International Research Journal of Interdisciplinary & Multidisciplinary Studies (IRJIMS)
A Peer-Reviewed Monthly Research Journal
ISSN: 2394-7969 (Online), ISSN: 2394-7950 (Print)
Volume-I, Issue-I, February 2015, Page No. 107-112
Published by: Scholar Publications, Karimganj, Assam, India, 788711
Website: http://www.irjims.com

Networking Technology & Its Users: A Growing Concept of Victimology

Mr. Debabrata Pani
Research Scholar in Law, Utkal University, Bhubaneswar, India

Abstract

The period of last two decades witnessed a major change in India in the areas of information explosion and technological advancement through wireless networking technology. In this study networking technology indicates two particular technological advancements which are widely used by the public available in the form of Mobile Phone and Internet. The users of these systems are frequently getting victimized during the course of their subsequent use. The users face many complicacies that are beyond their knowledge caused due to these systems. Such situation arises by an intruder, unlawfully without the authorization/permission of the user. As these technological systems work only by the command of the operator, they are unable to render safety to the user, because the operator/intruder may not be the user. Consequently all these three mechanisms are threatening more to their users. Numerous times the users have harassed and being victimized by the application of these systems. So the innocent users became the victims by using these technological systems. The users have surrounded by innumerable malicious items like viruses, worms, hacking, phishing, malware, spyware and many more during the use of these technological systems. Thus networking technology though renders optimum service to its users, but finally leads towards a newer concept of victimology and creates a State full of victims made out of it. On the other hand there are no perfect legal enforcements available in India to curb the victimization of the innocent users caused by the above said technologically developed systems.

Introduction: Technology has always been intertwined with society's progress but never before, in history, has technology been so visibly linked to improvements in standards of living. The human aspirations for a better life increasingly depend on technology and its effects on all aspects of life. Because of technology, our world is developing at a phenomenal speed. Technology's pace and scope of changes are having profound effects on every human being. In modern era of global capitalism, technological advancement and information explosion are became very crucial concepts viewing the recent technological progress. During the last two decades i.e. the last decade of 20th century and first decade of 21st century, radical changes have been observed in the sphere of networking technology in Indian context. Networking technology, in this study, implies communication of information by/to the individuals jointly or severally with the help of a wire free networking system available commonly in the form of Internet and Mobile Phone. These two items deal with very personal information and secrets of the concerned user which are also sensational in nature. The users communicate their personal matters and sharing with their close ones. But many times the users experience about malfunctioning of the above mentioned networking systems. They unnecessarily became accountable for misconduct committed by an intruder (offender). Thus a victim[1] loses his right to privacy, right to freedom etc. When use of technology takes the human desire to unlimited extent of facilities at that time these are some cases, which may disrupt the use of technology as it pilots the users towards victimization.

This paper provides a review of various modes of networking technology system responsible for victimizing the ignorant users along with the insufficient Indian legal system to curb the newly growing victimology concept.

Networking Technology Users and Victimology: Crime branch officials are stumped by a complaint from a West Delhi-based married woman who claimed her face was morphed on the torso of a lingerie model and put up on a US-based website that "promoted friendship between people of different sexes." Although the police managed to get her photograph removed from the website, they are unable to track the hacker who posted the picture[2]. An Internet user shocked by finding one day his personal photographs (husband & wife) on a porn site. A Mobile Phone user came to know that someone get into his phone without authority and steal his details. In the above cited examples one thing is common that all categories of users harassed by these technologically developed systems. So one may ask, what the wrong, they do? Do they commit mistake by using these sophisticated systems? Is it the consequence for using these systems? Undoubtedly answer to all the above questions are 'No'. But the users are getting harassment and being victimized only due to adoption of these technologically developed systems. In this way a relationship starts between the users and networking technology as victim and source of victimisation respectively.

Victimology: Victimology is the study of crime victims and the psychological effects of being a victim[3]. It is a branch of criminology that scientifically studies the relationship between an injured party and an offender by examining the causes and the nature of the consequent suffering[4]. This is the study of the ways in which the behaviour of crime victims may have led to or contributed to their victimization[5]. So victimology, is a study regarding the crime victims, psychology of the victims as he/she is innocent, reasons of suffering of the victims, ways leading the victims towards victimisation etc. Victim[6] is always an innocent and ignorant person. He/she may be led in the path of victimization distrustfully by anybody. Specifically, victimology focuses on whether the perpetrators were complete strangers, mere acquaintances, friends, family members, or even intimates and why a particular person or place was targeted[7]. In this particular study the offender is known as the intruder as he trespasses into the victim's personal database and software. He can control the systems used by the victim and even can damage the hardware of the systems by fraudulent exercise of malwares, viruses, worms etc. The intruder's deceitful act is mala in *se*, as declared by Indian Laws. The position of the victims due to networking technology is equal that with all other forms of victimisation. The user being targeted and victimized by the offender/intruder, without doing anything wrong on his part. Finally, the users get into the trap of offender of networking technology which may inflict economic costs, physical injuries, and psychological harm to them.

