B.C.A SEMESTER - IV

(B.C.A -403)

ELECTRONIC COMMERCE (E-COMMERCE)

(NEW SYLLABUS MATERIAL)

INSB BCA & PGDCA COLLEGE, IDAR

CREATED BY:

Mr.SMIT TRIVEDI

ASST.PROF B.C.A,M.C.A

Unit 3: *[17 MARKS]*

Topics:

E-Payments and Security:

<u>A brief overview following</u> :

- ✓ **Credit Card ,**
- ✓ **Debit card**
- ✓ **Smart Card (Electronic Credit Card),**
- ✓ **EFT (Electronic Funds Transfer)**
- ✓ **E-Wallet ,**
- ✓ **E-check and E-cash .**
- ✓ **Payment Gateway**

- ✓ **<u>Security in Cyberspace</u>-**
  Kinds of threats and crimes

- ✓ **Credit Card Frauds and Internet security using VPN and Firewalls.**

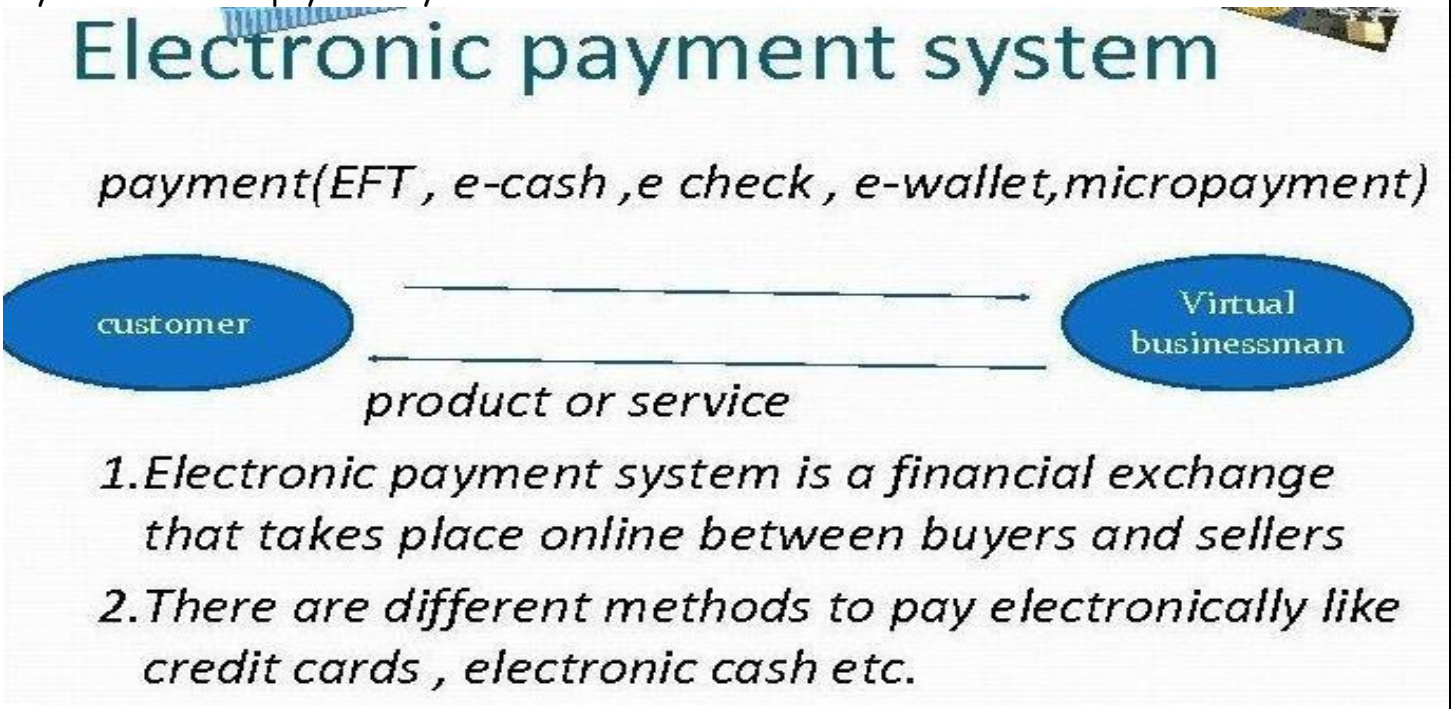
Topic-1 : Explain E-Payments and Security in detail

⇨ Introduction :

➔ Electronic payment system are online payment system.

➔ Used to transfer money over the internet.

➔An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It's also called an electronic payment system or online payment system.



➔Electronic Payment is a financial exchange that takes place online between buyers and sellers.

➔The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender.

Electronic payment system is a system which helps the customer or user to make online payment for their shopping.

- To transfer money over the Internet.
- Methods of traditional payment.
  - Check, credit card, or cash.
- Methods of electronic payment.
  - Electronic cash, software wallets, smart cards, and credit/debit cards.

Features Of E-Payment

➔Protecting customer from merchants scheme by keeping credit card number Unknown to merchants.
➔Allowing people without credit card to connect in online transactions.
➔Protecting confidentiality of customers.
➔In some cases providing secrecy(Secret) of customers.

Electronic payment system must provide :

(1) **Privacy**: Details about any transaction must be kept securely away from Unauthorized parties and stop transaction can expose a center to fraud or Theft.
➔privacy is usually ensure by using encryption techniques.

(2) **Integrity:** integrity can be ensured using digital signature and certificate.

(3) **Authentication:** the sender must me confident that the receive are who they say They are and vice versa.
➔Authentication is vital to prevent fraud .

(4) **Non Repudiation:** the ability to prove that a transaction has been made
an important aspect of trust is the ability for senders to prove they have made the Payment .
➔this can be done using receipts.

