# "Cyber Crime – A Threat to Persons,Property And Government"

**Ms Nisha[#1], Ms Usha[#2]**

[#]**Asst Professor, Computer Sc Deptt, GCW Karnal**

ncnisha24dec@gmail.com1

usha16feb@gmail.com2

***Abstract*- In the present day world, India has witnessed an unprecedented index of Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cyber crimes has increased over the last decade. Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. In this paper, i have discussed various categories of cyber crime and cyber crime as a threat to person, property, government and society. In this paper I have suggested various preventive measures to be taken to snub the cyber crime.**

## *A.* INTRODUCTION

Computer crime has been an issue in criminal justice and criminology since the 1970s. In this venue, the types of computer crimes have been categorized in two ways. First, a prevalent activity is that of criminals stealing computers. Second, criminals use computers to commit crimes. The recent development of the Internet has created a substantial increase in criminals using computers to commit crimes. Thus, an emerging area of criminal behaviour is cybercrime. Cybercrime is a criminal act using a computer that occurs over the Internet. The Internet has become the source for multiple types of crime and different ways to perform these crimes. The types of cybercrime may be loosely grouped into three categories of cybercrimes. First, the Internet allows for the creation and maintenance of cybercrime markets. Second, the Internet provides a venue for fraudulent behaviour (i.e., cyber fraud). Third, the Internet has become a place for the development of cybercriminal communities. The purpose of this research paper is to outline and exemplify these different forms of communities. The research paper then shifts into a discussion of policy steps to reduce some forms of cybercrime. In the present day world, India has witnessed a huge increase in Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking the data or system to commit crime. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cyber crimes has increased over the last decade. Cyber crime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Though there is no technical definition by any statutory body for Cyber crime, it is broadly defined by the Computer Crime Research Center as - "Crimes committed on the internet using the computer either as a tool or a targeted victim." All types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Cyber crime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber crime could also include non-monetary offenses, such as creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet. An important form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users. Various types of social networking sites are used for this purpose to find the identity of interested peoples. There are two ways this is done - phishing and harming, both methods lure users to fake websites, where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

## II. History

The first recorded cyber crime took place in the year 1820 which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since

3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cyber crime.

## III. Manifestations

Basically cyber crimes can be understood by considering two categories, defined for the purpose of understanding as Type I and Type II cyber crime.

*A) Type I:* cyber crime has the following properties: It is generally a single event from the perspective of the victim. For example, the victim unknowingly downloads or installs a Trojan horse which installs a keystroke logger on his or her machine. Alternatively, the victim might receive an e-mail containing what claims to be a link to a known entity, but in reality it is a link to a hostile website. There are large number of key logger softwares are available to commit this crime. It is often facilitated by crime ware programs such as keystroke loggers, viruses, root kits or Trojan horses. Some types of flaws or vulnerabilities in software products often provide the foothold for the attacker. For example, criminals controlling a website may take advantage of vulnerability in a Web browser to place a Trojan horse on the victim's computer. Examples of this type of cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

*B) Type II* : cyber crimes, at the other end of the spectrum, includes, but is not limited to activities such as computer related frauds, fake antivirus, cyber-stalking and harassment, child predation, extortion, travel scam, fake escrow scams, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities. The properties of Type II cyber crimes are : • It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations.

• It is generally facilitated by programs that do not fit into the classification of crimeware. For example, conversations may take place using IM (Instant Messaging). Clients or files may be transferred using FTP.

## IV. Prevention Of Cyber Crime

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. Identification of exposures through education will assist responsible companies and firms to meet these challenges. One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site. One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day. An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds. It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day. Web servers running public sites must be physically separately protected from internal corporate network. It is better to use a security programs by the body corporate to control information on sites. Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens. IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace. As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime. A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy

and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

## V. Conclusion

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. It is ironic that those who in secret break into computers across the world for enjoyment have been labeled as deviance. Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Hackers are as old as the Internet and many have been instrumental in making the Internet what it is now. In my view point hacking and computer crime will be with us for as long as we have the Internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. Luckily,the government is making an effort to control the Internet. Yet, true control over the Internet is impossible, because the reasons the Internet was created. This is why families and the institution of education of is needed, parents need to let their children know what is okay to do on the computer and what is not and to educate them on the repercussions of their actions should they choose to become part of the subculture of hackers. In finishing this paper, the true nature of what computer crime will include in the future is unknown. What was criminal yesterday may not be a crime the next day because advances in computers may not allow it. Passwords might be replaced for more secure forms of security like biometric security. Most of the recorded computer crimes cases in most organization involve more than individual and virtually all computer crime cases known so far are committed by employer of the organization. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Without question, law enforcement must be better prepared to deal with many aspects of computer-related crimes and the techno-criminals who commit them. This article is not meant to suggest that programmers or computer users are fraudulent people or criminal but rather to expose us to the computer-related crime and provides ways to prevent them. Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base ofcommunications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime.

## REFERENCES


[1] Communications Fraud Control Association. 2011 global fraud loss survey. Available:
[2] http://www.cfca.org/fraudlosssurvey/, 2011.
[3]
[4] F. Lorrie, editor. “Proceedings of the Anti-Phishing Working Groups”, 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.
[5]
[6] I. Henry, “Machine learning to classify fraudulent websites”. 3rd Year Project Report, Computer
[7] Laboratory, University of Cambridge, 2012.
[8]
[9] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available:
[10] http://www.microsoft.com/security/sir/.
[11]
[12] Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
[13]
[14] N. Leontiadis, T. Moore, and N. Christin. “Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade”. In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.
[15]
[16] Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved
[17] December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html.
[18] Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.