Modes of Victimisation: Cyber intruders/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 intruders 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 phising, 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 victimised 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 collapse of confidence among their consumers[8].

Internet:

a) Computer Viruses: A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Note that a program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "virus".

Many people use the term loosely to cover any sort of program that tries to hide its (malicious) function and tries to spread onto as many computers as possible. Viruses are very dangerous; they are spreading faster than they are being stopped, and even the least harmful of viruses could be fatal. For example, a virus that stops a computer and displays a message, in the context of a hospital life-support computer, could be fatal. Even the creator of a virus cannot stop it once it is "in the wild"[9].

Generally, there are two main classes of viruses. The first class consists of the file infectors, which attach themselves to ordinary program files. These usually infect arbitrary .COM and/or .EXE programs, though some can infect any program for which execution is requested, such as .SYS, .OVL, .PRG, & .MNU files. File infectors can be either direct action or resident. A direct-action virus selects one or more other programs to infect each time the program that contains it is executed. A resident virus hides itself somewhere in memory the first time an infected program is executed, and thereafter infects other programs when they are executed or when certain other conditions are fulfilled. The second category is system or boot-record infectors: those viruses that infect executable code found in certain system areas on a disk, which are not ordinary files. On DOS systems, there are ordinary boot-sector viruses, which infect only the DOS boot sector, and MBR viruses which infect the Master Boot Record on fixed disks and the DOS boot sector on diskettes. Examples include Brain, Stoned, Empire, Azusa, and Michelangelo. Such viruses are always resident viruses. Finally, a few viruses are able to infect both (the Tequila virus is one example). These are often called "multi-partite" viruses, though there has been criticism of this name; another name is "boot-and-file" virus. Stealth virus, polymorphic virus, fast and slow infectors are some categorised viruses[10].

Viruses are used by Hackers to infect the user’s computer and damage data saved on the computer by use of “payload” in viruses which carries damaging code. Person would be liable under I.T Act only when the consent of the owner is not taken before inserting virus in his system. The contradiction here is that though certain viruses causes temporary interruption by showing messages on the screen of the user but still it’s not punishable under Information Technology Act 2000 as it doesn’t cause tangible damage. But, it must be made punishable as it would fall under the ambit of ‘unauthorised access’ though doesn’t cause any damage. Harmless viruses would also fall under this expression.

b) Computer Worms: A computer worm is a self-contained program or set of programs that is able to spread functional copies of itself or its segments to other computer systems usually via network connections. Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms - host computer worms and network worms. Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Host computer worms where he original terminates itself after launching a copy on another host so there is only one copy of the worm running somewhere on the network at a given moment are also called "rabbits".

Network worms consist of multiple “segments”, each running on different machines and possibly performing different actions and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes. Network worms that have one main segment, which coordinates the work of the other segments, are sometimes called “octopuses”. The Internet Worm – 1988, The SPAN network worm – 1989, The Christmas tree Worm – 1987 are some world famous worms[11].

c) Trojan Horse: A Trojan horse program pretends to do one thing while actually doing something completely different. They let a hacker access the victim's hard disk, and also perform many functions on his computer (shut down his computer, open and close his CDROM drive etc.). Threats by Trojan horse are briefly described as below.

Password Trojans: Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. Whether it's an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via Email.

Privileges-Elevating Trojans: These Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileges users and give the attacker access to their account.

Key loggers: These Trojans are very simple. They log all of the victim's keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually don't take much disk space and can masquerade as important utilities, thus making them very hard to detect.

Destructive Trojans: These Trojans can destroy the victim's entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually ripping every file they encounter to pieces.

Joke Programs: Joke programs are not harmful. They can either pretend to be formatting your hard drive, sending all of your passwords to some hacker, self-destructing your computer, turning in all information about illegal and pirated software you might have on your computer to the police (or to Privacy Watch!) etc. In reality these programs do not do anything[12].

d) Phishing: 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[13].

e) Spoofing: This is carried on by use of deceiving Websites or e-mails. These sources imitate the original websites so well by use of logos, names, graphics and even the code of real bank’s site[14].

f) 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 unauthorised information[15].

g) Publishing Obscene Material: Any obscene or vulgar SMS, MMS, or even an audio clip from boyfriends, girlfriends, colleagues, spouses or acquaintances can prove costly for the sender and receiver[16]. Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and transmission of any material in electronic that’s lascivious or appeals to the prurient interest a crime.

h) 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[17].

i) Fake Identity: Giving fictitious details about self on the net or using offensive language, one can at risk being sent to jail for it[18].

