majority of respondents, followed by other information resources available on internet.

- The majority best part of respondents 33 (53.23%) not face Copyright Act problem for searching information on internet while 29(46.77%) respondents face copyright act problem

## Conclusion and Recommendations

The present study indicates that a majority of faculty members were used the Internet as one of their sources of information. Most of faculties are used Internet daily for teaching, e-mail, research and development purposes and seeking current knowledge. The study advices to college, To organize user awareness programmed on Internet, Provide internet facility for maximum hours in the college, To organize a workshop or Seminar for usefulness of internet in teaching-learning, learning internet tool kit, membership of various discussion forum, organize short term course on Internet and how its use, explain about search strategy and create a enviourment for maximum use of e-resources on internet and its use in their academic work.

## References


- Adegbore,A.M.(2010). Internet Access and Use by Students of Private Universities in Ogun State, Nigeria. Library Philosophy and Practice(March).2-4
- Biradar, B. S., Rajshekhar, G.R., & Sampath Kumar, B. T. (2006). A study of Internet usage by students and faculties in Kuvempes University. Library Herald 44 (4): 283-294.
- Biradar, B.S., and Sampath Kumar, B.T.(2005). Use of Internet by Physicists in Univeristy of Karnataka State : a Comparative study, ILA Bulletin 41(4). 26-39.
- Devendra Kumar.(2010). Faculty Use of Internet Services at a University of Agriculture and Technology. Library Philosophy and Practice.(February)1-8.
- Eynon, R. (2005). The use of the Internet in higher education: Academics' experiences of using ICTs for teaching and learning. Aslib Proceedings: New Information Perspectives 57 (2): 168-180.
- Kaur, A. (2000). Internet and libraries. Library Herald 38 (1).24-31
- Loan, Fayaz Ahmad (2011). Internet use by college students across disciplines: a study. Annals of Library and Information Studies.58 (June).118-127.
- Mahajan, P. (2005). Internet use by researchers: A study of Panjab University, Chandigarh . Library Philosophy & Practice.8 ( 2).
- Mandalia, S.H., and Raval, B.N. (2011). Internet consumption among the faculties of higher studies. Share Journal of Multidisciplinary Research and Studies, 2(1). 48-51.
- Prasher, R. G. (2003). Indian libraries in IT environment. Ludhiyana: Medallion Press.
- Rajeev, K., & Kaur, A. (2005): Use of Internet by teachers and students in Shaheed Bhagat Singh College of Engineering & Technology: A case study. Journal of Library and Information Science, 29 (1/2), 81-94.
- Raval, Bhavesh N. & Prajapati, Rajan I. (2012). Use of internet by faculty members of various colleges of Mehsana City, Gujarat : A Study. International Research Journal of Library and Information Science, 2 (1). http://www.irjlis.com/index.htm
- Savolainen, R. (1999). The role of the Internet in information seeking: Putting the networked services in context. Information Processing and Management, 35(6), 765-782.
- Singh, A.(2000). Uses of Internet in a Univeristy Library : A Case Study. ILA Bulletin, 37(4): 150-152
- Womboth, B.S.H., & Abba, T. (2008). The state of Information and Communication Technology (ICT) in Nigerian university libraries: The experience of Ibrahim Babangida Library, Federal University of Technology, Yola. Library Philosophy and Practice (December).




ISSN : 0976-4712 **S:H:A:R:E** A Study Hub for Analysis, Research and Evaluation


# Cyber Crime: Treats to Security System

**A. D. Gaur**
C. P. Patel & F.H Shah Commerce College, Anand, Gujarat

**G.K.S. Gaharwar**
School of Engineering & Technology, Navrachana University, Vadodara, Gujarat

*Information Technology has given a new dimension to communication in the present time Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the present pace of life but at the same time also resulted in various threats to the consumers and other institutions for which it's proved to be most beneficial. Various criminals like hackers, crackers have been able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. and have been successful in gaining "unauthorized access" to the user's computer system and stolen useful data to gain huge profits from customer's accounts.*

*This paper contributes an understanding of the effects of negative use of Information technology, and how far the present law in India is successful in dealing with the issue, and what way is the legal structure lagging to curb the crime.*

**Key word:** Information Technology Cyber Crime website hacking Cyber Law

## Introduction

Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the present pace of life but at the same time also resulted in various threats to the consumers and other institutions for which it's proved to be most beneficial. Various criminals like hackers, crackers have been able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. and have been successful in gaining "unauthorized access" to the user's computer system and stolen useful data to gain huge profits from customer's accounts.