➔ The various factors that have lead the financial institutions to make use of electronic payments are:

Topic-2 : Explain a brief overview of the following

(1) Credit Card (2) Debit Card (3) Smart Card (Electronic Credit Card) (4) EFT (Electronic Funds Transfer) (5) E-Wallet (6) E-check (7) E-cash

➔ The various types of E-payment systems are given below in detail.

(1) Credit Card

➔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.

- It is a Plastic Card having a Magnetic Number and code on it.
- It has Some fixed amount to spend.
- Customer has to repay the spend amount after sometime.

Figure 1,2,3,4 :

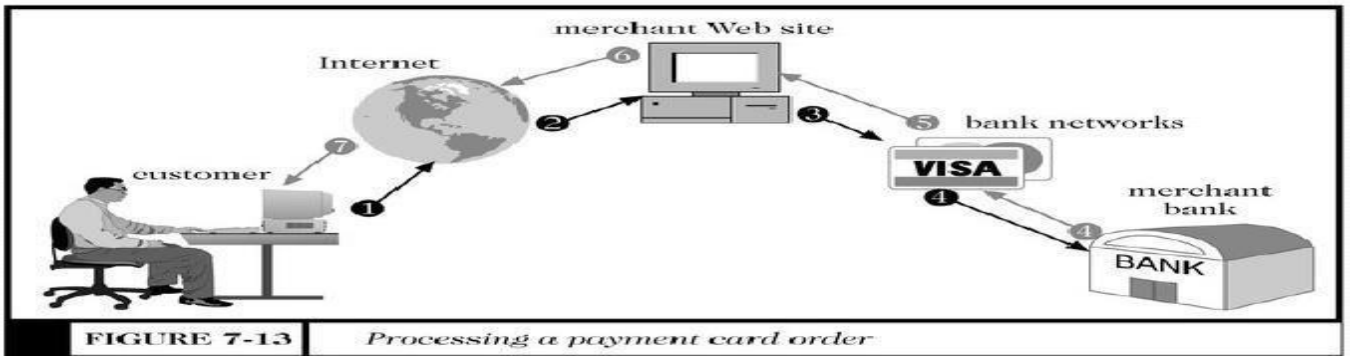


FIGURE 7-13 *Processing a payment card order*

Advantages

(1) Purchase large items :It can be difficult to save for expensive items, such as computers, TV's etc. Using a credit card allows us to pay it off bit by bit, over a number of months in a much more affordable way.

(2) Deal with emergencies: Things go wrong and credit cards are great to have available to cover emergencies such as paying for plumbing or electrical problems that need fixing urgently.

(3) Safety: Many credit cards offer card protection against fraudsters and stolen details. When you are internet shopping, or even buying from shops, this added protection can provide real peace of mind.

(4) Rewards: Credit card companies offer many incentives to using their card to shop with. Including such things as Air Miles, money back offers, vouchers for use in certain shops, prize draws and many more. These are things that you don't get when using debit cards or cash.

(5) Offer free use of funds, provided you always pay your balance in full, on time.
(6) Be more convenient to carry than cash.
(7) Help you establish a good credit history.
(8) Provide a convenient payment method for purchases made on the Internet and over the telephone.
(9) Give you incentives, such as reward points, that you can redeem.

Disadvantages:

(1) Interest: Because of credit card companies charging interest you will be paying off more than you borrowed, and if you are only making the minimum payments you will be paying off a lot more than you borrowed.

(2) Future earnings: By using credit cards you are basically borrowing against future earnings, assuming that you will be able to pay off that amount in the future. If you lose your job, become ill etc. you may well not be in a position to pay off the amount borrowed.

(3) Legal work : If you are unable to make the regular payments owed, for whatever reason, you can be faced with legal consequences, solicitors looking to take you to court, This can cost you money, stress and have a real impact upon your life.

(4) Credit rating. If you miss any payments it can have a negative impact upon your credit rating. This rating is used to determine if you are able to get loans, credit cards and mortgages. Having a positive credit rating is considered vital in modern times, the last thing you want is any negative impact.

(5) Cost much more than other forms of credit, such as a line of credit or a personal loan, if you don't pay on time.
(6) Damage your credit rating if your payments are late;
(7) Allow you to build up more debt than you can handle;
(8) Have complicated terms and conditions;

(2) Debit Card

➔Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number.

➔ Debit Card is also known as ATM Card and it is used for online shopping, online bill payments etc. Without going **bank** we can withdraw money from ATM machine with the help of debit card.
➔It is required to have a bank account before getting a debit card from the bank.

➔The major difference between a debit card and a credit card is that in case of Payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

➔Debit cards free the customer to carry cash and cheques.

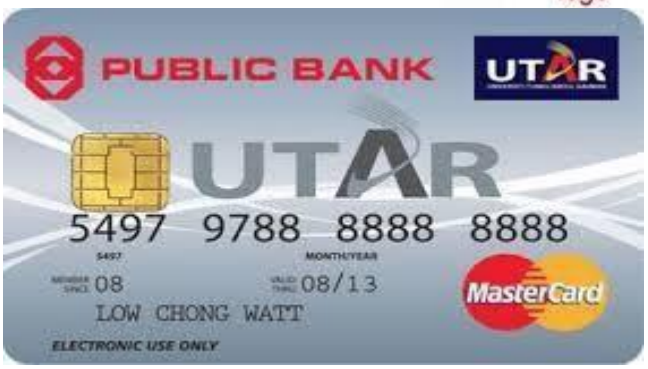
➔Even merchants accept a debit card easily.

➔Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

➔ This type of card, as a form of payment, also removes the need for checks as the debit card immediately transfers money from the client's account to the business account.

➔Debit cards are also considered to be a safer form of payment as a code is required to access the account funds, while checks can be easily stolen.

Figure 1 , 2 :



Advantages

1. **No need to carry cash:** Just about every merchant accepts the debit card and some thrift shops. You do not need to worry about losing cash or misplacing it . If your purse or wallet is stolen your money is safe since the perpetrator would need your PIN number to access your funds.

