ORIGINAL RESEARCH PAPER
Volume-6 | Issue-12 | December-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 93.98
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

CYBER CRIME

Physiology

Malika Singh JR General Surgery

Abhinav Singh JR General Surgery

K.Singh* Professor Physioloigy, PGIMS, Rohtak

ABSTRACT

Cyber Crimes are threats and they are rising day by day due to easy availability of internet. It can be defined as crime, which is not only physically harm the subject, but also give mental and emotional trauma, harm the reputation of subject in society, also involves group of subjects, occurs through modern telecommunication networks through internet e.g.-mail, and mobile phones (via Blue Tooth/ SMS/ MMS). As telecommunication techniques are advanced, immediately interception of these techniques developed by peoples, who are intelligent enough and expert in these technologies but have criminal tendency, thus it is difficult to prevent these crimes. It also breaches the privacy of individual, government offices, nations while disclosing the confidential information's. It spreads wrong and liar information's in public produces terror, panic and fearness, which are sometimes difficult to manage by government, as recently happened when Ram Rahim Baba, chief of Sachcha Sauda Dera in India was convicted in rape case. So, a precautionary measure, net was put off, to prevent wrong, foul spread of news. Activities and informations crossing the international borders are called cyber warfare. Cybercrime against women are defined as crimes against women with a motive to intentionally harm the women psychologically, emotionally, mentally and physically through internet or mobile phones (MPs). So, it is our legal duty to provide cyber security and cybercrime legislation are needed to protect our privacy and data, but this is the paradox as crime legislations are lagging behind the cyber crime.

KEYWORDS

cyber crime, Internet, Mobile Phone, Telecommunication.

Introduction

Cyber crime, also called computer related crime targets the individual or group of individuals using computer or mobile phones as tools, breaches the person's confidentiality, also privacy, produces damage to persons image in society, which may cause physical, mental, emotional, and psychological trauma to individual, even person may make suicidal attempt or suicide[1]. So, proper legislations and prosecutions are required to overcome them. Since technologies are so advanced changing day by day, cyber crime legislations are lagged behind[2]. But, it is very necessary to maintain individual's right of privacy (i.e., fundamental right declared by court) and integrity, privacy of public and private network system.

There are many types of cyber crimes such as:

Hacker: - Computer Hacker refers to a computer user who wants to access data of other individuals via computer through unauthorized means, without his permission or willingness[2].

Cracker: – is referred to hacker with criminal intentions.

To prevent them anti spyware and antivirus solutions capable of detecting viruses are used as security tools. These are present on internet. These programmers automatically scan computer security weaknesses, but some of these are also used by attackers. So, one should be cautious of potential vulnerability of computer system due to availability of potentially malicious security tools and high quality attacks[2].

Cyber Warfare: - It includes cyber espionage, web espionage, and web vandalism, political propaganda distributed denial of services, equipment disruption, cyber attack on critical infrastructures such as power, water, fuel and communications. It is the cyber crime by one country against other country[2]. Example is cyber attack on Estonia infrastructure in 2007 by Russian hackers, as a result country lost billion of Euros, had reduced productivity and business. To combat this BCP38 network ingress filtering techniques were used[3].

Theft: - When a person downloads games, music, movies, methodology, plan and software without the permission from where they originate, thus avoiding law of copyright, it is theft. Since there are some sharing websites, which allow software piracy and plagiarism. But now a day's peoples have becoming aware of copyright and there are laws which avoid persons from piracy[4].

Identity Theft:- This is the problem of those persons, who used online payment mode of money transaction. Here cyber criminal accesses other person's bank account details, debit cards, credit cards, Social Security, personal and other sensitive information, (through face book or else), drain the money or do shopping, buy things online in victim's name. These are also used to fraudulently apply for credit, file taxes, or medical services. It results in major financial losses or even destroys credit history of victim[4].

Cyber stalking: - It is a form of online harassment, where criminal gives online massages, e-mails, personal information, writes wrong things socially. Since they know the victim, use internet to stalk. Sometimes use both online and offline stalk, thus victim's life is deserted, unless victim is not very strong or takes some help[4].

Child soliciting and abuse: - Cyber criminals solicit minors for purpose of child pornography[4].

