International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

E-Commerce's Crime/Cyber Crime

Suresh Kumar

Research Scholar, Department of Laws, Panjab University Chandigarh

Abstract: Cyber-crimes use computers and networks for criminal activities. Computers can be used for committing anoffense in one of the following three ways: as aninstrument, as a target, and both as a tool and target. For illustrations: frauds related to e-banking, e-commerce, electronic data-interchange etc. are committed by using computer. This paper has been discussed through heading like introduction of cybercrimes, types of cybercrimes and conclusion.

Keyword:*Cyber-Crimes.*

Introduction

E-commerce merchants and consumers face many of the same risk as participants in traditional commerce, albeit in new digital environment. Theft is theft, regardless of whether is a digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, and vandalism all crimes in a traditional commercial environment are also present in e-commerce.[1]Electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavours will be that much greater. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds, the sale and leaseback of automatic teller machines, and worldwide telephone lotteries.[2]

The "digital age", in which the internet has played a critical role, has seen dramatic and rapid communications, economic and social developments. The words "electronic commerce" is commonly used of a computer, or other network-accessible device, and the Internet to trade goods and services in a new, direct and electronic manner.[3]Our growing dependence on computers and the

[1]Kenneth C. Laudon and Carol Guercio*Traver, E-commerce, Business, Technology, Society*262 (Pearson Education, Dorling Kindersley India Pvt. Ltd., New Delhi, 2009).
[2]SaritaJand, *Forensic Science & Law*216 (New Era Law Publication, Faridabad, Haryana, 1st edn., 2017).
[3] Hyde William Cornish, *Intellectual Property Rights* 443 (Global Vision Publishing House, New Delhi, 1st edn., 2011).

Internet has made us all potential victims of Internet threats. Some countries have enacted legislations that specifically deal with computer crime and yet others have adapted their existing laws to make computer crime an offence under existing statutes.[4]

E-Commerce Crime

It is new form of crime which has emerged broadly because of computerization of various activities in a networked environment in an organization. Normally, cyber-crime is a computer crime in a cyber space using computer as a tool, which is connected to internet against any other computer which is also to the same. In such crimes both the complainant and the criminal must have knowledge of computer. These include; hacking and hijacking, internet theft and piracy, blocking of service, intrusion, spoofing and spanning, banking network, communication network, e-mail bombing, introduction of viruses, promotion of terrorism, cyber talking etc.[5]Computer crime is the treat caused by the criminal or irresponsible actions of computer users who are taking advantage of widespread use of computer networks in our society. It thus presents a major challenge to the ethical use of IT.[6]

Cyber-crimes use computers and networks for criminal activities. Computers can be used for committing a crime in one of the following three ways: as a tool, as a target, and both as a tool and target. The first type of crime is basically an extension of 'real world' crimes, such as forgery, fraud or copy right piracy using computers. Existing laws can be used to bring criminal to justice. The second type of crimes is a real cyber-crime in which culprits' damage or modifies the victims' computer system and networks through illegal access, and cause heavy loss to the victims.[7] The internet can provide as many security risks as opportunities for a company-and some would number

[4]Gurvinder Singh and Rachhpal Singh, *E-Commerce* 238 (Kalyani Publishers, New Delhi, 2004).
[5]Dr. B.P. Maithi, *Physical Evidence in Criminal Investigation & Trials* 375 (Selective & Scientific Books, Delhi, 1st edn., 2012).
[6]C.S.V. Murthy, *E-Commerce, Concept, Models, Strategies* 254 (Himalaya Publishing House, Girgaon, Mumbai, Reprint 2007).
[7]Kamlesh K. Bajaj and Debjani Nag, *E-Commerce the Cutting Edge of Business* 285 (Tata McGraw-Hill Publishing Company Limited, New Delhi, Reprint 2006)

the opportunities online "infinite," security issues-hackers, viruses, and the like-are frightening issues for companies with any level of internet connectivity.[8]

