXI:

Fraudulent lottery schemes, web page hijacking is a type of cyber fraud. (Yes/No)

Question XXII:

Name of illegal articles on Sale are _____, _____ and _____.

Question XXIII:

Cyber pornography, online gambling, cyber stalking are types of cybercrime. (Yes/No)

Question XXIV:

Email bombing refers to sending a large number of email to victim, resulting in crashing the victim email account. (True/False)

Question XXV:

Salami attacks are used for commission of _____.

Question XXVI:

Virus is programs that attach themselves to _____.

Question XXVII:

Virus does not affect data on computer. (True/False)

Question XXVIII:

Trojan is also called _____.

Summary

All business processes are generally contained in ERP system. Any information that is stored in company's ERP might be stealed by cybercriminal, fraud or competitor.

This information may include financial, customer or public relation, Intellectual property, personally identifiable information, and so on. If got stealed it could cause significant damage for business

Glossary

- Warehouse
- Business Support System(BSS)
- Privacy
- Integrity
- Non-Repudiation
- Denial-of-services (DoS)
- Phishing attacks
- Tokens
- Open Profiling Standards (OPS)
- Cyber law
- Cyber crime
- Cyber stalking
- Identity theft (ID Theft)
- Web page hijacking
- Voice over Internet Protocol (VoIP)
- Malware
- Online gambling
- Email spoofing
- Salami attacks
- Logic Bombs

Questions

Q 1. Define Enterprise resource planning and give its characteristics.

Q 2. What are the various functional areas of an ERP System?

Q 3. Discuss various security issues e-commerce in context to privacy Integrity, Authentication & Non-Repudiation.

Q 4. Discuss technical and non-technical attacks in context to privacy of information in e-commerce.

Q 5. Discuss at least three tools to provide secure e-commerce.

Q 6. Discuss the need of cyber law give at least three reasons.

Q 7. What is a Trojan attack?

Q 8. Explain the effects of email-spoofing.

Q 9. Define the followings

(i) Tokens

(ii) Secure Electronic Transaction (SET)

(iii) Digital Certificates

Q 10. Describe Phishing Attacks and Denial of Service Attacks to e-commerce.

Answers to Self-check Exercise

Question I: Enterprise Resource planning

Question II: False

Question III: ERP Module

Question IV: False

Question V: Data Integrity, client authentication and Non-Repudiation

Question VI: Technical Attack

Question VII: Source of Attack

Question VIII: True

Question IX: Bank Customer, online auction site

Question X: Platform for privacy principle

Question XI: Netscape Communication Corporation

Question XII: Yes

Question XIII: Authentication of user

Question XIV: Provide Legal reorganisation to ecommerce

Question XV: ITA-2000, IT Act

Question XVI: New and complex legal issues

Question XVII: Yes

Question XVIII: True

Question XIX: Computer related

Question XX: Computer related crime

Question XXI: Yes

Question XXII: Narcotics, weapons and wildlife

Question XXIII: Yes

Question XXIV: True

Question XXV: Financial Crimes

Question XXVI: Computer files

Question XXVII: False

Question XXVIII: Unauthorised program

Chapter 10

INFORMATION TECHNOLOGY ACT, 2000

Objectives:

- Information Technology Act 2000

10.1 Information Technology Act 2000

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act,1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to, —

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;

(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;

(d) a will as defined in clause *(h)* of section 2 of the Indian Succession Act, 1925 ncluding any other testamentary disposition by whatever name called;

(e) any contract for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central

Government in the Official Gazette.

2. Definitions

(1) In this Act, unless the context otherwise requires, —

(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;

(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,—

(i) Enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) "computer network" means the interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(l) "Controller" means the Controller of Certifying Authorities appointed under sub-section of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section *(4)* of section 35;

(r) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message; "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

DIGITAL SIGNATURE

3. Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller,

set known' as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III

ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signatures.

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and

cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies.

(1) Where any law provides for—

(a) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued; the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause *(a)*

7. Retention of electronic records.

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette.

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6,7 and 8 not to confer right to insist document should be accepted in electronic form.

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established

by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature.

The Central Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.