2. **You don't need to make a trip** to the bank every time you need to withdrawal money. You can use your card just about anywhere you go, and if you need the cash you can access your money at an ATM machine any time of day or night.

Disadvantages

1. With a debit card you must keep accurate records. You must record each transaction so you will know what your account balance is at all times. If you do not keep records you run the risk of overdrawing your account which will result in bank fees. Not to mention the discomfort you will suffer at the checkout line when your card is denied.

2. If your child needs lunch money you can't just hand them the debit card. You have to drive to the nearest ATM machine to access a few rupees to send to school with your child.

3. Some ATM machines charge a fee for their use and then your bank adds another foreign ATM charge (if the machine is not from your bank). Know ahead of time what the fees are and where you can access your money for free if possible.

(3) Smart Card (Electronic Credit Card)

➔Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it.
➔It has the capacity to store a customer's work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.
➔ Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing.
➔Mondex and Visa Cash cards are examples of smart cards.
➔Smart Cards enable information for different purposes to be stored in one location.
➔Stored value cards.
➔Can hold private user data.
➔Can store about 100 times more information than a magneticstrip plastic card.
➔Available for over 10 years.
➔So far not successful in U.S .But popular in Europe, Australia and Japan.
➔Unsuccessful in U.S. partly because few card readers available.
➔Smart card gradually reappearing in U. S. success depends on.

Types of smart card

1. **Contact**
2. **Contact Less**

(1) Contact :

➔These are the most common type of smart card.
➔Electrical contacts located on the outside of the card connect to a card reader when the card is inserted.
➔This connector is bonded to the encapsulated chip in the card.

(2) Contact Less

➔A **contactless smart card** is a contactless credential whose dimensions are credit-card size.

➔Its embedded integrated circuits can store (and sometimes process) data and communicate with a terminal.

➔ Commonplace uses include transit tickets, bank cards and passports.

Figure 1 , 2 :

➔ The most common smart card applications are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- Satellite TV
- Government identification

What are the advantages and disadvantages of smart cards?

Advantages:

1. Larger memory.
2. High levels of security.
3. Reduced fraud.
4. Organized information.
5. Reliability.
6. Information Security.
7. Ease of use without need for connections online or via telephone.
8. User comfort.
9. Privacy.

Disadvantages:

1. A more powerful virus.
2. Discomfort to retrieve information from a stolen card.
3. For its size can be easily misled.
4. The card must be recharged.
5. Increased cost of production.
6. Bank fees associated with credit card.
8. We need a smart card reader.
9. Not widely used.
10. Fees applied with the use of a card
11. It gives liability issues if stolen or lost.
12. The accuracy of information is small.
13. Lack of technology to support users
14. potential for too much data on one card if lost or stolen .
15. potential area for computer hackers and computer viruses

(4) EFT (Electronic Funds Transfer)

➔Electronic funds transfer (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer-based systems, without the direct intervention of bank staff.

➔EFT transactions are known by a number of names across countries and different payment systems.

➔**For example**, in the United States, they may be referred to as "electronic checks" or "e-checks".

➔PayPal, online bill pay, and mobile payments are all examples of recent advancements.

➔These changes are referred to as electronic funds transfer, or the electronic transfer of money from one account to another.

➔Electronic funds transfer uses computer systems to move funds without the need for paper documents.

Figure 1 , 2 ,3

For example, when you use your debit card to make a purchase at a store or online, the transaction is processed using an EFT system. The transaction is very similar to an ATM withdrawal, with near-instantaneous payment to the merchant and deduction from your checking account.

➔Direct deposit is another form of an electronic funds transfer. In this case, funds from your employer's bank account are transferred electronically to your bank account, with no need for paper-based payment systems.

Advantages :-

• **Direct deposit:** This is perhaps the most common type of payment. Most companies in the United States today pay their employees via direct deposit instead of paper check. Direct deposit is also

used by government entities to make Social Security and other benefit payments and to issue refunds to taxpayers.

- **Direct debits and credits:** These types of electronic payments can be made from business-to-consumer and from business-to-business. Consumers pay many recurring bills, such as utilities, insurance, and health club memberships and many businesses pay their vendors and suppliers .
- **Federal, state, and local taxes:** EFT has become a common funds transfer mechanism for the payment of corporate taxes at all levels of government.

Disadvantages : -

➔ The major disadvantages is the risk of security issues. Electronic banking's largest adversary is the hackers who try to steal the customer's information and money.

➔When the account has been compromised, money can be stolen. Hackers can also use the information obtained to steal one's identity.

(5) E-wallet

Definition:

" E-wallet is a type of electronic card which is used for transactions made online through a computer or a smartphone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments".

Descriptions:

➔ E-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction.

➔An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

➔E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data.

➔The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc.

➔For setting up an E-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user's information on the payment form.

➔To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.

Figure 1 , 2 ,3

Advantages

- The e-wallet makes online shopping easier because it fills in the fields in an online order form automatically, saving you the trouble of doing it yourself.
- This is also a great advantage for online merchants, because customers sometimes abandon online purchases if they feel that the order form is too confusing or frustrating.
- The e-wallet can overcome this phenomenon by automating the completion process.

Disadvantages

- If you try to use the e-wallet with an online order form whose blank fields are in a different order from those in your e-wallet, or if the form has fields that the e-wallet does not recognize, the form may be left incomplete or be completed incorrectly.
- This would force you to erase all the fields and enter your personal information manually, defeating the purpose of the e-wallet.

(6) E-Check

➔ E-cheques are a mode of electronic payments.
➔ E-cheques work the same way as paper cheques and are a legally binding promise to pay.
➔Electronic cheques address the electronic needs of millions of businesses, which today exchange traditional paper cheques with the other vendors, consumers and government.