Intentional use of information technology by cyber terrorists for producing destructive and harmful effects to tangible and intangible property of others is called "cyber crime". Cyber crime is clearly an international problem with no national boundaries. Hacking attacks can be launched from any corner of the world without any fear of being traced or prosecuted easily. Cyber terrorist can collapse the economic structure of a organization if there is no proper security and safety to protect the data from being misused. The only safeguard would be better technology to combat such technology already evolved and known to the Hackers. But that still has threat of being taken over by the intellect computer criminals.

Though there are many techniques evolved to curb the criminal activities by cyber terrorists but still the problem persists due to inadequate legal structure in the country and has failed to produce a deterring effect on the

criminals.

**What is Cyber Crime?**

Cyber terrorists usually use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. Internet is one of the means by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling illegal articles, pornography etc. this is done through many methods such as phishing, spoofing, pharming, internet phishing, wire transfer etc. and use it to their own advantage without the consent of the individual.

Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and threatened by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages. And it's been reported that many institutions in US, Britain and Europe have secretly paid them to prevent huge meltdown or collapse of confidence among their consumers.

## Various types of Threats

**Computer Viruses**

"The essential feature of a computer program that causes it to be classified as a virus is not its ability to destroy data, but its ability to gain control of the computer and make a fully functional copy of itself." It mimic the attributes of their real-world counterparts. Computer viruses replicate, cause damage to an otherwise healthy system, and can spread from host to host. Like real-world viruses, a computer virus needs a host, a means of transportation. In the digital world this can be in e-mail, other programs, or media (cd/floppy/tape/usb flash). There is one caveat however - computer viruses need to be activated. Much the same way those carcinogens in our bodies won't give us cancer unless they are activated, computer viruses need to be activated as well, usually via a click or open command.

Viruses are used to infect the user's computer and damage data saved on the computer by use of "payload" in viruses which carries damaging code.

**Phishing**

"Phishing is online identity theft in which confidential information is obtained from an individual." By using e-mail messages which completely resembles the original mail messages of customers, hackers can ask for verification of certain information, like account numbers or passwords etc. here customer might not have knowledge that the e-mail messages are deceiving and would fail to identify the originality of the messages, this results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it.

**Spoofing**

This is carried on by use of deceiving Websites or e-mails. These sources mimic the original websites so well by use of logos, names, graphics and even the code of real bank's site.

Commonly observed that see spoofed accounts used to send spam, phishing content, or malicious viruses. Spammers will steal a real person's e-mail address in order to trick anti-spam filters and make the e-mail seem legitimate and written by a real person, possibly someone you know.

**Internet Pharming**

Hacker here aims at redirecting the website used by the customer to another bogus website by hijacking the victim's DNS server (they are computers responsible for resolving internet names into real addresses - "signposts of internet), and changing his I.P address to fake website by manipulating DNS server. This redirects user's original website to a false misleading website to gain unauthorized information.

**Pornography**

The literal mining of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc."





This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Adult entertainment is largest industry on internet. There are more than 420 million individual pornographic WebPages today.

Research shows that 50% of the web-sites containing potentially illegal contents relating to child abuse were 'Pay-Per-View'. This indicates that abusive images of children over Internet have been highly commercialized.

**Investment Newsletter**

We usually get newsletter providing us free information recommending that investment in which field would be profitable. These may sometimes be a fraud and may cause us huge loss if relied upon. False information can be spread by this method about any company and can cause huge inconvenience or loss through junk mails online.

**Banking/Credit card Related crimes**

Wire transfer is the way of transferring money from one account another or transferring cash at cash office. This is most convenient way of transfer of cash by customers and money laundering by cyber terrorists. There are many guidelines issued by Reserve Bank of India (RBI) in this regard, one of which is KYC (Know Your Customer) norms of 2002. Main objective of which is to:

1) Ensure appropriate customer identification, and
2) Monitor the transaction of suspicious nature and report it to appropriate authority every day bases.

Huge loss may cause to the victim due to this kind of fraud. This is done by publishing false digital signatures. Most of the people lose credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.

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.

Uses of stolen card information or fake credit/debit cards are common. Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami

**Identity Theft**

"The popular media definition of identity theft specifies the appropriation of an individual's personal information to provide access for the criminal to credit lines, purchases and cash."

Identity theft is the fastest growing crime in countries like India. Identity theft is when someone uses personal information about you in an attempt to impersonate you. Identity thieves often do this to make purchases, establish accounts in your name, and sometimes commit more serious crimes. Identity theft is a vehicle for perpetrating other types of fraud schemes.

**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. It also includes automatic changing the financial information for some time before processing and then restoring original information.