A new generation of crimes has cropped by the advent of Internet. Computer hacking, software piracy, internet paedophilia, password breaking, spoofing, telecommunication frauds, e-mail bombing, and the availability of illicit or unlicensed products and services that have already made their mark. New problems emerging on the scene includes: (a) credit card fraud, (b) cyber terrorism, and (c) cyber laundering and criminal use of secured internet communications.[9]

Indian Parliament has adopted two-fold strategies to control cyber-crimes: (i) It has amended IPC to cover cyber-crimes expressly, and (ii) Has provided provisions in the Information Technology Act, 2000 which was basically enacted to facilitate e-commerce in India to deal with computer-related crimes.[10]This may also promote our technology base to keep pace with global trends. As India has already enacted IT Act, 2000, this allows transactions signed electronically for e-commerce primarily to be enforceable in a court of law.[11]

These crimes generally include: (i) Sabotage of computer systems or computer networks; (ii) Theft of data/information; Theft of intellectual property, such as computer software; (iii) Theft of marketing information; and Blackmailing based on information gained from computerised files such as personal history, financial data etc. For examples: frauds related to e-banking, e-commerce, electronic data-interchange etc. are committed by using computer. Software piracy, online gambling, copyright infringement, trade mark violations are some illustrations of such crimes.[12]

[8]SteffanoKorper and Juanita Ellis, *E-Commerce Book Building the E-Empire*189 (Academic Press, A Harcourt Science and Technology Company, USA, 2001).
[9]B.B. Nanda and R.K. Tiwari, "Cyber Crimes-A Challenge to Forensic Science", *The Indian Journal* 103 (Aril-Sept., 2000).
[10]Prof. K. Uma Devi, Dr. G. Indira PriyaDarsini, et, al., *the Law of Intellectual Property Rights* 203 (Regal Publications, New Delhi, 2012).
[11]Dr. K.N.S. Kang, Ms SamarjitSandhu, et, al., (eds.), *Information Technology & Management* (MukeshPruthi, JaspreetKaur, et., al., Intellectual Protection Using Public Key Cryptography) 202 (Unistar Books Pvt. Ltd., Chandigarh, 2006).
[12] Prof. N.V. Paranjape, *Criminology and Penology* 135 (Central Law Publications, Allahabad 13th edn., 2007).

International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Internet Crime

Internet crime is crime committed on the Internet, using the Internet and by means of the Internet. Computer crime is a general term that embraces such crimes as phishing, credit card frauds, illegal downloading, cyber terrorism, creation and distribution of viruses etc. all such crimes are computer related and facilitated crimes.[13]

The different types of Internet crime vary in their design and how easily they are able to be committed. Internet crimes can be separated into different categories. There are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. Such new crimes devoted to the Internet are email "phishing", hijacking domain names, virus, and cyber vandalism.[14]

Cyber Terrorist Related to Online Illegal Money

The monitoring of Internet communications is a monumental task and one that is increasing rapidly given the growth rate of use of the Internet. For example, analysing illegal online money-raising and flows of funds requires identifying relatively small amount of funds and transactions in amongst billions of such transactions.[15]

Terrorism is the use of violence and other activities to instil fear in the targeted public. There are very few studies in relation to the specific fear of cyber terrorism, as much of the literature focuses on the fear of cyber-crime, yet these studies do provide an insight into criminological discourse on fear and terrorist use of the Internet.[16]

E-commerce Privacy

E-commerce merchants have two concerns related privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain

[13]*Supra* note 2 at 237.
[14]*Ibid.*
[15]Imran Awan and Brian Blakemore (eds.), *Policing Cyber Hate, Cyber Threats and Cyber Terrorism* 178 (Ashgate Publishing Limited, Wey Court East, England, 2012).
[16]*Id* at174.

access to credit card or other information, this not only violates the confidentiality of the data, but also the privacy of the individuals who supplied the information.[17]**E-Commerce/Investment Frauds**

Sales and investment frauds are major acts committed. An offering that uses false or fraudulent claims to solicit investment or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities; merchandise or services that were purchased or contracted by individual online are never delivered.[18]

