Cyber space

Content…

- Definition of cyber space
- Origin of cyber space
- Threat to cyber space
- Solution for threats
- Advantages of cyber space
- Disadvantages of cyber space

Definition of cyber space

- Cyber space refer to the virtual computer world, and more specially is an electronic medium used to form a global computer to facilitate online communication.
- It is large computer network made up by many worldwide computer networks that employ TCP\ IP protocol to aid in communication and data exchange activities.
- In effect , cyber space can be thought of as the interconnection of human begins through computers and telecommunication, without regard of physical geography.

Origin of cyber space

- The tern cyber space fist appeared in the visual art in the late 1960s, when Danish artist **Susanne Ussing** (1940-1998)and her partner architect **Carsten Hoff** constituted themselves as a atelier cyberspace. Atelier cyberspace worked at a time when the internet did not exist and computers were more or less off-limit to artists and creative engagement.

Threats In cyber space

- Cyber crime
- Hacking
- Cyber terrorism
- Cyber espionage

1.Cyber crime
cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense.
Examples - hacking , phishing, spamming , hate crimes etc

2.Hacking
Hacking is the act of breaking into a computer system for a politically or socially motivated purpose. The individual who perform an act of hacking is said to be hacker. It can also be said as unauthorized excess over a system.

3. Cyber terrorism
Cyber terrorism is the use of internet based attacks in terrorist activities , including acts of deliberate , large scale disruption of computer networks especially of personal computers attached to the internet by the means of tools such as computer.

4. cyber espionage
Unauthorized spying by computer. The term generally refer to the development of viruses that clandestinely observe or destroy data in the computer system of government agencies and large enterprises

Solution for threats

- Use different user id\password combination for different accounts and avoid writing them down.
- make the password more complicated by combining letters , numbers, special characters(minimum 10 characters in total) an change them on regular basis.
- Firewalls are the first line of cyber defense ; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- Prevent viruses from infecting our computer by installing and regularly updating anti-virus software.

Advantage of cyber space

- Unlimited communication
- Abundant information and resources
- Easy sharing
- Online services and e-commerce

1.Unlimited communication

The internet has made it easy for people to communicate with other because it is cheap and convenient. As such people are able to share their thought and views on matters affecting the globe. The internet acts as common global platform where people explore ideologies and cultures without limitation.

2. Abundant information and resources

the internet is swamped with information about anything and everything. There are multiple searches engines that have made it easier for internet users to find information. For example it is now common for people to look for free advice from the internet on all sorts of issues

3.Easy sharing

Internet sharing information is fast and seamless. We can use social media sites such as Facebook or an IM app for sharing information , they will all get the news at the same time. We can also share music, videos, and any other files.

4.Online services and E-commerce

Today it is possible to carry out financial transactions online. We can transfer funds, pay taxes and utility bills or book movie tickets over the internet in the comfort of our office or the home.

Disadvantages of cyber space

- Software vulnerabilities
- Data vulnerabilities
- Interruption of privacy
- Remote access
- Crosses all geographical boundaries
- Assists crime

Definition

- Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication.
- It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.
- Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

Threats in Cyberspace

- Hacktivism
- Cybercrime
- Cyberespionage
- Cyberterrorism

Hacktivism

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a ***hacktivist.***

Acts of hacktivism may include website defacement, denial-of-service attacks (DoS), website parodies, information theft, virtual sabotage and virtual sit-ins.

Cybercrime

❖Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

❖Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes.

❖ Criminals can also use computers for communication and document or data storage.

❖Criminals who perform these illegal activities are often referred to as hackers.

Cyber espionage

Unauthorized spying by computer. The term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large enterprises.

Cyber terrorism

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as comp

Advantages of Cyberspace

- Informational resources
- Entertainment
- Social networking

Informational resources

The Internet is a virtual library of information. We can get any kind of information on any topic that we desire, it will be available on the Internet.

Entertainment

Entertainment is another popular reason why many people prefer to surf the Internet. We can download games and music instead of going out of our comfort zone to get the latest and the game or CD. There are numerous games that can be downloaded for free.

Social networking

Social networking also plays a major role in cyberspace. One cannot imagine an online life without Facebook or Twitter. Social networking has become so popular amongst youth that it might one day replace physical networking. It has evolved as a great medium to connect with millions of people with similar interests.

Disadvantages of Cyberspace

Personal Information: If we use the Internet, our personal information such as name, address, etc. can be accessed by other people. If we use a credit card to shop online, then our credit card information can also be 'stolen' which could be akin to giving someone a blank check.

Pornography

This is a very serious issue concerning the Internet, especially when it comes to young children. There are thousands of pornographic sites on the Internet that can be easily found and can be a detriment to letting children use the Internet.

Spamming

This refers to sending unsolicited e-mails in bulk, which serve no purpose and unnecessarily clog up the entire system.

Solution for Threats:

Use Strong Passwords:

Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

Secure your computer

- Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- Prevent viruses from infecting our computer by installing and regularly updating anti-virus software.
- Prevent spyware from infiltrating our computer by installing and updating anti-spyware software

- Make sure your social networking profiles (e.g. Face book, Twitter, YouTube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
- Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

Ethics in Cyber Space

What are Ethics anyway?

- Understanding how your actions affect other people
- Knowing right from wrong
- Taking personal responsibility for your actions

- So , "Ethics is about putting principles into action. Consistency between what we say and ... what our actions say... is a matter of integrity."