**E-commerce/ Investment Frauds:-**

An offering that uses false or fraudulent claims to solicit investments 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 individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

**Sale of illegal articles:**

This would include trade of narcotics,

weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily people receive so many emails with offer of banned or illegal products for sale.

## Measures to Curb the Crime

Though by passage of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers, crackers etc. various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users. Few basic prominent measures used to curb cyber crimes are as follows:

**Anti-virus software**

Anti-virus software is the countermeasure program used to "inoculate" computer viruses.

Anti-virus software works in two ways. The first and the staple of the industry are based on signature files. When a computer virus is reported, the virus is examined and a signature file is created for inoculating the virus. This inoculation is added to the anti-virus software database and is used when scanning computers to identify and destroy viruses. Unfortunately this is a reactive process so someone has to be the guinea pig and get infected.

The other more progressive way of identifying viruses is called heuristics. This method will be the future of the industry and is basically the only hope we have in eliminating computer viruses. Heuristics monitor all activity on your computer and if a program is "acting" like a virus, then a red flag is raised and it is destroyed or contained and reported.

**Encryption**

"Encryption is a way of 'scrambling' a message before sending it and then 'unscrambling' it when it is received at the other end." This is considered as an important tool for protecting data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way except for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.

Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method. Usual problem lies during the distribution of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill. Public key cryptography was one solution to this where the public key could be known to the whole world but the private key was only known to receiver, it is very difficult to derive private key from public key.

**Synchronized Passwords**

These passwords are schemes used to change the password at user's and host token. The password on synchronized card changes every 30-60 seconds which only makes it valid for one time log-on session. Other useful methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases

**Firewalls**

"Firewalls inspects each packet to ensure that it adheres to the policy that has been configured or not, and then perform the necessary action associated to that particular rule."

It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in computer which is recognised and verified by one's system. It only permits access to the system to ones already registered with the computer.

**Digital Signature**

"Digital signature can be described as a method of authenticating data i.e. to verify that the received document is indeed from the claimed sender and its content has not been altered in any way since the person has created





it."

Digital signatures are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer's signature is identified by using this method before banks enter into huge transactions.

## Search Procedures

**Investigations**

Section 75 of Information Technology Act, 2000 takes care of jurisdictional aspect of cyber crimes, and one would be punished irrespective of his nationality and place of commission of offence. Power of investigation is been given to police officer not below the rank of Deputy Superintendent of police or any officer of the Central Government or a State Government authorised by Central Government. He may enter any public place, conduct a search and arrest without warrant person who is reasonably expected to have committed an offence or about to commit computer related crime. Accused has to be produced before magistrate within 24 hours of arrest. Provisions of Criminal Procedure Code, 1973 regulate the procedure of entry, search and arrest of the accused.

**Problems Underlying Tracking of Offence.**

Most of the times the offenders commit crime and their identity is hard to be identified. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of other countries. Most of the countries lack skilled law enforcement personnel to deal with computer and even broader Information technology related crimes. Usually law enforcement agencies also don't take crimes serious, they have no importance of enforcement of cyber crimes, and even if they undertake to investigate they are posed with limitation of extra-territorial nature of crimes.

## Data Protection

Information stored on the owner of the computer would be his property and must be protected there are many ways such information can be misused by ways like 'unauthorized access, computer viruses, data typing, modification erasures etc. Legislators had been constantly confronted with problem in balancing the right of the individuals on the computer information and other people's claim to be allowed access to information under Human Rights. Personal information shall only be obtained for lawful purpose, it shall only be used for that purpose, mustn't be disclosed or used to effectuate any unlawful activity, and must be disposed off when the purpose is fulfilled.

Though Data Protection Act aims at protecting privacy issues related to the information but still we find no mention of the word "privacy" in the Act, nor is it defined, further the protection comes with various exemptions, including compulsory notification from the Commissioner in certain cases of the personal data. Due to the change in the regime of information technology for the date European Convention came, on which the Act is based amendments in the Act is advised for matching the present situation and curbing the crime in efficient way.

There is no Data Protection Act in India, the only provisions which talks about data protection are Section 72 and Section 43 of Information Technology Act, 2000. There must be a new Law to deal with the situation for a person to know that the Controller is processing his data concerning him and also that he must know the purpose for which it has been processed. It is a fundamental right of the Individual to retain private information concerning him provided under Article 21 of the Indian Constitution, which says: "No person shall be deprived of his life or personal liberty except according to procedure established by law". And due to the increasing trend of the Crime rate in the field separate legislation is required in this context for better protection of individuals.

## IT ACT 2000

**Emergence of Information Technology Act**

In India, the Information Technology Act 2000 was enacted after the United Nation

General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step towards the Law relating to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. It was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996.