Some fraudulent investment promoters will fool you with web sites that make their "investment company" look like a solid, top-rated Wall Street investment firm with slick-looking websites that use graphics, audio and video clips.[19] The input, alteration, erasure on suppression of computer programs, or other interference with the course of data processing that influences the result of data processing thereby causing economic or possessory loss of property of another person will the intent of procuring an unlawful economic gain for himself or for another person or with the intent to unlawfully deprive that person his property.[20]

Digital Signature Security Risk

Digital signatures, variation of which is being explored by several companies, are the basis for secure commerce. A digital signature provides a way to associate the message with the sender, and is the cyberspace equivalent of "signing" for purchase.[21] Digital signatures are also used to authenticate each of the parties involved and hashing algorithms used to ensure that messages have not been altered. The main security risks associated with these systems relate to the possibility that private

[17]*Supr*a note 1 at 264.
[18]*Supra* note 2 at 192.
[19]YogeshBarua, *Frauds & FinancialCrimes in Cyberspace* 72 (Dominant Publishers and Distributors, New Delhi, 1st edn., 2005).
[20]*Supra* note 10 at 213.
[21]Ravi Kalakota and Andrew B. Whinston, *Electronic Commerce a manager's Guide*142 (Pearson Education Pvt, Ltd., Delhi, 7th Indian Reprint, 2005).

encryption keys could be stolen or used without authorisation by people who have obtained them illegitimately.[22]

Card Insertion misuse

Access to a computer can be made by use of cards. Such a card is similar to a password, which prevents misuse of computer and its data. Cards are basically of two types: (i) Magnetic strap cards-cards of this nature used for getting access to specified data. Use of this card involves transfer of authorisation and identification data in MICR, which is read by the computer before allowing or refusing the access, and (ii)Microchips cards-such a card contains a microchip with memory, and the manner of access to data in a computer is the same as in magnetic straps cards.[23]

Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.[24]Examples include forging or counterfeiting documents, exchanging valid computer taps, cards, or disks with prepared replacements, data entry violations, punching extra holes or plugging holes in cards, and neutralizing or avoiding manual control.[25]This offence involves changing or erasing of data in subtle ways which makes it difficult to put the data back or be certain of its accuracy. This is resorted to for the purpose of illegal monetary gains or for committing a fraud or financial scam.[26]

[22]PrakashTalwar (eds.), *Corporate Crime* 197 (Isha Books, Delhi, 2006).
[23]AnoopamModak, *Scientific Techniques in Criminal Investigation* 52 (Universal Law Publishing an Imprint of Lexis Nexis, 3rdedn., 2016).
[24]*Supra* note 2 at 193.
[25]Donn B. Parker, *Fighting Computer Crime* 71 (Charles Scribner's Sons, New York, 1983).
[26]*Supra* note 12 at 139.

International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Computer Espionage

The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent there to cause economic loss to the person entitled to the secret or obtain an unlawful economic advantage for oneself or a third person.[27]

Online OffersMisuse

Recall that a valid offer is one that a reasonable person in the position of the offered would believe will create a contract if accepted, and that advertisement are typically not considered offers, but rather invitations to deal. In general, website merely displaying product information is considered an advertisement but, as with physical world advertisements, an ad that is sufficiently specific can be offer.[28] Many newsletters on the internet provide the investors with free advice recommending stock where they should invest. Sometimes these recommendations are totally bogus and cause loss to the investors.[29]

Electronic Impersonation

In e-commerce, individuals, their writings, signatures, voice, etc. do not figure. It is only through PASSWORDS that identification of an individual is established. Thus, stolen passwords are creating havoc. Illegal money transfer, diversion, collection and expending are is causing extensive damage. Better electronic identities through biometrics promise better impersonation prevention.[30]

Database Server

Electronic commerce systems store user data and retrieve product information from database connected to the Web server. Besides product information, database connected to the Web contain

[27] *Supra* note 10 at 214.
[28] Robert Dunne, *An Introduction to Basic Legal Principles and Their Application in Cyberspace* 33 (Cambridge University Press, New York, 1st edn., 2009).
[29] Rachhpal Singh, KapilGoyal, et, al., *E-Commerce & E-Business*236 (Kalyani Publishers, Ludhiana, 2004).
[30] B.R. Sharma, *Scientific Criminal Investigation* 34 (Universal Law Publishing Co. Pvt. Ltd., New Delhi, Reprint 2012).