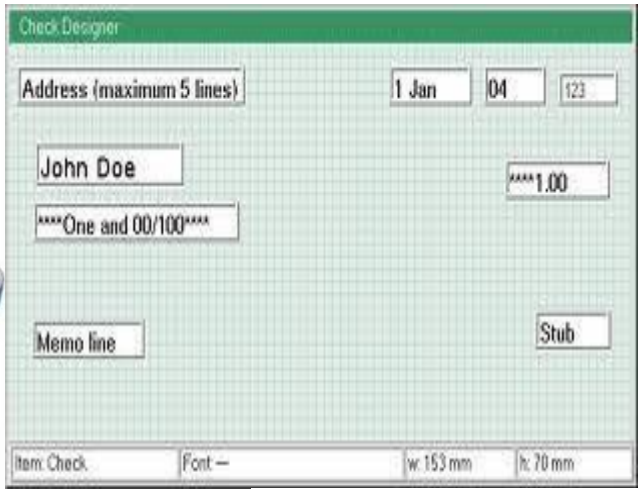
Working of E-cheques

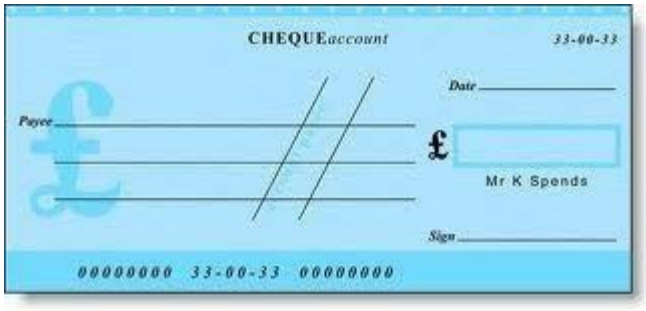
➔ E-cheques work the same way as paper cheques and are a legally binding promise to pay. The payment system uses digitally signed XML documents that provide mechanism to authenticate parties to a transaction.

➔E-cheques are defined using FSML (financial services markup language) which allows for addition and deletion of document blocks, signing, co-signing, endorsing, etc.

➔Signatures are accompanied by bank-issued certificates which tie the signer's key to a bank account.

Figure 1,2,3,4





Advantages of E-cheques

➔It seems that consumers would gain from having E-cheques available to make payments for online purchases. The online merchants on the other hand could receive payments instantly and since the customer's bank will be involved in the transaction.

➔It would be impossible for an E-cheques to bounce.

➔Banks can do paperless, efficient transactions.

Disadvantage of E-cheques

➔ The problems come when your merchant does not accept E-cheques.

➔ The other problem could be when you have more than one signer or endorser.

(7) E-Cash

➔ **Electronic money** is money that is exchanged electronically. This involves the use of computer networks, the internet and digital stored value systems.

➔ Bank deposits, electronic funds transfer (EFT), direct deposit, payment processors, digital currencies such as bitcoin are all examples of electronic money.

➔ E-cash is used over the Internet, email, or personal computer to other workstations in the form of secured payments of "cash" that is virtually untraceable to the user. It is backed by real currency from real banks.

➔The way e-cash works is similar to that of electronic fund transfers done between banks. The user first must have an e-cash software program and an e-cash bank account from which e-cash can be withdrawn or deposited.
➔The user withdraws the e-cash from the account onto her computer and spends it in the Internet without being traced or having personal information available to other parties that are involved in the process.

➔ The recipients of the e-cash send the money to their bank account as with depositing "real" cash.
➔Electronic cash is a secure.

Figure 1,2,3:-

Advantages of E Cash

- Electronic cash transactions are more efficient and less costly than other methods
- The distance that an electronic transaction must travel does not affect cost.
- The fixed cost of hardware to handle electronic cash is nearly zero.
- Electronic cash does not require that one party have any special authorization

Disadvantages :

➔ These can include fraud, failure of technology, possible tracking of individuals and loss of human interaction. No doubt, fraud over digital cash has been a pressing issue in recent years.

➔ Hacking into bank accounts and illegal retrieval of banking records has led to a widespread invasion of privacy and has promoted identity theft. There is also a pressing issue regarding the technology involved in digital cash.

➔ Power failures, loss of records and undependable software often cause a major setback in promoting the technology.

Topic-3 : Explain Payment Gateway in detail.

➔A **payment gateway** is a merchant service provided by an e-commerce application service provider that authorizes credit card or direct payments processing for e-businesses, online retailers, bricks and clicks.
➔The payment gateway may be provided by a bank to its customers, but can be provided by a specialized financial service provider as a separate service, such as a payment service provider.
➔A payment gateway facilitates a payment transaction by the transfer of information between a payment portal (such as a website, mobile phone or interactive voice response service) and the front end processor or acquiring bank.
➔The payment gateway protects the details on a credit card by encrypting the sensitive information it holds.
➔This process ensures that personal private details are passed securely between the customer and the merchant.
➔When a customer orders a product from a payment gateway-enabled merchant, the

payment gateway performs a variety of tasks to process the transaction.

1) A customer places an order on website by pressing the 'Submit Order' or equivalent button, or perhaps enters their card details using an automatic phone answering service.

2) If the order is via a website, the customer's web browser encrypts the information to be sent between the browser and the merchant's web server. In between other methods, this may be done via SSL (Secure Socket Layer) encryption.

3)The merchant then forwards the transaction details to their payment gateway. This is another (SSL) encrypted connection to the payment server hosted by the payment gateway.

4) The payment gateway converts the message from XML to ISO 8583 or a variant message format (format understood by EFT Switches) and then forwards the transaction information to the payment processor used by the merchant's acquiring bank.

5) The payment processor forwards the transaction information to the card association.

6) The credit card issuing bank receives the authorization request, verifies the credit or debit available and then sends a response back to the processor (via the same process as the request for authorization) with a response code.

7) The processor forwards the authorization response to the payment gateway.