**Some Noteworthy Provisions of the Act**

| Section | Cause | Provision |
|---|---|---|
| 43 | Damage to Computer system etc. | Compensation for Rupees 1crore. |
| 66 | Hacking (with intent or knowledge) | Fine of 2 lakh rupees, and imprisonment for 3 years. |
| 67 | Publication of obscene material in e-form | Fine of 1 lakh rupees, and imprisonment of 5years, and double conviction on second offence |
| 68 | Not complying with directions of controller | Fine up to 2 lakh and imprisonment of 3 years. |
| 70 | Attempting or securing access to computer | Imprisonment up to 10 years. |
| 72 | For breaking confidentiality of the information of computer | Fine up to 1 lakh and imprisonment up to 2 years |
| 73 | Publishing false digital signatures, false in certain particulars | Fine of 1 lakh, or imprisonment of 2 years or both. |
| 74 | Publication of Digital Signatures for fraudulent purpose. | Imprisonment for the term of 2 years and fine for 1 lakh rupees. |

**How Efficient Is Information Technology Act 2000?**

It can't be disputed that Information Technology Act, 2000 though provides certain kinds of protections but doesn't cover all the spheres of the I.T where the protection must be provided. Copyright and trade mark violations do occur on the net but Copy Right Act 1976, or Trade Mark Act 1994 are silent on that which specifically deals with the issue. Therefore have no enforcement machinery to ensure the protection of domain names on net. Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn't hinder the violations caused in the cyberspace.

Even the Internet Service Providers (ISP) who transmits some third party information without human intervention is not made liable under the Information Technology Act, 2000. One can easily take shelter under the exemption clause, if he proves that it was committed without his knowledge or he





exercised due diligence to prevent the offence. It's hard to prove the commission of offence as the terms "due diligence" and "lack of knowledge" have not been defined anywhere in the Act. And unfortunately the Act doesn't mention how the extra territoriality would be enforced. This aspect is completely ignored by the Act, where it had come into existence to look into cyber crime which is on the face of it an international problem with no territorial boundaries.

## Conclusion

No one can deny the positive role of the cyber space in today's world either it be political, economic, or social sphere of life. But everything has its pro's and corns, cyber terrorists have taken over the technology to their advantage. To curb their activities, the Information Technology Act 2000 came into existence which is based on UNICITRAL model of Law on e-commerce. It has many advantages as it gave legal recognition to electronic records, transactions, authentication and certification of digital signatures, prevention of computer crimes etc. but at the same time is inflicted with various drawbacks also like it doesn't refer to the protection of Intellectual Property rights, domain name, cyber squatting etc. There is an urgent need for unification of internet laws to reduce the confusion in their application. For e.g. for publication of harmful contents or such sites, we have Indian Penal Code (IPC), Obscenity Law, Communication Decency law, self regulation, Information Technology Act 2000 ,Data Protection Act, Indian Penal Code, Criminal Procedure Code etc but as they deal with the subject vaguely therefore lacks efficient enforceability mechanism. There's need for a one Cyber legislation which is coordinated to look after cyber crimes in all respects. With passage of time and betterment of technology in the present date, has also resulted in numerous number of Information technology related crimes therefore changes are suggested to combat the problem equally fast.

## References


- Sachin Dnyandeo Ubarhande, 'Computer Viruses', International Journal of Scientific & Engineering Research Volume 2, Issue 12, Dec. 2011 ISSN 2229-5518.
- Aaron Emigh, 'Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures' ITTC Report on Online Identity Theft Technology and Countermeasures
- Sankar Sen, 'Human Rights & Law Enforcement', 1st ed., 2002, Concept Publishing Co., New Delhi.
- Dr. Subhash Chandra Gupta, 'Information technology Act, 2000 and its Drawbacks', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
- Mark Poster, 'THE SECRET SELF: The case of identity theft' Cultural Studies Vol. 21, No. 1 January 2007, pp. 118 _140, ISSN 0950-2386 print/ISSN 1466-4348 online.
- Mark Buckley, 'Newsletter of the British Computer Society', LMSG News, ISSN 1336-8749, Issue 44, November 2002.
- Yadav Priyanka , Srivastava Sindhu & Trehan Vani, 'DIGITAL SIGNATURE', I.J.E.M.S., ISSN 2229-600X ,VOL.3(2) 2012: 115 - 118
- Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi. 1992 U.S. App. LEXIS 9562 (4th May 4, 1992)
- Justice S.B. Sinha, 'Cyber Crime in the Information Age', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
- S.K Verma and Raman Mittal, 'Legal Dimensions of Cyber Space, 2004, Indian Law Institute, New Delhi.