valuable and private information that could irreparably damage a company if it were disclosed or altered. [31]

Fraud on Internet

Internet fraud is said to be big business. But what is it, and does using the Internet create the fraud, or is the Internet just a different way of delivering 'traditional' fraud is different question. The term "Internet fraud" refers generally to any type of fraudulent scheme that uses one or more components of the Internet-such as chat rooms, e-mails, message boards, or websites to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or transmit the proceeds of fraud to financial institutions or to other connected with the scheme.[32]Phishing operates by sending forged e-mail, impersonating an online bank, auction or payment site; the email directs the user to a forged website which is designed to look like the login to the legitimate site but which claims that the user must update person information. A number of malicious 'Trojan horse' programmes have also been used to snoop on Internet users while online, capturing keystrokes or confidential data in order to send it outside sites.[33]

The Internet is also proving to be a great boon to fraudsters. As electronic commerce continues to expand in terms of the range of products and services which are offered for sale on-line, and as the number of users continues to increase, so the opportunities for dishonesty and fraud have also increased.[34]Additionally if the security code is broken and the message is intercepted, the hacker will be able to perpetrate fraud on the recipient of the message.[35] When the computer networks were Intranets, the computer frauds were limited to manipulations of data, by some insider, concerning invoices, account balances or payment of salary.[36]

[31]Gary P. Schneider and James T. Perry, *Electronic Commerce* 164 (Thomson Asian Pvt. Ltd, Singapore, 1st Reprint 2001).
[32]*Supra* note 10 at 181.
[33]*Supra* note 2 at 253.
[34]*Supra* note 22 at 190.
[35] S .B. Verma, R.K. Shrivastawa, et., al, *Dynamics of Electronic Commerce* (Tripti Singh, Cyber Crimes and Internet Security Concepts) 259 (Deep & Deep Publication Pvt. Ltd., New Delhi, 2007).
[36]Dr. S.V. JogaRao, *Law of Cyber Crimes & Information Technology Law* 57 (Wadhwa and Company Nagpur, New Delhi, 1st edn., 2004).

International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cyber Squattingand Data Leakage

Cybersquatting however, is a bit different in that the domain names that are being "squatted" are (sometimes but not always) is being paid for through the registration process by the Cyber squatters. Cyber squatters usually ask for prices for greater than that which they purchased it.[37]It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on right of using it before the other or using something similar to that previously.[38]A wide range of computer crime involves the physical removal of data or copies of data from a computer system. The data may be trade secret information, secret marketing data, personal credit information, or any other item of information from which a perpetrator might make gain by selling it or by using it to another's disadvantage.[39]

Cyber Stalking

The Internet a new way of communication is wide open to both exploitation and exploration. The hard fact is that, there are no police on the Information Superhighway. There is no one to protect you or to look-up virtual criminals. This lack of supervision and enforcement leaves users to watch out for themselves and for each other.[40]Stalking generally involve harassing or threatening behaviour that an individual engages in repeatedly such as following a person, appearing a person home or place of business, making harassment phone calls, leaving written messages or objects, or vandalizing a person's property.[41] Stalking is not a new crime form of crime. It has existed from time immemorial. However, it is only recently that it has received attention as a serious crime from the criminologists.[42]

Banking/Credit card Related Crime

In the corporate world, internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information. Use of

[37]N.C. Jain, *Cyber Crime* 213 (Allahabad Law Agency, Faridabad, 1st edn., 2008).
[38]*Supra* note 2 at189.
[39]*Supra* note 25 at 97.
[40]*Supra* note 10 at 178.
[41]*Supra* note10 at 195.
[42]*Supra* note 36 at 51.

stolen card information or fake credit/debit card is now-a-days very common.[43] Fraudulent use of a credit card in a shop requires the possession of the card, fraudulent use online only needs the card and account holder details. The credit card company can carry out checks that the transaction 'seems reasonable' and there is an audit trail of the use of the card in the vendor's records but the system can be and is abused.[44]