8) The payment gateway receives the response, and forwards it onto the website, or whatever interface was used to process the payment, where it is interpreted as a relevant response, then relayed back to the merchant and cardholder. This is known as the Authorization or "Auth."

9) The entire process typically takes 2–3 seconds.

10)The merchant then fulfills the order and the above process can be repeated but this time to"Clear" the authorization by consummating the transaction.

11) the merchant submits all their approved authorizations, in a "batch" (end of the day), to their acquiring bank for settlement via its processor. This typically reduces or "Clears" the corresponding "Auth" if it has not been explicitly "Cleared."

12) The acquiring bank makes the batch settlement request of the credit card issuer.

13)The credit card issuer makes a settlement payment to the acquiring bank (the next day in

most cases).

14) The acquiring bank subsequently deposits the total of the approved funds into the merchant's nominated account (the same day or next day).

15) The entire process from authorization to settlement to funding typically takes 3 days.

Figure 1

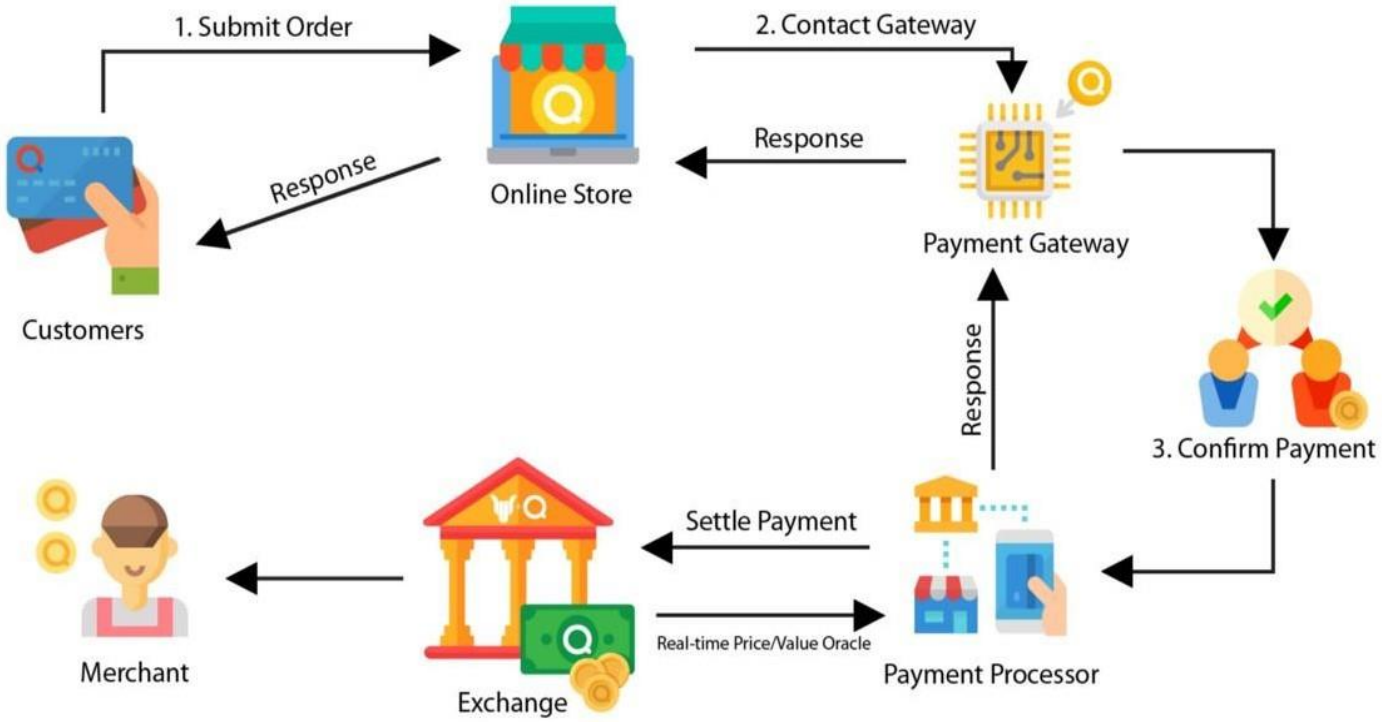
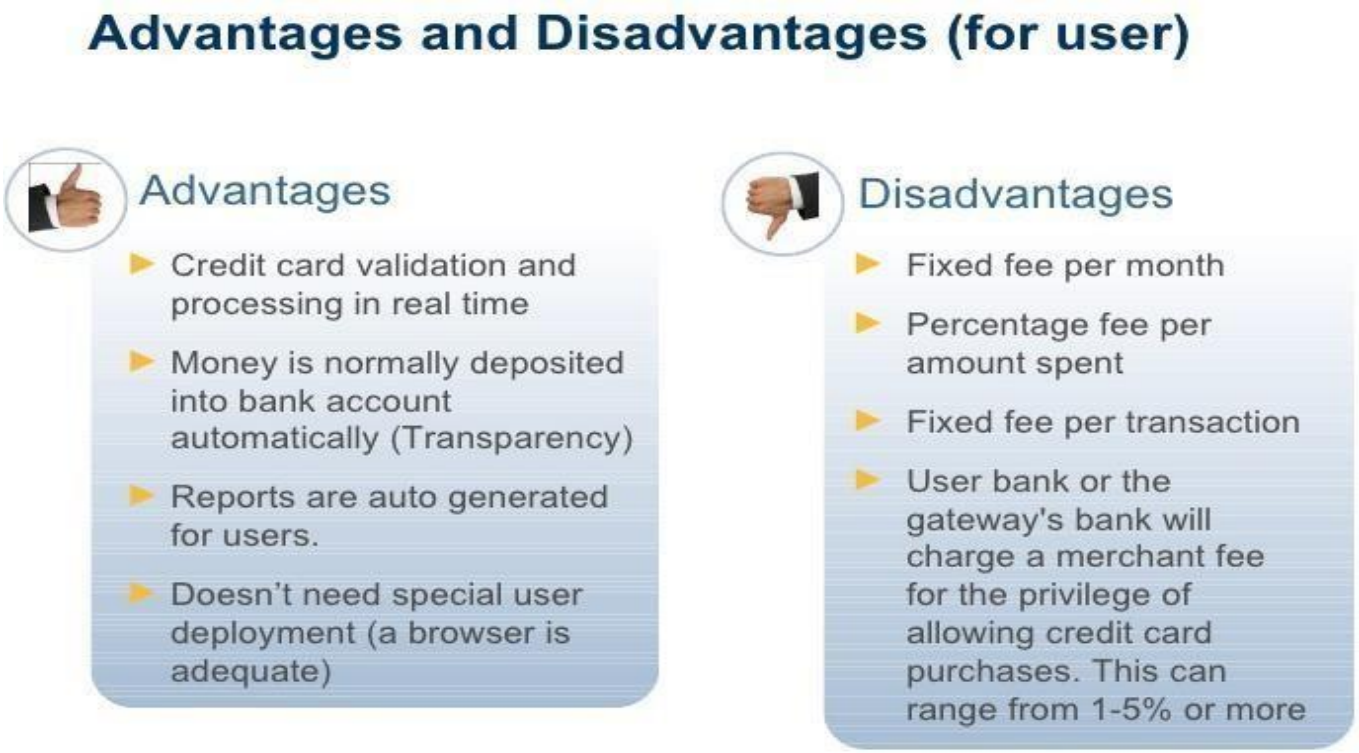