Malicious software: - This is internet based software or programs that disrupt the network or other software. In simple words they are called computer virus. Mostly virus destroys the sensitive information or data or software present in system itself. They are also known as worms, Trojan horse, Web jacking, e-mail bombing.

Computer Vandalism: - This cyber crime destroys the data instead of stealing, thus transmits the virus.

Cyber Terrorism: - It can be defined as an act of terrorism committed through the use of cyber space or computer resources (Parker 1983), like spread of news of Bomb in train or aero plane, although on search nothing is found. It also includes hacking activities towards individuals, families, companies, and nations. These are organized by groups within networks, to create fear among peoples, for demonstrating power, for making robberies, for blackmailing, after collecting information to destroy people's lives[4,5].

Cyber terrorists make intrusions in foreign intelligence services, make holes in internal security, government officials and information technology, creating internet and server problems. That's why to prevent spread of rumor, government put server down, as it occurred in Haryana state of India at the time of Jat's agitation for reservation.

Cyber Extortion: - It is a type of extortion in which a website, e-mail server, or computer system is repeatedly denying services. In turn these hackers demand money or some information to stop attacks and to offer protection. These cyber extortionist usually attack corporate websites and network, interferes with their services[5]. In 2014 Sony pictures was victimized by cyber extortion[6].

Software piracy: - In this software of some programmer or method or anything is copied illegally and distributed to others or kept with own for personal benefits. It is done at personal level or at company level. In this way software license agreement is broken. Software piracy may cause authorized use, duplication, distribution, or sale of commercially available software. It is also called soft lifting, counterfeiting, internet piracy, hard-disk loading, and OEM unbundling and unauthorized renting.

Denial of service attacks:- In this bandwidth of victim's network or e-mail box is filled up with spam mail, so he cannot utilized his own services for which he is paying.

Harassment: - It is the use of vulgar, obscene, derogatory comments against specific individual taking in consideration of religion, race, and nationality, gender mostly of sexual orientation via computer, net or e-mail. It also includes revenge porn. In some countries law against harassment is made[7,8,9].

Cyber bullying: It is similar to harassment, but not of sexual nature.
Recently it is reported by cyber security firm e-set that maximum cyber attacks occurred on Indian companies (75% on small companies) taking in consideration of India, Japan, Thailand, Singapur, Honkong companies.Every company lost 20 lakhs. Reasons given are use of device from outerside 22%, use of services of third party 19%, security lapse from IT department 17%, funding problem 15%, lapse in cyber security 14%, lack of cyber expert 13%.

So following measures are required like:

1. **Legislation against cyber crime: -** Existing cyber legislation is not efficient to combat and prevent cyber crime even in china, where computer users are maximum. An effective legal framework, technology and laws are required to stop making cyber crime. Although computer fraud and Abuse act (CFAA-1984) is there and used by computers of federal government[2,10].
2. **Internet Security: -** A www represents World Wide Web, which through web server makes information available on network system. Web browsers access the information, which is stored in server and make it available on user's computers. Web through common Gateway Interface provide information with some improvement[2].
3. **Detection system: -** Intrusion detection systems are software and hardware solutions, which detect unwanted attempts to access, manipulate, interfere, and making computers nonfunctional. The IDS consists of sensors to generate security events, a console to generate alerts through a system of rules[2].
4. **Cyber system security standard: -** Cyber system security standard are needed to provide security techniques to reduce cyber attacks and provide guidelines for implementation of cyber securities.
5. **Network Forensics: -** It is concerned with production of digital evidences in court by capture the cyber crime from computer via net[2,4].

Prevention of cyber crimes[4]:

1. Install the antivirus software.
2. Use of firewall so can be protected from hackers.
3. Only secured and standard websites should be used. Credit card, debit card, and money related and personal information's should not be provided to a website seems to be suspicious and stranger.
4. Prepare a password that includes not only letters but also numerals and symbols in such a way nobody can imagine. Also updates password on and off.
5. Children specially below the 17 years of age, should not be allowed to use mobile phones, computers, and net frequently. Parents should always watch how they are using mobile, computers and other things. The parental control software should be installed to keep an eye on them. Now a day's a suicidal Blue Whale game is spreading among teenagers and due to this game many children made suicide worldwide.
6. Social network should be used carefully and online information if posted should be after proper security checking.
7. Secured the mobile devices. We should try to use built in security features in mobile phones, so that nobody can access personal information. One should not store passwords, pin numbers or address, or any other personal information.
8. Encryption should be used for sensitive files e.g., tax returns or financial records, make regular back-ups of all important data, and also store all these at other place.
9. Use public Wi-Fi, Hot spots only in emergency and carefully. Financial or corporate transaction should be avoided on these networks.
10. We should avoid disclosing e-identity and financial information, unless websites are secured.
11. We should be careful to be scammed, should not use a link or file of unknown origin, or any e-mail in box. Always try to find out the source of message.