Theft credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen frequently prevents users from making online purchase.[45] Financial fraud crimes have becomes more prevalent in recent years as international criminals take advantage of the significantly greater personal and corporate financial information now available, and readily exploitable, through computer technology and access devices such as credit cards, debit cards and smart cards.[46] Credit card fraud is widespread as a means of stealing from banks, merchants and client. A credit card is made of three plastic sheet of polyvinyl chloride. These cards are of particular size and many data are embossed over it. But credit cards fraud manifest in a number of ways. They are: (i) Genuine cards are manipulated, (ii) Genuine cards are altered, (iii) Counterfeit cards are created, (iii) Fraudulent telemarketing is done with credit cards, and (iv) Genuine cards are obtained on fraudulent applications on the names/addresses of other persons and used.[47]

Web Spoofing and DNS Spoofing

While IP and DNS spoofing depend on sophisticated technical knowledge, web-spoofing attacks use a much simpler approach. These are based on optical illusion in general. Hyperlink on web pages can contain characters that make an address look real, but in fact lead to a wrong website.[48]DNS spoofing describes the faking of host masks during the resolution of Internet hostnames. DNS or "Domain Name Service" provides the mapping between hostnames and IP addresses. Every access

[43]*Supra* note 2 at 192.
[44]David Whiteley, *E-Commerce Strategy, Technologies and Applications* 201 (Tata McGraw-Hill Publishing Company Ltd., New Delhi, 2011).
[45]*Supra* note 1 at 275.
[46]*Supra* note 19 at 352.
[47]*Supra* note 2 at 252.
[48]*Ibid.*

request on the Internet using the host's name has to be resolved to its IP address, which is done by communicating with a DNS-server which stores the host masks in data base.[49]

Cyber Smearing

Cyber smearing is used to blacken the good name of a company or its product through internet. These are not foolish pranks but loaded messages to harm anyone's reputation. Companies have to keep on scanning chat room, news groups, business forum etc., for loaded messages, besmirching their reputation.[50] This is a genus of pure cybercrime that has similarities with old strategy of registering trademarks only prevent others from using it.[51]

Money Laundering Crime

Money laundering is an illegal activity through which criminal proceeds take on the outward appearance of legitimacy. This process is an unavoidable support system in virtually all profile making criminal activities, as the criminal requires stashing away their ill-gotten money and then bringing it in circulation after giving it the necessary legitimacy.[52]A sum of money electronically transferred from bank account of one country to an anonymous bank account in another country, with the object of conversion of ill-gotten/black money into an official one, is an instance of money laundering.[53]

Unauthorised Access for E-commerce& Hacking

Unauthorised intrusion of computer facilities of an organisation or of another person by an individual renders the status of the individual, a hacker. Hackers normally comprise of students, enthusiasts of information technology, egoists, and spy agents of other Governments or computer belonging to another person, consequent to acquiring of password of the computer by unfair means, with the object of commission of offence of mischief, wrongful gains, destruction of data, utilisation of paid time on the internet connected to the computer, manipulation of accounts under debit/credit

[49]*Supra* note 36 at 53.
[50]*Supra* note 10 at 196.
[51]*Supra* note 36 at 61.
[52]*Ibid.*
[53]*Supra* note 23 at 49.

International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

cards.[54]A new breed of 'hackers', who are skilled young professionals, are known to penetrate web sites to break, destroy, alter or steal files, programmes, codes etc., as a challenge to carry out crime, either for excitement or for monetary consideration.[55]

Forgery E-commerce/Counterfeiting

In forgery and counterfeiting of data the best example to cite will be when a person learns of computer software and later detaches himself from the organisation to make copies of this popular package, dressing them up to look like original and sells them.[56]Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. Impersonating another person is also considered as forgery.[57] The input, alternation, erasure or suppression of computer data of computer programs,[58] or other interference with the course of data processing in a manner or under such conditions which would, according to national law, constitute an offence of forgery if it had been committed with respect to traditional object of such an offence.[59]

Viruses

Virus is a program created by human agent to alter or destruct digital information. They usually affect the data on a computer, either by altering it or deleting it. It is a computer program that is loaded onto your computer without your knowledge and runs against your wishes. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.[60]

[54]*Ibid.*
[55]B.S. Nabar, *Forensic Science in Crime Investigation* 377 (Asia Law House, Hyderabad, 3rdedn., Reprint 2014).
[56]Barkha& U. Rama Mohan, *Cyber Law & Crimes* 15 (Asia Law House, Hyderabad, Reprint 2007).
[57]*Supra* note 2 at 192.
[58]*Supra* note 10 at 213.
[59]*Id*214.
[60]*Supra* note10 at 176.