What do we mean by CYBERETHICS ?

- **Cyberethics** is the philosophic study of ethics pertaining to computer networks, encompassing user behaviour.
- what networked computers are programmed to do, and how this affects individuals and society.
- Cyber-Ethics is the Ethics applied to the online environment.

Why should we be Concerned about Cyber Ethics ?

- Anonymous posting to blogs, websites and social media can encourage bad behaviour anytime.
- Information in cyberspace can be accessed globally.
- what is right and wrong for Internet users can do,
- what are the social impacts of Information Technology (IT).
- understand security, privacy issues, and major negative impacts of IT on cyberspace
- Computer Networks can be threatened by many internal and external hazards internationally,

Why Cyber Ethics ?

Cyber Ethics underpin actions that must be taken not only to harness the power of the IT itself, but also to survive its revolution so it should be the concern of everyone.

Let's review and discuss some common cyber-ethical concerns…

Acceptable Use Policy (AUP) Violations

- Disregard for technology or network rules and policies. This could be willful or unintended disregard.

Piracy

- Unauthorized duplication and distribution of items such as games, software, DVDs, music, etc.
- End User License Agreement Violation : When you purchase a game or CD, you are purchasing license to *USE* them; you do not *OWN* them.

Plagiarism

- Using another person's ideas, words, images, or original works as your own without acknowledging the source.

Cyber-bullying

"Cyber-bullying" is when a child or teen is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another child or teen using the Internet, interactive and digital technologies, or cell phones.

Cyber-libel

- Deliberate misrepresentation of people or events.
- False statements that harm another's reputation.

Worms and Viruses

- Malicious programs shared with the intent of shutting down a computer or computer system.

Violating Privacy

- Willfully using another person's password to access his or her email or documents online, distributing private information of or about another.

Cyber-stalking

- The use of the Internet, email, or other electronic communications devices to stalk another person.

Call into Questions…

- Is it ok to display personal information about other on the Internet ?
- Who owns digital data (such as music, movies, books, webpages etc.) and what should users be allowed to do with it ?
- Who is allowed to access the data and information?
- How can we safeguards to ensure that the information can be accessed only by the right person or organizations?

Who should be Concerned about Cyber Ethics ?

- businesses and governments rely on technical measures to protect themselves from false information, stealing, deny access, or even destroy valuable information.
- Self-protection is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced.
- Cyber ethics must be taught and reinforced at every level of computer use
- From the novice user just learning to navigate a computer and the internet, to an information technology professional
- Those who use the internet in any mode must be taught ethical practices in every aspect of its use

The Rules of Ethical Cyber Activity

- Basic Rule - Do not do something in cyber space that you would consider wrong or illegal in everyday life
- Do not use rude or offensive language
- Do not be a bully on the Internet. Do not call peoples name, lie about them, send embarrassing pictures of them, or anything else to try to heart them.
- Don't encourage the cyberbullies. Do report cyberbullying.
- Do use internet for research and information but don't use copyrighted information as your own.

The Rules of Ethical Cyber Activity

- Do not break into someone else's computer.
- Do not attempt to infect or in any way try to make someone else's computer unusable.
- Don't share personal information too easily.
- Do use the internet to expand your social and business network but don't hamper other in doing so.

CONCLUSION

- The new world of information society with global networks and cyberspace will inevitably generate a wide variety of social, political, and ethical problems.
- Basic issues have been solved partially using technological approaches and legal laws in cyberspace.
- Guidelines and strategies should be implemented so that global information can be exploited in a socially and ethically sensitive way for our future benefit and applications.

Cyber Law

- Cyber law is a term used to describe the legal issues related to use of communications technology.
- It is also known as “internet law” is the area of law that regulates how people use the internet.
- It is rule which controls the conducts of the cyber activity & the security under the cyber space

Need of cyber law

- Internet has dramatically changed our life .
- Transition from paper to paperless world.
- Law of real world cannot be interpreted in the light of emerging cyberspace.

Cyber crime

- Any crime with the help of computer and telecommunication technology.
- Any crime where either the computer is used as an object or subject.

Importance of cyber law

- We are living in highly digitalized world.
- All companies depends upon their computer networks and keep their valuable data in electronic form.
- Government forms includes income tax returns, company law forms etc are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.

IT ACT 2000

- The information technology act 2000, came into force on 17 October 2000.
- The primary purpose of the act is deals with cybercrime and electronic commerce in India.
- It is based on United Nation Model Law on electronic commerce 1996.
- Information technology act 2000 consisted of 94 sections segregated into 13 chapters.

Special attractions of the ITA 2000

- Even the persons of other nationalities can also be indicated under the law, if the crime involves a computer or network located in India.

Objective of the ITA 2000

- The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.
- Facilitate the electronic filing of documents with Government agencies and also departments.
- Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions.
- Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.
- Aims to provide the legal framework to all electronic record.

Cyber Contravention

- Cyber Contraventions are 'civil wrongs' for which compensation is payable by the defaulting party.
- Cyber contravention may lead to civil prosecution
- Covered under (section 43-45) of the Act, this deals with illegal access to computer system or network
- The offender may be charged with a fine up to Rs. 1 Crore.