An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt.

(1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of dispatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the

originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic, record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section, —

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

"usual place of residence", in relation to a body corporate, means the place where it is registered

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

14. Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including—

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(a) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.

The Controller may perform all or any of the following functions, namely:—

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities; specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(d) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(e) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key,

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities.

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository.

(1) The **Controller** shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(a) make use of hardware, software and procedures that are secure intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

21. Licence to issue Digital Signature Certificates.

(1) Subject to the provisions of sub-section

(2) any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(3) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government A licence granted under this section shall—

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence.

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence.

An application for renewal of a licence shall be—

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees,

as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence.

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of licence.

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,—

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the standards specified under clause *(b) of* sub-section of section 20;

(d) contravened any provisions of this Act, rule, regulation or order made there under revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him:

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

26. Notice of suspension or revocation of licence.

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such

suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.

Every Certifying Authority shall, —

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

32. Display of licence.

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

34. Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

Disclosure.

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

35. Certifying Authority to issue Digital Signature Certificate.

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by

the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection

36. Representations upon issuance of Digital Signature Certificate.

A Certifying Authority while issuing a Digital Signature Certificate shall certify that--

(a) it has complied with the provisions of this Act and the rules and regulations made there under,

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair,

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate.

(1) Subject to the provisions of sub -section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,—

(a) on receipt of **a request** to that effect *from*—

(i) the subscriber listed in toe Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber,

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section

(3) and without prejudice to the provisions of sub -section

(1) a CertifyingAuthority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent **or** dead or where a subscriber is a firm or a company, which has been dissolved, wound-up **or** otherwise ceased to exist

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation.

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate—

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay

to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX

PENALTIES AND ADJUD1CATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network; downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(b) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(c) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(d) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made there under to—

(a) furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; file any return or furnish any information, books or other documents within the time specified there for in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate.

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer' for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section

(1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58, and—

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

47. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—

a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

b) the amount of loss caused to any person as a result of the default;

c) the repetitive nature of the default

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he—

(a) is, or has been. or is qualified to be, a Judge of a High Court; or

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding

Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government

57. Appeal to Cyber Appellate Tribunal.

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of tony-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of tony-five days if it is satisfied that there was sufficient cause tor not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to" the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal.

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:—

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it *ex pane;*

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal

60. Limitation.

The provisions of the Limitation Act, 1963, shall, as far as may be, *apply* to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction.

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions.

(1) Any contravention under this Chapter may, either before or after the institution of

adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.—For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was

previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant

68. circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees **Power of Controller to give directions.**

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a Fine not exceeding two lakh rupees or to both.

69. Directions of Controller to a subscriber to extend facilities to decrypt information.

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

70. Protected system.

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars.

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for

any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention commited outside India.

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act. rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

77. Penalties or confiscation not to interfere with other punishments.

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. Network service providers not to be liable in certain cases.

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—"network service provider" means an intermediary; "third party information" means any information dealt with by a network service provider in his capacity as an intermediary use.

QUESTIONS

Q. 1 Explain IT act 2000

Q. 2 What is the penalty for damage to computer or its devices.

Q.3 Define secure electronic record.

Q.4 Explain the penalty for misrepresentation.

Q.5 Describe hacking the computer system.

Q.6 How is digital signature certificate accepted.

Q.7 What are the functions of the controller.

Q. 8 Explain retention of records.

Q.9 Describe the term affixing digital signature.

Q.10 What is a computer network.

ASSIGNMENT

Q. 1 Discuss how e-commerce has changed the outlook of the society.

Q.2 Elaborate Business models.

Q.3 Keeping in view the customer's perspective it is believed that the e-deals are beneficial. Do you agree. Justify.

Q.4 Describe the steps of e-payment.

Q.5 List the various activities of e-banking.

Q.6 Discuss the importance of search engine in advertising.

Q.7 Explain viral marketing, its role and issues related to it.

Q.8 Elaborate the significance of customer relationship management systems.

Q.9 What are the security issues in e-commerce.

Q.10 Write notes on digital signature and certifying authorities.