International Journal of Research in Social Sciences
Vol. 9, Issue 2, February - 2019,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Server Threats

This server is the link in the client-Internet-server trio embodying the electronic commerce path between the user and a commerce server. Servers have vulnerabilities that will be exploited by anyone determined to cause destruction or to illegally acquire information. One entry point is the Web server and its software. Perhaps the most dangerous entry points are common gateway interface programs or utility programs residing on the server.[61]

Tax Evasion

With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional counter measures against money laundering and tax evasion may soon be of limited value.[62] E-Commerce also becomes a major concern when use for Tax Evasion. To find an effective solution to the problem of E-Commerce, following issues need to be resolved.[63]

E-mail Frauds

E-mail is an inexpensive and popular device for distributing fraudulent messages to potential victims. The most common e-mail fraud is 'phishing' i.e., personal information fraud. Since electronic funds transfer systems have now begun to proliferate, there is greater risk of transactions being intercepted or diverted. Now a day's valid credit card numbers can be intercepted electronically as well as physically and the digital information stored on a card can be counterfeited.[64] Electronic mail and Internet addresses may be manipulated by including details which are misleading or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the Internet.[65]

Electronic Funds/Transfer Fraud

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well

[61] *Supra* note 31 at 162.
[62] *Supra* note 2 at 215.
[63] *Supra* note 35 at 259.
[64] *Supra* note 12 at 138.
[65] *Supra* note 22 at 194.

as physically; the digital information stored on a card can be counterfeited.[66]Most of the large scale electronic funds transfer frauds which have been committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers or financial institutions. In many cases offenders have worked within financial institutions or corporations themselves and been privy to the operation of the security system in question.[67]

Illegal Interception of Telecommunication

Developments in telecommunications provide new opportunities for electronic eavesdropping. From activities as time-honoured as surveillance of an unfaithful spouse, to the newest forms of political and industrial espionage, telecommunications interception has increasing applications.[68] The switching instruments and exchanges use the similar technology as in the routers of computer networks.[69]

Internet Based Banking Crime

Certain bank products offering electronic cash management services may be used by bank customers to launder money. The central problem with virtual banks is that there is virtually no oversight, not least because it is not clear who has jurisdiction or where the crime is being committed. In many cases, banks and other financial institutions have no inclination to know their customers, especially if it puts them at a competitive disadvantage.[70]

Intellectual Property Right Crimes

Copyright means the exclusive right of an author to do or authorise others to do certain acts for the commercial exploitation of the copyrighted material, which may include literary, dramatic, musical and artistic works, cinematograph film and sound recording.[71]The explosion of digitalization and the

[66]*Supra* note 2 at 217.
[67]*Supra* note 22 at 196.
[68]*Supra* note 2 at 216.
[69]Donn Parker and Susan H. Nycum, "Communications of the ACM" Volume 27 Number 4, April 1984 and Grabosky, Peter N. et,al.,*Crime in the Digital Age: Controlling Telecommunication and Cyberspace Illegalities* (New South Wales, Federation Press, 1998).
[70]*Supra* note 19 at 383.
[71]*Supra* note 36 at 59.

internet have further facilitated the intellectual property right violators copy and illegally distribute trade-secrets, trade-marks, logos theft or computer source code etc. Computer pirates steal away valuable intellectual property when they copy software music, graphics/pictures, books, and movies etc. which are available on the Internet.[72]