Figure 2



Topic-4 : Explain Security in cyberspace – kinds of threats and crimes in detail.

➔Today, the Internet has become a source of information that no country or company can forgo. It is not only used to communicate or entertain, but most importantly to operate utilities and public services such as banking or air traffic. As the reliance on computer networks across societies and economies keeps growing, so do **security risks** in cyberspace - referred to as "cybersecurity."

DEFINITION OF CYBER SECURITY OR (COMPUTER SECURITY)

➔ "Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. "Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation."

Description: Major areas covered in cyber security are:

1) Application Security

2) Information Security

3) Disaster recovery

4) Network Security

Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance.

Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: **a)** Identification, authentication & authorization of user, **b)** Cryptography.

Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Network security components include: **a)** Anti-virus and anti-spyware, **b)** Firewall, to block unauthorized access to your network.

Cyber Security : kinds of threats

Types of Cyber Security Threats.

- ✓ Malware
- ✓ Phishing
- ✓ Man-in-the-middle
- ✓ Denial-of-service attacks
- ✓ SQL Injection attack
- ✓ Cross-Site Scripting
- ✓ Ransomware
- ✓ Password Attack
- ✓ Trojan Horses
- ✓ Drive-By Download Attack

1 Malware

Malware is considered as software that deliberately developed to disrupt computers, servers, and other computer networks.

- ✓ Blocks access to key components.
- ✓ Install harmful software.
- ✓ Steal valuable information from your system
- ✓ can damage certain hardware components.

2 Phishing

Phishing is a form of social engineering commonly used to steal user data such as credit card numbers and credentials for logging in.

- ✓ Take fraudulent action to cheat users.
- ✓ Steal restricted and private information.

Man-in-the-middle

3

In Man-in-the-middle (MitM), the invader can modify the chats and dialogues between two individuals who communicate with each other.

- ✓ Interference from the third party.
- ✓ Modify chats

Denial-of-service attacks

4

In Denial-of-service attacks, the offender to attempt to make digital assets unavailable to its expected users in a denial-of-service attack.

- ✓ Make digital assets inaccessible
- ✓ Using different IP addresses

SQL Injection attack

5

In the SQL Injection attack, the intruder can access the data and can easily add, modify, and delete the data from the database.

- ✓ Personal data
- ✓ Intellectual property
- ✓ Customer information
- ✓ Trade secrets, and more.

Cross-Site Scripting

6

In Cross-Site Scripting, the intruders sent malicious code to different users by embedding them into a trusted site, usually as a browser-side script.

- ✓ Browser-side script
- ✓ Access to personal data

Ransomware

7

Ransomware is a kind of malware attack that restricts access to your devices or files and displays a pop-up message that demands payment for the restriction to be removed.

- ✓ Restricts access to devices
- ✓ Contains malicious attachments.

Password Attack

8

Passwords are the main gateways to enter into your personal accounts securely. The passwords are usually connected to our life's incidents, people, and places that can easily sniff and gain access to our unencrypted passwords.

- ✓ Unencrypted passwords.
- ✓ Enter personal accounts

Trojan Horses

9

Trojans are considered among the most dangerous types of all malware, as they are often designed to steal financial information.

- ✓Influence a victim to install it.
- ✓They are specially designed to steal financial information.

Drive-By Download Attack

10

Drive-by –download attack is a commonly used method to spread malicious scripts or codes on users' systems. These scripts will be automatically installed in the system or might redirect to a website that is controlled by the attacker.

- ✓Automatically installed
- ✓Spread malicious scripts

Topic : Cyber Security : kinds of crimes

➔ Cybercrime also refers to any activity where crime is committed using any **computer system**.

Cyber criminals are publicly known as hackers.

What are the different kinds of cybercrime?

Here are some of the most common ways systems and networks get attacked every day.

(1) Identity theft

➔Also known as identity fraud, It starts with someone stealing your identity, allowing digital criminals to use identifiable data including your name, driver's license, social security information and more — to commit fraud, steal property, misappropriate goods or use services in your name.

(2) Illegal data

➔The Internet is full of illegal content: this includes all data restricted by international laws from around the world.

➔ Examples of illegal content include child and animal-related material, selling drugs online and copyrighted materials (such as videos, music, books, software, etc).