Cyber Offence

- Cyber offences on the other hand constitute cyber frauds and crimes which are criminal wrongs for which punishment of imprisonment and/or fine is prescribed by the Information Technology Act 2000.
- Cyber offences may result in criminal prosecution.
- Covered under (Sections 65-74) of the Act, this deals with serious cyber crimes related to computer system and network
- The criminal can be punished with confinement, fine or both.

Case studies

Case 1:

CBI Website Hacked In an incidence, it was reported in year 2013 that the official website of CBI was hacked for few hours.


Central Bureau of Investigation

Ooooppsss! WTF? CBI? Cyber Crime? Hacked? hahaha funny a

A message by Pakistan Cyber Army

Pakistan Zindabad!

Section 43 and section 66 of the IT Act cover the civil and criminal offenses of data theft or hacking respectively.

CONTRAVENTIONS

Section 43:Penalty and compensation for damage to computer, computer system, etc.

If any person who damage to system without permission of the owner or any other person who is in charge of a computer, computer system or computer network.

(a) accesses or secures access to such computer, computer system or computer network or computer resource.
(b) 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.
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programme residing in such computer, computer system or computer network.
(e) disrupts or causes disruption of any computer, computer system or computer network.
(f) denies or causes the denial of access to any person authorized 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.
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Section 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

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

If any person who is required under this Act or any rules or regulations made thereunder 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.

(b) file any return or furnish any information, books or other documents within the time specified therefor 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

Case 2:

The Ministry of Women & Child Development has taken note of Two instances of fak website where some perpetrators created fake websites using name and logo of the Ministry and advertised vacancies of teachers and other posts. In both cases, the applicants were requested to pay examination fee online through the websites. The Ministry lodged FIR with Delhi Police in both cases which were registered by Delhi Police under Section 420 of the IPC and Section 66-D of the IT Act. As informed by the Delhi Police, the person involved in one case was arrested and sent to judicial custody.

OFFENCES

Section 65 – Tampering with Computer Source Documents

Any person tamper, conceal, destroy, or alter any computer source document intentionally, then he shall be liable to pay penalty upto **Rs.2,00,000/-**, or Imprisonment upto **3 years**, or both.

Related Case:

29 JUL, 2005 , ***Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh*** In this case, Tata Indicom. employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.
Verdict: *Court held that tampering with source code invokes Section 65 of the Information Technology Act.*

Section 66 – Computer Related offenses

Related Case:

Kumar v/s Whiteley In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users. Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers. The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorized use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.
Verdict: *The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).*

Section 66A – Punishment for sending offensive messages through communication service

Any person who sends, by means of a computer resource or a communication device,-
(a) any information that is grossly offensive or has menacing character.

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device.

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.-For the purposes of this section, terms —electronic mailll and electronic mail messagell means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 66A – Punishment for sending offensive messages through communication service

Case #1:

Fake profile of President posted by imposter On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook.The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Case #2:

Bomb Hoax mail In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

Section 66B- Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C – Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66C – Punishment for identity theft

Case #1:

Fake profile of President posted by imposter On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook.The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Case #2:

Bomb Hoax mail In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

Section 66D – Punishment for cheating by impersonation by using computer resource

- ***Relevant Cases:***
- On June 12, minister G. Kishan Reddy approached the Hyderabad police complaining that on May 20 he had received threatening calls twice on his mobile phone. The anonymous caller had used an international sim to make the call. The police had registered a case under Section 66D ITA Act-2008 and Section 506, 507 IPC.
- The investigation finally led to the arrest of the accused who had gone to Kuwait in 2017 to work as a driver. While on the job, Ismail started watching speeches of political leaders and news on social media platforms.
- He later searched for contact information of Kishan Reddy, who won as MP of Secunderabad, and made the call as an anonymous person.

Section 66D – Punishment for cheating by impersonation by using computer resource

- Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E – Punishment for violation of privacy

- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
- Explanation.-For the purposes of this section-

(a) Transmit means to electronically send a visual image with the intent that it be viewed by a person or persons.

(b) capture, with respect to an image, means to videotape, photograph, film or record by any means.

Section 66E – Punishment for violation of privacy

- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
- Explanation.-For the purposes of this section-

(a) Transmit means to electronically send a visual image with the intent that it be viewed by a person or persons.

(b) capture, with respect to an image, means to videotape, photograph, film or record by any means.

Section 66E – Punishment for violation of privacy

(c) private area means the naked or undergarment clad genitals, public area, buttocks or female breast.

(d) publishes means reproduction in the printed or electronic form and making it available for public.

(e) under circumstances violating privacyll means circumstances in which a person can have a reasonable expectation that

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured.