Software Piracy

Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copy right protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.[73]Software piracy is a serious crime. Software this crime every year and the amount is increasing every year. The pirated software cost only the floppies and disks. The pirated software cost only thee floppies and disks. Consequently the pirated software is dirt cheap as piracy is an expanding crime. The 'industry' has unlimited scope for software piracy. However, some special programmes are being developed to counter the abuse.[74]

Online Fraud & Cheating

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering etc.[75] It means the person who is doing the act of cyber-crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.[76]

Spam (Junk) Web Sites

Junk or spam web sites typically appear on search results, and do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, post their names on

[72]*Supra* note 12 at 139.
[73]*Supra* note 2 at 277.
[74]*Supra* note 30 at 35.
[75] Dr. (Mrs.) Rukmani Krishnamurthy, *Forensic Science in Criminal Investigation* 549 (Selective & Scientific Books, Delhi, 1st edn., 2011).
[76]*Supra* note 2 at 187.

open Web forums, and redirect traffic to known spammer-redirection domains such as vip-online-search info and web resources info.[77]

Password Attacks and Internet Time Theft

Password attacks can be implemented using several different methods like the brute force attacks, Trojan horse programmes. IP spoofing can yield user accounts and password. Password attacks usually refer to repeated attempts to identify a user password or account. These repeated attempts are called brute force attacks.[78]Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person.[79]

IP Spoofing and Sniffing

An IP attack occurs when attacker outside the network pretends to be a trusted computer either by using IP address that is within its range or by using an external IP address that you trust and to which you wish to provide access to specified resources on your network. Normally, an IP spoofing attack is limited to the injection of data or command into an existing stream of data passed between client and server application.[80]Sniffing, the most common threat online occurs when confidential financial information is read and abused by a third party causing financial harm to one or both parties in an online transaction.[81]

Misuse Electronic Payment System/Stolen payment cards

Criminal are able to communicate with each other in secret, disguise their identities in order to avoid detection, and manipulated electronic payment systems to obtain funds illegally. They are also able to perpetrate crime on much wider scale than in the past, duplicating countless fraudulent invoices,

[77]*Supra* note 1 at 276.
[78]*Supra* note 29 at 276.
[79]*Supra* note 2 at 189.
[80]*Supra* note 29 at235.
[81]Rajesh Chakrabarti and VikasKardile, *The Asian Manager's Handbook ofE-Commerce*159 (Tata Mcraw-Hill Publishing Company Limited, New Delhi, 2002).

or establishing large numbers of accounts that only exist in cyberspace. Their victims may also be located anywhere in the world.[82]

Unwanted Programs

In addition to malicious code, the e-commerce security environment is further challenged by unwanted programs such as adware, browser parasites, spyware, and other applications that install themselves on a computer typically without the user's informed consent.[83]

Denial of Service (DOS) Attacks

In a denial of service (DOS) attack, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate request.[84]

Cyber Law

Information Technology Act, 2000 is the principal legislation dealing with rules and provisions relating to cyber world; it provides a step forward in the field law with the modernized changing dimension of the crime world. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various Cyber Crimes and provides strict punishments (imprisonment terms up to 10 years and compensation up to Rupees 1 crore). The IT Act has also brought many amendments in the other legislations to enhance their scope and applicability wise:[85] (i) The Indian Penal Code (as amended by the IT Act) penalize several Cyber Crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. (ii) Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act, 1872, and (iii) Investigation and

[82] *Supra* note 22 at 186.
[83] *Supra* note 1 at 27.
[84] Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems Managing the Digital Firm* 379 ((Pearson Education, Dorling Kindersley India Pvt. Ltd., New Delhi, 2006).
[85] Nash Haynes, *Cyber Crime*191 (Tech Press, UK, 2018).

adjudication of Cyber Crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

Conclusion

Cybercrime is a serious crime in all over the world. Cybercrimes are internet crime, online illegal money, data diddling, online offense misuse, fraud internet, cybersquatting, data leakage, cyber-staking, web spoofing, viruses etc. Information Technology Act, 2000 is the main statute dealing with directions and requirements relating to cyber world; it provides a step forward in the field law with the modernized changing measurement of the crime world. The main purpose of the Act is to provide lawful recognition to electronic commerce and to assist filing of electronic records with the Government.