We should not reply to e-mails which seem to use to verify the information or confirm users ID or password. Since the Phishing is propagated through e-mails. Phishing e-mails may contain links to other e-mails or websites thus affected by malware or may be connected to fake online banking or websites to steal private account information.

1. **Legislations:-** In developing countries law against cyber crimes are weak, so easily exploited. But in developing countries like in United States, it is difficult to invade FBI[11]. In 2015 executive orders are passed in United States to freeze assets of cyber criminals, who are convicted and block their economic acivities[12].
2. **Penalties:-** In New York States penalties for cyber crimes can range from fine and jail for short time or 3-15 years in prison for class C felony.

Some hackers are hired by private companies as information security experts, and in this court can ban convicted hackers from using Internet or computers, even if they are released from jail. This type of punishment is thought to be harsh and draconian.

Conclusion:- Cyber crimes are increasing day by day. Any person who is using Internet can be a victim. So, in these days, everybody should know how the information's are sought through internet.

References:

1. Halder D, Jaishanker K. Cyber crime and victimization of women: Laws , Rights and Regulations. http://www.igiglobal.com/bookstore/titledetails.aspx? Titeid=50518& detailstype+description)Hershey,PA,USA:IGIGLOBAL.ISBN978-1-60960-830-9.
2. Shoba V. An analysis of cybercrime and internet security. www.wjpps.com, 6(5): 2017.
3. Dennis Murphy. War is war? The utility of cyberspaceoperationsin contemporary operational environment. (htpp://web.Archieve.org/web20120320012856/ http://www.carlisle. army.mil/DIME/documents/war%20is%20war%20issue% 20paper%20final2. (DDF.Centre forstrategic Leadership.Archievedfrom the original (htpp:www. carlisle.army.mil/DIME/documents/war%20is%20war% 20issue% 20paper%20final2.pdf) (PDF) on 20 March2012.
4. Types and prevention of cyber crime.htpp://www.civilserviceindia.com/currentaffairs/ articles/types-and-prevention-of –cybercrimehtml.12.8.17.
5. Cybercriminals Need Shopping Money in 2017,Too-Sentinel One(http://sentilone. comRetrieved2017-03-24.
6. Mohanta.Abhijit"Latestest Sony Pictures Breach:A Deadly Cyber Extortion" (http:www.cyphort.com/ latestest –sony –pictures-breach-deadly-cyber – extortion/). Retrieved20September2015.
7. "Save browsing"(http://gooleonlinesecurity.blogspot.jp/2012/06/safe browsing-protecting-web-users-for.html).google. 14 phishing
8. Cybercrime httpps://en.wikipedia.org/wiki/cybercrime.8.12.2017.
9. "1.In Connecticut, harassment by computer is now a crime"(htpps:// web.archive.org/ web/20080410230359/http:www.nerac.com/family/NeracReports/Cybercrimes_CT.ht m) on April10,2008.
10. Blackley CJ. Cybercrime law: international best practices, Doha information Security Conference, Doha, Qatar, June 10-11, 2008.
11. Kshetri, Nir. "Diffusion and Effects of Cyber Crime in Developing Countries" (htpp://web.a.ebscohost.com/ehost/detail/detail?vid==3&sid==21efdbs54-ad43-447fab46-ce7fa854a98f%40sessionmgr4003&hid=4109&bdata = JnNpdGU9Z Whve3 QtbG12ZQ%3D%3#db=buh&an=55328703/).
12. Northam, Jackie."US Creates First Sanctions Program AgainstCybercriminals" (htpp://www.npr.org/blogs/the twoway/2015/ 04/01/396811276/u-s-creates-first-sanctions-program-against-cyberceiminals).