(ii) (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66E – Punishment for violation of privacy

- ***Relevant Cases:***

Nagpur Congress leader's son MMS scandal On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

Section-66F Cyber Terrorism

- with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-
- denying or cause the denial of access to any person authorized to access computer resource.
- attempting to penetrate or access a computer resource without authorization or exceeding authorized access.
- (iii) introducing or causing to introduce any computer contaminant

Section-66F Cyber Terrorism

- ***Relevant Cases:***

The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case. The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday. The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna," said an officer.
Status: *The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act.*

Section 67 – Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted 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 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 three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

Section 67 – Punishment for publishing or transmitting obscene material in electronic form

- ***Relevant Cases:***

Karnataka achieved its first conviction in a cyber crime case under Section 67 of the Information Technology (IT) Act on Friday, September 7. The verdict came in a case relating to a decade-old incident which involved a software engineer who had sent obscene emails and photographs of his victims from a cyber cafe. Interestingly, the engineer accused in the case had quit his job and turned into a lawyer so that he could defend himself in the court. The convict Shivaprasad Sajjan has been sentenced to two years imprisonment and fined for Rs 25,000 after he was found guilty by the ACMM Court under Section 67 of the Information Technology Act. [Shivaprasad Sajjan vs State (2018)]

- **News #1:** A Keralite gets 3 years in Jail for snooping through camera (July 2017):

The Kozhikode First Class Judicial Magistrate Court sentenced a youth to three years of imprisonment and fined ₹20,000 in connection with his involvement in an incident in which a mobile phone camera was placed in the women's toilet of a restaurant seven years ago. The court found Akhil Jose, 29, a former employee with Hotel Sagar on Mavoor Road under 67 and other relevant provisions of the Information Technology Act.

- **News #2:** Kolkata man held for Cyber Stalking former classmate for over 9 years:

Kolkatta Police received a complaint from a Delhi based girl's father that the accused Tushar Kumar Biswas, who was former classmate of her daughter in a well reputed Law School, has been cyber stalking her since 2008. Tushar Kumar had propsed the girl in the past but could not take the rejection and therefore, have been continously stalking her online on various social media sites, harassed through email as well by sending her across obscene photos and clips. The matter has been registered under section 66C/67A of Information Technology Act and also various section of Indian penal Code!

Section-68: . 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 thereunder.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.

Section-69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

69A. Power to issue directions for blocking for public access of any information through any computer resource

69B. Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security

Section-69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Case: In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut.The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m. ***Verdict:*** *Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.*

Section 70: Protected system

The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system, Any person who fails to comply with the notification, then he shall be liable to Imprisonment of **10 years**, along with the **fine**

Section 71: Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or 1 [electronic 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.

Section 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, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, 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.

Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars.

No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

- the Certifying Authority listed in the certificate has not issued it.
- (b) the subscriber listed in the certificate has not accepted it.
- (c) the 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.

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 1 lakh rupees, or with both.

Section 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.

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.

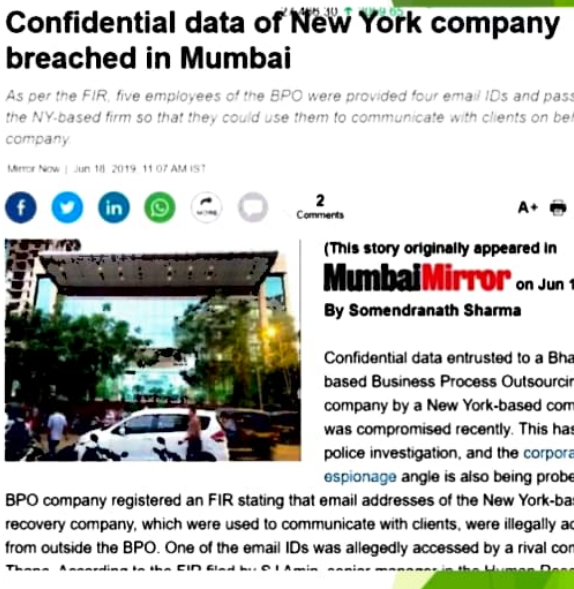
CASE:

- The Central Bureau of Investigation (CBI) has lodged an FIR in connection with illegal phone tapping of several politicians and officers of Karnataka.
- The phone-tapping controversy came to light during the elections when an alleged phone conversation was leaked to the media in which an IPS officer was named.
- Names of senior Congress leader Ahmed Patel and former PWD Minister HD Revanna of the JD(S) had also figured in the leaked phone tapes.
- The CBI has lodged an FIR on the request of Karnataka government against unknown public servants and private persons.
- Before CBI, the case was being investigated by the Cyber Crime Police Station of Bangalore under section 72 of the Indian Technology Act, 2000 and Section 26 of Indian Telegraph Act, 1885.

CASE:

Sub-Division Police Officer (SDPO) (Mira-Bhayander) Atul Kulkarni said that it could be a case of corporate espionage by a competitor. "Epicenter Technology has lodged a complaint on June 13 and the confidential data is suspected to have been given to competitors. We are probing the role of some of the employees of the BPO who had access to the email IDs. We are recording statements of the employees who had left the BPO and are also probing if there was any hacking of email IDs etc.

A case has been registered under sections 43A (Compensation for failure to protect data), 66C (identity theft), 66D (cheating by personation by using computer resource) and 72A (disclosure of information in breach of lawful contract) of Information Technology Act against unknown persons," said Kulkarni.



The Consumer Protection Act, 1986

Introduction

1. Lok Sabha : 9th December, 1986
2. Rajya Sabha : 10th December, 1986
3. Assented by the President of India : 24th December, 1986
4. Published in the Official Gazette : 26th December, 1986

Came in to force : 1st July, 1987

Who is a Consumer

1. Consumer is defined as
2. someone who acquires goods or services
3. for direct use or ownership
4. rather then for resale or use in production & manufacturing.