(3) Crime against the Individuals

➔Crimes against the individual refers to those criminal offences which are committed against the will of an individual to cause certain harm to them like physical or mental harm. For example harassment, kidnapping etc. but in cyber crimes the nature of crimes against individual changes a little bit and takes the form of cyber stalking, pornography, cyber bulling, child abuse, fraud, cyber threats etc. Such as cyber defamation is committed to cause harm to the reputation of an individual in the eyes of other individuals through the cyberspace. A few cybercrimes against individuals are:

1. Harassment via electronic mails.
2. Dissemination of obscene material.
3. Cyber-stalking.
4. Defamation.
5. Indecent exposure.

6. Cheating.
7. Unauthorized control/access over computer system.
8. Email spoofing.
9. Fraud.

(4) Crime against Governments or Organizations

➔There are certain cyber-crimes committed to threaten the international governments or organizations. These cyber-crimes are mainly committed for the purpose of spreading terror among people of a particular country.

➔Cybercrimes against Government include cyber-attack on the government website, military website or cyber terrorism etc. In these kinds of cyber-crime, cyber criminals hack governments or organization's websites, government firm, and military websites and then circulate propaganda or threats or rumors. Following are the few examples of crime against Governments or Organizations: (1) Unauthorized access / control over computer system.(2) Cyber terrorism against the government or organization.

(5) Crime against Society

➔Those cyber-crimes which affect the society at large are known as cybercrimes against society. These unlawful acts are committed with the intention of causing harm or such alterations to the cyberspace which will automatically affect the large number of people of society. The main target of these types of crimes is public at large and societal interests. The cybercrimes against society include the following types of crimes:

1. Indecent exposure of polluting the youth financial crimes.
2. Sale of illegal articles.
3. Trafficking.
4. Forgery.
5. Online gambling.
6. Web jacking.

(6) Crime against Property

➔businesses and consumers are increasingly using computer and the internet to create, transmit and store information in the electronic from instead of traditional form.

➔ These types of cybercrimes include cyber tracing to steal information of other organizations or to steal someone's bank details, use software to gain access to an organization's website etc.

➔This is similar to instances of a criminal illegally possessing an individual's bank or credit card details.

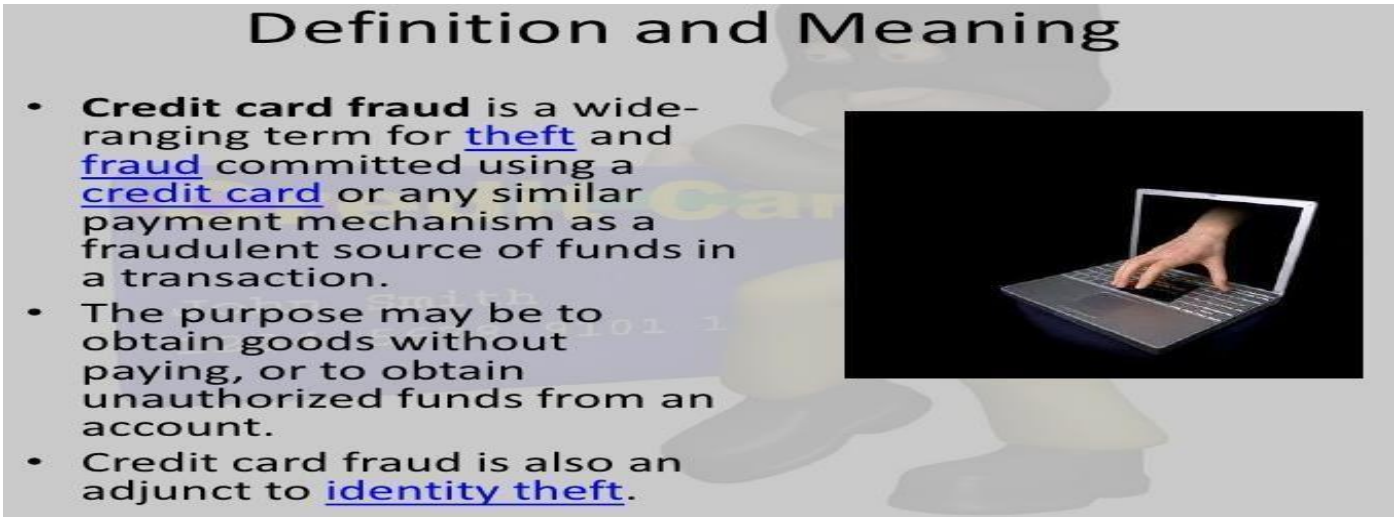
➔In cyber-crime, the hacker steals a person's bank details to gain access to funds, make purchases online to get people to give away their information.

➔They could also use any kind of malicious software to gain access to a web page with confidential information. These types of crimes include tracing of computers, intellectual property crimes (Copyright, patented, trademark etc), online threatening etc. Cybercrimes against property include:

1. Computer tracing.
2. Transmitting virus.
3. Net-trespass.
4. Unauthorized access / control over computer system.
5. Internet thefts.
6. Intellectual Property crimes:

- Software piracy.
- Copyright infringement.
- Trademark infringement.

Topic-5 : Explain Credit Card Frauds in detail.



Types of Frauds

- 1. Counterfeit credit card

  Makes up for 37% of all funds lost through credit card frauds. To make fake cards criminals use the newest technology to "skim" information contained on magnetic stripes of cards and to pass security features such as holograms

- 2. Lost or Stolen Cards

  Cards stolen from their cardholders or lost by them account for 23% of all card frauds. Often, cards are stolen from the workplace, gym, and unattended vehicles

- 3. No-Card Fraud

  Comprises 10% of all the losses and is completed without the physical card in hand. This can happen by giving your credit card information on the phone to shady telemarketers and deceptive Internet sites that are promoting the sales of their non-existent goods and services.