Mobile Phone:

A) Mobile phone Cloning: The new tech crime of cell phone cloning involves copying the unique markers of one cell phone onto another. Calls made from the second will then be indistinguishable from those made from the first. The service provider will, of course, bill them to the actual client---the victim who wakes up only when he sees a detailed bill and finds numbers he’s never called[19].

Each cell phone has an erasable-programmable read-only memory (EPROM), its nucleus as it were. Embedded in this chip are the cell phone’s electronic serial number (ESN) and electronic machine identification number (EMIN), comparable to the DNA that makes an individual unique. Unscrupulous cell phone dealers and repairers who have access to the ESN and EMIN of someone’s cell phone may offer it to mobile cloners. Sometimes the information is obtained from service providers. Using special software, the cloner embeds these numbers on the EPROM of another cell phone, from which a user can make calls for which someone else pays.

b) Mobile Spyware: The biggest fear of the mobile users is that the phone has been 'bugged' by any number of spyware programs available for purchase. While some users are a bit paranoid, others have been 'infected' by such software. Due to the fact that these programs are manually installed by the supposed owner of the phone, any and all warnings that may popup due to signing requirements are not an issue. And once the software is installed, it remains hidden to those without technical skills to find them. So, while malicious code (ie. viruses, trojans, etc.) is an issue, it has a lot to overcome to be an effective attack vector. Spyware on the other hand, is prebuilt for specific phone models[20].

c) Malware: Software code designed to invade surreptively to a mobile system and performs some unauthorized destructive activities[21].

d) Phone Phishing: Is done by use of in-voice messages by the hackers where the customers are asked to reveal their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc[22].

e) Spam: Spam is anonymous junk email, and includes several different types of content: adverts; political messages; requests for assistance; emails that ask one to invest large amounts of money or to get involved in pyramid schemes; emails aimed at stealing passwords and credit card numbers, and emails that ask to be sent to friends (chain letters)[23].

f) Theft of Contact List: Theft of corporate contact data could have dire consequences for the employee and the company. We already mentioned that mobile malware can "steal" a contact list and send out short messages containing malware or a link to malware. It would be even worse if the malware packaged your contact information and sent it to a malicious third-party[24].

Resultant effects on Victimology: Intentional use of information technology by cyber intruders for producing destructive and harmful effects to tangible and intangible property of others heads towards a rising concept of victimology in long run. Role of cyber intruders 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 intruders can collapse the economic structure of a country from a place where that country might not have any arrangements like "extradition treaty" to deal with that criminal. In such situation how can be a victim compensated for the loss accrued to him/her. The user-cum-victim goes to whom to claim the liability of the offender. In this way the victimization process will be augmented by the successive use of the networking technology. The Indian legal system have still restricted within the cage of IT Act and least corresponding changes have been made in IPC and CrPC to combat these growing threats due to the use of networking technology.

A Snapshot of Important Cyber Law Provisions in India

Offences	**Section under IT Act**
Hacking (with knowledge)	Sec.43 & Sec.66
Publication of Obscene Material	Sec. 67
Unauthorised access to protected system	Sec. 70
Breach of Confidentiality and Privacy	Sec. 72
Publishing false digital signature	Sec. 73
Publishing digital signature for Fraudulent purpose	Sec.74

Note: Sec.78 of I.T. Act empowers Deputy Superintendent of Police to investigate cases falling under this Act.

Offences	**Section under IPC**
Sending threatening message by email	Sec.503
Sending defamatory message by email	Sec. 499
Forgery of electronic records	Sec.463
Cyber frauds	Sec. 420
Email spoofing	Sec.463
Web Jacking	Sec. 383
Email abuse	Sec 500

This much is not enough to curb the victimization caused by the use of networking technology.

Conclusion: The networking technology imparts great service to mankind through its faster communicative system all together creates a new concept of victimology. The innumerable threats in the form of Virus, Malware, and Trojan etc. are developed by the intruders or so called cyber terrorists to earn heavy amount within minutes by victimizing the innocent and ignorant users. 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. Therefore Nations need to update the Law whether by amendments or by adopting *sui* generic system.

References:

1. Article 1, UN Convention on Justice and Support for Victims of Crime and Abuse of Power
2. The Times of India, 25 Aug.2004
3. Retrieved from Dictionary.com.
4. Encyclopedia Britannica, 2008
5. www.merriam-webster.com
6. ibid.
7. Encyclopedia Britannica. 2010. Encyclopædia Britannica Online. 15 Jul. 2010
8. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
9. www.planetindia.net
10. B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.
11. www.planetindia.net
12. www.planetindia.com
13. www.cybersmart.in
14. www.planetindia.net
15. www.lawersclubindia.com
16. The Times of India, 18 Dec. 2007
17. www.planetindia.net
18. The Times of India, 15 Oct. 2007
19. www.AYJW.org
20. www.About.com
21. www.businessdictionary.com
22. www.cybersmart.in
23. www.ectnews.com
24. www.mcafee.com

*****