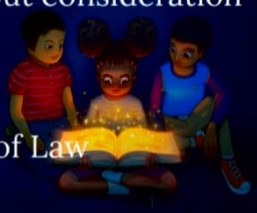
For Example :
When your father buys an apple for you and you consume them, then your father as well as you will be treated as Consumers.

Concept :

To protect the consumers
To develop countries like India
To provide simple, quick and better protection to the consumers

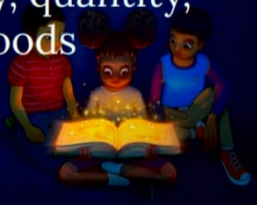
Not a Consumer

1. A person who purchased goods for resale
2. A person who purchased goods for commercial purpose
3. A person who obtains services without consideration
4. Tax payers to Municipalities
5. Contractors
6. Applicants for Jobs
7. Persons who filed suits in the court of Law



Objectives of Consumer Protection Act, 1986

1. Right to be protected against marketing of goods & services which are hazardous to life & property
2. Right to be informed : quality, quantity, purity, standard & price of goods
3. Right to be heard
4. Right to be assured



5. Right to Consumer Education
6. Right to seek redressal against unfair trade practices
7. Right to get protection against defective goods and services
8. Right to seek compensation
9. Right to choose variety of goods and services
10. Right to speak out and make a complaint

4.3.2 CONSUMER PROTECTION ACT 1986 AND CYBER CONSUMER

The Consumer Protection Act 1986 was passed by the Indian Parliament to protect consumer rights and to redress consumer complaints and resolve consumer disputes. It protects the consumers from unfair trading or unfair trade practices.

The Consumer Protection Act was passed in 1986 and it came into force fromI July, 1987. The main objectives of the Act are to provide better and all round protection to consumers and effective safeguards against different types of exploitation such as defective goods, deficient services and unfair trade practices.

Features Of CPA 1986

i) Uniformity:-This Act applies to all kinds of goods, services and unfair trade practices unless there is specific exemption made by the central government. All the sector whether they are private, public or cooperative is covered under this Act.

ii) 3-Tier Redressal:-This Act gives consumers three tiers redressal system. There is redressal forums at centre, state and District levels for providing justice to the victim consumer. Three tiers are:-

- National commission :- Section 20 to 27A of the Act talks about the composition of the commission, applications of the complaint, procedures, appeal etc. The complaint must exceed amount of one core. The goods if found defective after testing are asked for replacement or compensation for that defects.
- State commission (Section 16-19A) :- State commission is formed by each state which consist of two members and president. The complaint should be at least amount of 20 lakh and not exceed more than one core. If the goods are found defective after testing then assured party are asked for replacement and compensation.
- District Forum (Section 9-15) :- This forum is set up by the state at District level which consists of two members and a president. Among these members one should be woman and is appointed by the state government. The complain should not be entertained if amount exceed twenty lakh.

iii) Umbrella Of Legislation:-This Act is an umbrella of legislation covering goods and services but excluding all the transactions undertaken by the person not coming under the ambit of section 2(1)(d).

4.3.3 PROBLEMS FACED BY CONSUMERS IN E-COMMERCE:-

1. Quality issues

The biggest problem while buying things online is that you have no guarantee of a product's quality. With the volume of goods e-commerce companies handle these days, it can be quite difficult for them to conduct quality checks on each and every one of the products they're selling.

2. Delivery and logistics

Delivery of product in shopping online is a big chaakange. While all e-commerce sites have order tracking systems for their customers, they aren't always accurate. no way to fix a particular time slot for the delivery to take place. This same issue exists while returning products. Another problem is that the vast majority of the Indian population which lives in rural areas and Tier-III cities is unable to shop online because all e commerce sites do not provide deliveries there

3.Digital payment failures

E wallet is now used by majority of customer's like Paytm, G-Pay credit/debit card, net banking, the failure of digital payments is always lthere while making online transactions. A faltering internet connection or a technical glitch often results in the payable amount being debited from a customer's account without being credited to the selling party.

4. Additional charges

Many a times customer ends up paying additional charges in the name of delivery charges or shippment charges. These hidden charges are normally informed at the payment gateway.

5. Unclear return and guarantee policies

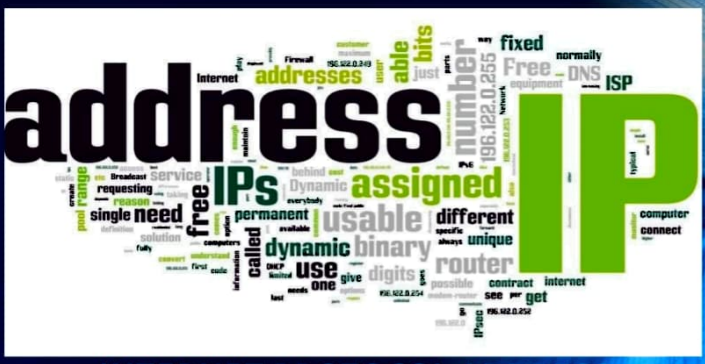
Many e-commerce sites does not provide return policy or any guarantee with respect to quality of goods. As a result consumers on these platform often faces issues pertaining to return or quality of goods

6. Lack of security

Cyber security, or more precisely the lack of it, is a major problem on the internet today. E-commerce sites record important customer data like name, phone number, address, and bank details, that can easily be misused if proper care is not taken.