- 4.Non-Receipt Fraud

  Is responsible for 7% of all losses. It occurs when new or replaced cards mailed by your card company are stolen during the process of being mailed.

- 5.Identity Theft Fraud

  Accounts for 4% of all losses, and occurs when criminals apply for a card using someone else' identity and information

Topic-6 : Explain Internet security using VPN in detail.

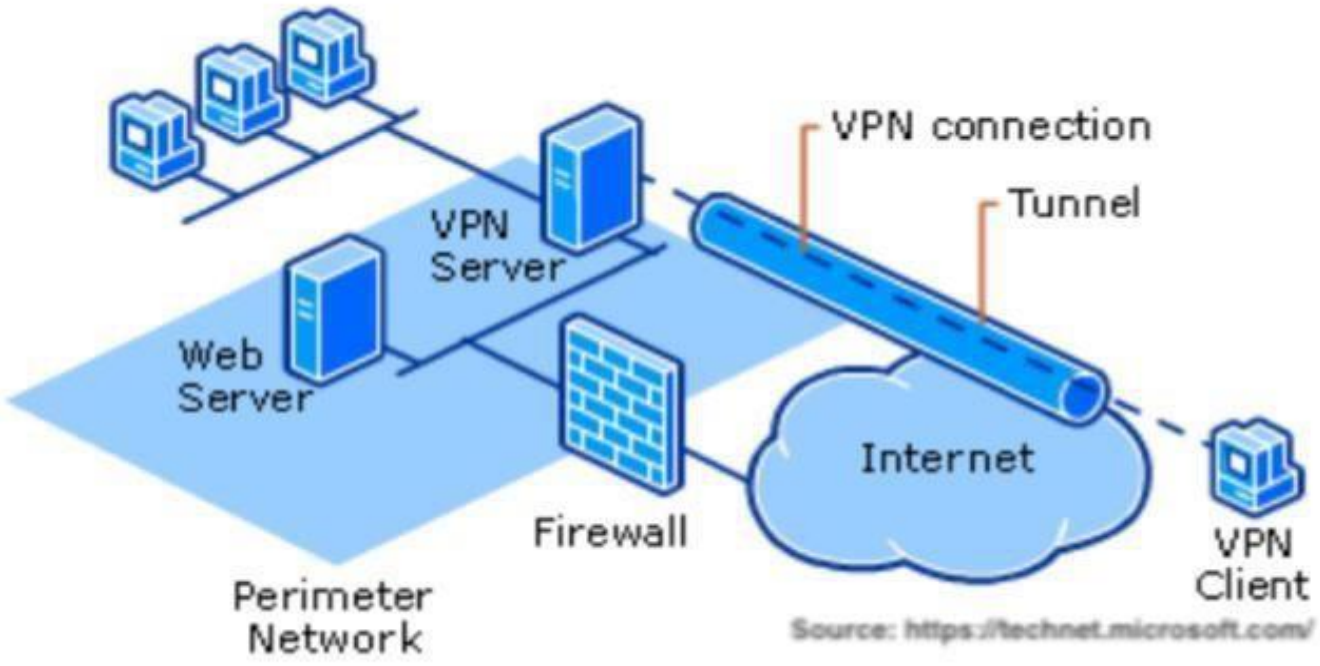
➔ A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel.

➔This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks.

- ➔ A VPN is the easiest solution in all cases wherein an economical, isolated, secure, private network needs to be created or accessed over the Internet
- ➔ A VPN allows you to leverage existing centralized network security infrastructure to provide a unified defense against cyber threats throughout the company's networked devices regardless of location
- ➔ A VPN provides secure access to needed internal services for a mobile workforce increasing their productivity
- ➔ A VPN reduces security risk by allowing access to specific network resources to only users who are authorized, encrypting data and thereby protecting against insecure Wi-Fi access, and providing continuity of centralized unified threat management.
- ➔ computing technology, and pervasiveness of the Internet, it became possible to encrypt data traffic and tunnel it over the Internet to a server located in the private network.
- ➔ The secure tunnel creates a virtual link which extends the private network over a public network.
- ➔ This kind of network that makes use of public networks to provide private network connectivity is called **Virtual Private Network (VPN)**.
- ➔ VPN or Virtual Private Network has been associated from private network to public network. VPN could access from any place any time through server by sending and receiving across internet.
- ➔ The company could reduce cost from communicate and time with company's branch.
- ➔ In addition, employees don't need to travel to other place for receiving data.

Figure-1 :

Figure-2 :



➔ A VPN can make use of one of many technologies such as Internet Protocol Security (IPsec) to securely connect devices or networks, over public networks, in order to extend or form a private network.

➔ The same technology that is used to create virtual connectivity between networks can also be used to connect a user's devices to a private network.

➔A common use of VPNs is to provide remote employees secure access over the Internet to their company's IT services. Employees use VPN clients installed on corporate laptops or mobile devices to connect to a VPN server that is present in the company's private network.

➔The remote access use case is not limited to access for employees. Any Internet-connected device can use a VPN to be a part of a private network.

➔Devices can range from normal computing devices like laptops to specialized industrial sensors or consumer electronics like smart TVs.

Topic-7 : Explain Internet security using firewalls in detail.

➔ In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

➔A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

➔ "A Firewall is a software-based network security system that helps to protective and control suspicious incoming and outgoing traffic network such as hacker, viruses, Trojans, and other by analyzing the data and determining whether they should be allowed thorough or not, based on options".

Figure :

Nowadays, people are connected to internet world which grant you're comfortable to do any financial and personal information. In the meantime, your data is in vulnerable to access information by hacker and other malicious attack.

A firewall has a great deal of functions owing to research and development following:

1. Protect an attack from any traffic.
2. Prevent the data or IP address hide to protect hosts
3. Keep important information to be not leak out from insider
4. Controlling user only the applications they need
5. Keep log to substantiate true identity log server

****