CASE STUDY

Case of *Rediff. com India Ltd. v/s UrmilMunjal*[6], wherein the consumer was dissatisfied with the goods delivered by the online shopping website. While the consumer wanted to return the product and claim refund, he did not find a Return Policy, which provided details of the address to which the products were to be returned. Since the online portal was facilitator between the sellers and buyers as mentioned in the terms and conditions, it was the duty of the facilitator to inform the consumer as to how the goods are to be returned to the seller. The Court held the online portal liable on the grounds of 'Deficiency in Service' for not providing sufficient information.



INTERNET PROTOCOL ADDRESS

Contents

- What is IP Address ?
- Understanding IP Addressing
- The Format of an IP Address
- Different Classes of IP address
- A brief description on IPv4
- A brief description on IPv6

What is IP Address ?

An **IP address** (abbreviation of **Internet Protocol address**) is an identifier assigned to each computer and other device (e.g., printer, router, mobile device, etc.) connected to a TCP/IP network that is used to locate and identify the node in communications with other nodes on the network. IP addresses are usually written and displayed in human-readable notations, such as **172.16.254.1** in IPv4, and in IPv6

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Understanding IP Addressing

- The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIR) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers.
- The *IPv4* standard is most familiar to people and supported everywhere on the Internet, but the newer IPv6 standard is gradually replacing it. IPv4 addresses consist of four bytes (32 bits), while IPv6 addresses are 16 bytes (128 bits) long.

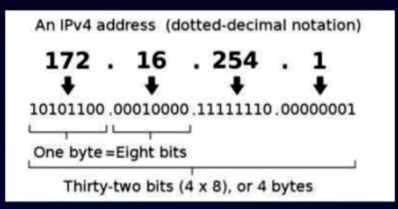
Understanding IP Addressing

There are private IP addresses, public IP addresses, static IP addresses, and dynamic IP addresses.

- **private IP addresses** are used "inside" a network, like the one you probably run at home. These types of IP addresses are used to provide a way for your devices to communicate with your router and all the other devices in your private network. Private IP addresses can be set manually or assigned automatically by your router.
- **Public IP addresses** are used on the "outside" of your network and are assigned by your ISP. It's the main address that your home or business network uses to communicate with the rest of the networked devices around the world (i.e. the Internet).
- Both private IP addresses and public IP addresses are either dynamic or static, which means that, respectively, they either change or they don't.
- An IP address that is assigned by a DHCP server is a **dynamic IP address**. If a device does not have DHCP enabled or does not support it then the IP address must be assigned manually, in which case the IP address is called a **static IP address**.

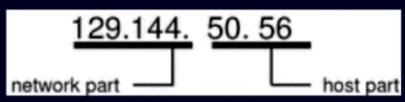
The Format of an IP Address

- An IP address consists of 32 bits, often shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form. For example, the IP address: 168.212.226.204 in binary form is 10101000.11010100.11100010.11001100.
- But it is easier for us to remember decimals than it is to remember binary numbers, so we use decimals to represent the IP addresses when describing them. However, the binary number is important because that will determine which class of network the IP address belongs to.



The Two Parts of an IP Address

- IP address have two parts prefix and suffix
- The address prefix identifies the physical network to which the computer is attached , While suffix identifies the individual computer on the network
- Prefix is also called network address
- Suffix is also called host address



Different Classes of IP address

Class A Network

In a Class A Network binary address start with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network and the remaining 24 bits indicate the host within the network. An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

Class B Network

In a Class B Network, binary addresses start with 10, therefore the decimal number can be anywhere from 128 to 191. The number 127 is reserved for loopback and is used for internal testing on the local machine. The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

Different Classes of IP address

Class C Network

Binary addresses start with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

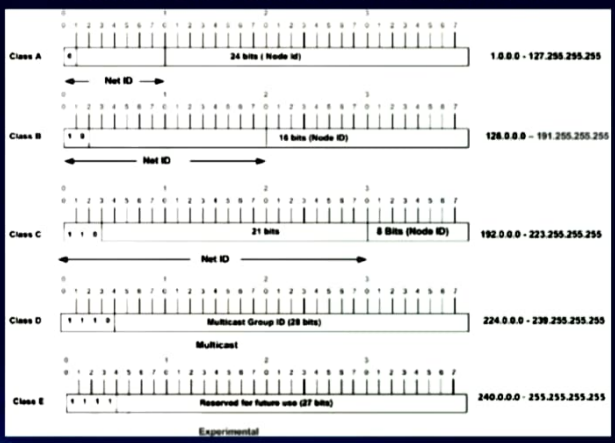
Class D Network

In a Class D Network, binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

Class E Network

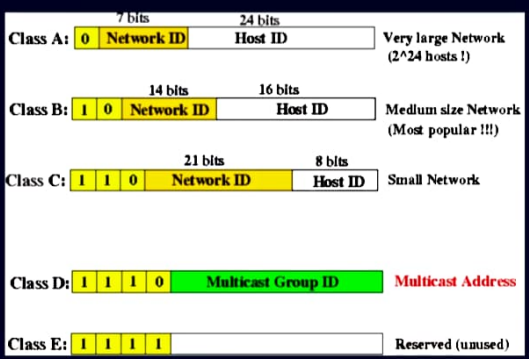
In a Class E Network, binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented or utilized in a standard way.

Different Classes of IP address



Different Classes of IP address

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255



Different Classes of IP address

ADDRESS CLASS	BIT IN PREFIX	MAX.NO OF NETWORKS	BIT IN SUFFIX	MAX.NO OF HOSTS PER NETWORK
A	7	128	24	1,67,77,216
B	14	16,384	16	65,536
C	21	20,97,157	8	256

IPv4

- **Internet Protocol version 4 (IPv4)** is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet.
- IPv4 uses 32-bit addresses which limits the address space to 4294967296 (2^{32}) addresses.

IPv4

Version. Version no. of Internet Protocol used (e.g. IPv4).

IHL. Internet Header Length; Length of entire IP header.

DSCP. Differentiated Services Code Point; this is Type of Service.

ECN. Explicit Congestion Notification; It carries information about the congestion seen in the route.

Total Length. Length of entire IP Packet (including IP header and IP Payload).

Identification. If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

Flags. As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.

IPv4

Fragment Offset. This offset tells the exact position of the fragment in the original IP Packet.

Time to Live. To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross

Protocol. Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol.

Header Checksum. This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address. 32-bit address of the Sender (or source) of the packet.

Destination Address. 32-bit address of the Receiver (or destination) of the packet.

Options. This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv6

- **Internet Protocol version 6 (IPv6)** is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.
- An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:).
- The hexadecimal digits are case-insensitive, but IETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

IPv6

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

IPv6

Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.

Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet.

Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information.

Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload.

Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU.

IPv6

Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely.

Source Address (128-bits): This field indicates the address of originator of the packet.

Destination Address (128-bits): This field provides the address of intended recipient of the packet.

4.4 SECURITY ISSUES IN E-COMMERCE

- **Risk Management Approach To E-Commerce**

The growth of E Commerce in recent times has grown three folds and so is the risk. The security issues are also increasing with same rate, and it is important to take necessary measures that can safeguard the users interest. Risk in on line transaction is unavoidable.

Managing risk is very important in E Commerce. It plays a critical role to protect the organization and its ability to perform their business and not just its IT assets. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Following are the most important procedures for managing risk in e-commerce transactions.

1. Understand the risks and train staff

It is important in order to minimise the risk in E Commerce that staff should know clearly what risks e-commerce business may have to deal with. Everyone in business structure needs to understand the types of risks inherent in online payments. Establishing a procedure on avoiding and solving risks, which is a must for all staff to follow.

2. Ensure information security

Information related to customer databases, buying requests, payment process.etc. is very important in E –Commerce. Hacking by

hackers is very common problem, so there is a need to ensure good security all the time to avoid data being changed or stolen. There is a need to set up a secure and efficient process for submitting authorization requests over the internet, before starting accepting card payments online. It is important for E-commerce companies to look for)DSS (Data Security Standards).

3. Select the right acquiring bank and merchant services provider.

Bank and Merchant are key players along with the customer in E Commerce. The right acquiring bank and merchant services provider will provide effective risk management support if they have a complete understanding of e-commerce fraud risk and liability associated with online transactions.

4. Create and display effective policies

Website is the first place where interaction between buyer and seller starts. Hence website must list all privacy, shipping, return and refund policies very clearly on each page. Customers should not be forced to search for them. This will also create satisfaction and convenience for customers to visit web page more often.

5. Use collection efforts to minimize losses

It is important to have control over charge-backs and especially the ones resulting from processing errors. A well-designed collection system can help recover unwarranted chargeback losses

hackers is very common problem, so there is a need to ensure good security all the time to avoid data being changed or stolen. There is a need to set up a secure and efficient process for submitting authorization requests over the internet, before starting accepting card payments online. It is important for E-commerce companies to look for)DSS (Data Security Standards).

3. Select the right acquiring bank and merchant services provider.

Bank and Merchant are key players along with the customer in E Commerce. The right acquiring bank and merchant services provider will provide effective risk management support if they have a complete understanding of e-commerce fraud risk and liability associated with online transactions.

4. Create and display effective policies

Website is the first place where interaction between buyer and seller starts. Hence website must list all privacy, shipping, return and refund policies very clearly on each page. Customers should not be forced to search for them. This will also create satisfaction and convenience for customers to visit web page more often.

5. Use collection efforts to minimize losses

It is important to have control over charge-backs and especially the ones resulting from processing errors. A well-designed collection system can help recover unwarranted chargeback losses

6. Secure the process of routing your authorizations.

In E–Commerce it is important that authorizations are handled carefully, it is important to ensure a system that all authorizations are submitted in a secure and efficient manner, before it starts accepting card payments over the internet. The routing of information has to be through secured mode.

7. Establish a process for handling transaction post-authorizations.

In E- Commerce transactions it is important to deal separately with approved and declined authorizations. A system has to be developed for filtering it.

8. **Build a fraud screening process.**

A strong and secure system has to be in place for fraud screening and control. When adequately implemented, the screening of online card transactions can help in minimizing fraud for high-risk transactions.

The Internet has driven a huge increase in the level of trade conducted electronically, and had lead a growth in E-commerce. Lot of transaction for buying and selling happens on a daily basis. But with this growth comes security issues in e-commerce . These security issues has

become a great threat . Any e-commerce system must meet certain criteria to guard against these potential threats.

E commerce security threats are causing havoc in online trading. There is approximately 32.4% of threats that is experienced annually in online trading.

4.4.1 SOURCES / TYPES OF SECURITY ISSUES IN E COMMERCE:-

1. Financial frauds

Financial fraud has been a very common in on line trading. There are various kinds of Financial frauds prevalent in the e-commerce industry, but we are going to discuss the two most common of them.

a. Credit Card Fraud

It happens when hacker steal the credit card data or any other personal details , used by the customer on any of the site . It can be identified as normally shipping and billing address varies. AVS - Address Verification System can be used by the companies to detect and control these frauds.

b. Fake Return & Refund Fraud

Some hackers engage in refund frauds, where they file fake requests for returns. Sometimes even they perform unauthorized transactions and clear the trail, causing businesses great loss.

6. Phishing

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need. a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

7. Spamming

Spamming is when one person or company sends an unwanted email to another person. **Spam** emails are the computer version of unwanted "junk mail" that arrives in a mailbox, such as advertising pamphlets and brochures.

8. DOS & DDoS Attacks

A Denial-of-Service (**DoS**) **attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. **DoS attacks** accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Many e-commerce websites have incurred losses due to disruptions in their website and overall sales because of Distributed Denial of services (DdoS) attacks.

9. Malware

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a common word used for many "malicious software." Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransom ware.

10. Exploitation Through Vulnerabilities

Attackers are on the lookout for certain vulnerabilities that might be existing in an e-commerce store. Often an e-commerce store is vulnerable to SQL injection and Cross-site Scripting (XSS).

a. SQL Injection

It is a malicious technique where a hacker attacks your query submission forms to access your database. They corrupt your database with an infectious code, collect data, and later wipe the trail.

b. Cross-Site Scripting (XSS)

The attackers can plant a malicious JavaScript snippet on your e-commerce store to target your online visitors and customers. Such codes can access your customers' cookies and compute.

11. Bots

A bot short form of "robot" is an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input. There are many different types of bots, like web crawlers, chat room bots, and malicious bots.

12. Brute Force

Under this type of security issues the hackers normally attack admin panel of the user and try to crack password. They connect to the website and try to obtain user passwords.

13. Man in The Middle

The users are more vulnerable to this type of security issues . A hacker may listen in on the communication taking place between-commerce store and a user.

14. E –Skimming

E-skimming involves infecting a website's checkout pages with malicious software. The intention is to steal the clients' personal and payment details.

4.4.2 SOLUTIONS TO SECURITY ISSUES IN E- COMMERCE:-

1. HTTPS and SSL certificates

HTTPs protocols not only keep users' sensitive data secure but also boost website rankings on Google search page. They do so by securing data transfer between the servers and the users' devices. Therefore, they prevent any interception.

2. Anti-malware and Anti-virus software

An Anti-Malware is a software program that detects, removes, and prevents infectious software (malware) from infecting the computer and IT systems.

Anti-Virus is a software that was meant to keep viruses at bay. Although a lot of Anti-virus software evolved to prevent infection from other malware as well.

3. Securing the Admin Panel and Server

Using complex passwords that are difficult to figure out, changing them frequently is one of the practice that can keep a check on these insecurity.

4. Securing Payment Gateway

Storing the credit card information of clients on database should be totally avoided. A third party such as PayPal and Stripe can handle the payment transactions away from website. This ensures better safety for customers' personal and financial data.

5. Deploying Firewall

Firewall are a part of a computer system that is designed to prevent people from getting information without authority but still allows them to receive information that is sent to them. Deploying firewalls can keep away fishy networks, and helps in regulating the traffic on website..

6. Additional security implementations

Always scan your websites and other online resources for malware Back up your data. Most e-commerce stores also use multi-layer security to boost their data protection.

It is important that these security related issues need to be managed carefully and efficiently in E commerce

ENCRYPTION

CONTENTS

- What is encryption?
- **why is it important?**
- Why use encryption?
- Examples of Encryption
- How it works??

Encryption

- **Encryption** is the most effective way to achieve data security
- Encryption is the process of converting data to an unrecognizable or "encrypted" form.
- Encryption is also used to secure data sent over wireless networks and the Internet

why is it important?

- Encryption **is important** because it allows you to securely protect data that you don't want anyone else to have access to.

Why use encryption?

- **Authentication**
  - Protects personal data such as passwords.
- **Privacy**
  - Provides for confidentiality of private information.
- **Integrity**
  - Ensures that a document or file has not been altered.

Examples of Encryption

- Web browser encryption
- Email encryption
- Hard drive encryption

How it works??

- Start with a message that has to be sent securely. This could be
- ✓Text.
- ✓Numeric Data.
- ✓Secret Codes

Next we need an encryption key. This could be a phrase like My secret password phrase

The computer receiving the message knows the digital key and so is able to work out the original message.

Encryption methods

- **Hashing Encryption**

  Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash, thereby alerting a user to potential tampering. Some common hashing algorithms are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA).

- **Symmetric Methods**
  - also called private-key cryptography, is one of the oldest and most secure encryption methods
  - A sender encodes a message into ciphertext using a Private key, and the receiver uses the same key to decode it

- **Asymmetric Forms**
  - Asymmetric, or public key, cryptography is, potentially, more secure than symmetric methods of encryption.
  - Uses two keys, a "private" key and a "public key," to perform encryption and decryption