2012 International Conference on Education Technology and Computer (ICETC2012)
IPCSIT vol.43 (2012) © (2012) IACSIT Press, Singapore

Computer crimes, problems, Law enforcement for solving complaints and education

Elham Fariborzi +1 , Mahnaz Hajibaba2

[1] Islamic Azad University, Mashhad Branch, Department of Educational Sciences, Mashhad, Iran
[2] Islamic Azad University, Mashhad Branch, Department of Information Technology, Mashhad, Iran

Abstract. Today, computer crimes are increasing in different countries. Computer crime is an illegal act which is done by a computer. Considering the extent and complexity of computer crime in cyberspace, and using different tools in this space for doing the crime made different the conditions of dealing with the crime in cyber and physical space. There is the extent of occurrence of computer crime these days, so computer users should be careful regarding to their computer security. But if these attacks happened, how can we defend ourselves right? Is there any Law enforcement for the protection of individuals, organizations for dealing with offenders in Iran? The objective of this paper was to describe the problems arising from computer crime, and also introduces legal authorities to resolve complaints of computer crime and give information for prevention of computer crimes to the beloved countrymen. In this paper, there is a systematic review on this matter. In addition, there are some recommendations regarding to computer crime. More results are subsequently explained in the paper.

Keywords: Crime, Computer Crime, Computer Complaints, Computer Problems, Legal Authorities

1. Introduction

Due to being in cyberspace and expansion of the use of computers and the Internet, problems related to them is growing as well. Because many people today have Internet access, computer crime has become a social problem. Nowadays, all the people who are dealing with Internet and computers are worried about being attacked by unknown persons and criminals. Computer crimes may occur by anyone with variable purposes, whether with the goal of breaking the law or learning about information systems and software. Computer crimes are so commonplace that we all should be careful about the security of our computers. But how can we defend if we are the victim of these attacks? Are there any legal centers to support us and deal with the offenders?

This paper outlines the problems of computer crimes and also introduces legal authorities and educates people to learn different ways of prevention and elimination of these crimes as well as reporting.

2. Literature Review

Crime, as a human-social phenomenon, is the result of interaction between human and society. Since personal characteristics of a person are affected by his surroundings, we can consider the environment as the most fundamental cause of the tendency of people to commit crime.

2.1. Definitions of crime

There are various definitions of crime which three of them are given below.

- Punishable under criminal law, as determined by the majority, or in some cases, by a powerful minority [1].

+ Corresponding author. Tel.: (+989155187872); fax: (+985118409110).
E-mail address: (ef_lecturer@yahoo.com; e-fariborzi@mshdiau.ac.ir).

- Any act which is punishable according to the law (Article 2 of the Penal Code).
- Violations of criminal laws of a state, province or federal jurisdiction without any legal justification [2].

Although the term "computer crime" is used every day, there is no general acceptable definition for that. Below are four examples of these definitions:

- A computer crime is an illegal activity that is executed via a computer [3].
- The use of computers or computer related equipment by individuals, groups and organizations with special knowledge of computers [4].
- Misuse of computers, including any illegal or immoral behavior related to automated processing and data transfer [5].
- A crime which is related to technology, computer and Internet [6].

o 2.2. Examples of computer crimes

There are many different types of computer crime and they are getting more expanded. Here we mention some of the most common computer crimes.

- Use a computer to harm or access to information. Here the computer is the target [7].
- Money laundering, child pornography and illegal banking transaction [7].
- Logical bomb: It remains inactive in a system until a specified time or event. Then, it starts to delete system or network files [7].
- Identity theft: Criminals try to get username and password of others in order to access their online accounts. If this is done by deceiving the account holder to reveal his confidential information, using fraudulent sites or emails, it is called Phishing [8].
- Denial of service: A purposeful attempt to disrupt the legitimate user to access a desired service [9].

3. Method and Findings

Based on the literature review regarding to computer crimes, researchers have done a study for identifying the different types of computer crimes, problems and law enforcement for solving complaints. This study was a systematic review on computer crime. A systematic review is literature review focused on a single question that tries to identify, appraise, select and synthesize all high quality research evidence relevant to that question [10].

3.1. The status of computer crime in Iran and abroad

In the following, we will discuss the enacted laws, current computer crimes and ways of reporting them in America, China, Canada, Switzerland and Iran.

3.1.1. America

The first federal computer crime law, Counterfeit Access Device and Computer Fraud and Abuse Act, was enacted in 1984 by America's congress [11]. Based on reports from 494 U.S. companies, government agencies, financial and medical institutions, most attacks have been related to: Domestic abuse of network access (59%), virus (52%), mobile or laptop theft (50%), phishing (20%) and misuse of instant messaging (25%) [12].

The following chart which has been reported by IC3 [2], shows the Internet fraud in America from 2000 to 2010. Most of these complaints are related to electronic commerce, including online auction and credit card. Additionally, identity theft has increased in the recent years [13].

[2] Internet Crime Complaint Center

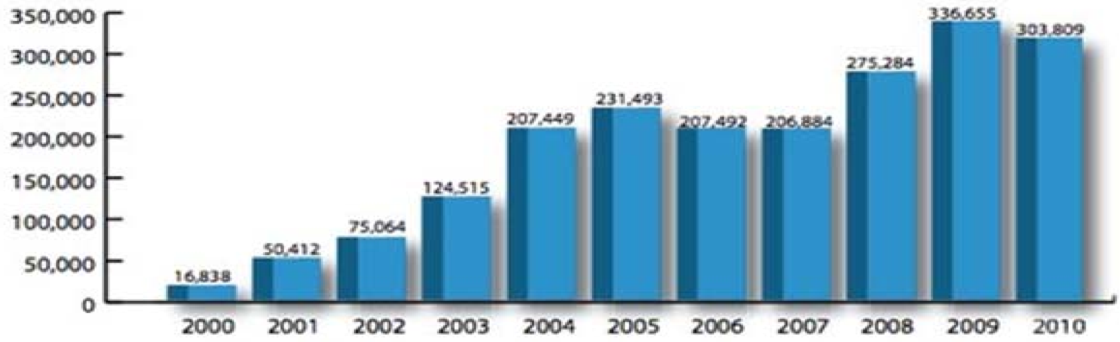

Chart 1: Internet Fraud in America From 2000 to 2010 (IC3)

According to chart 1, Internet fraud in 2000 had the lowest and in 2009 had the highest rate. It is noticeable that the crime rate in 2010 has fallen to 32846 cases compared to 2009.

There are diverse centers in America to report computer crimes. The California Highway Patrol is one of the state agencies that deal with computer crimes. According to its laws, some crimes require immediate attention, such as damaging or changing data, accessing to computer systems and using the Internet domain of another person [14].

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, we can refer to the following table [15].

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (i.e. hacking)	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Password trafficking	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Counterfeiting of currency	• U.S. Secret Service
Child Pornography or Exploitation	• FBI local office • if imported, U.S. Immigration and Customs Enforcement • Internet Crime Complaint Center
Internet fraud and SPAM	• FBI local office • U.S. Secret Service • Federal Trade Commission (online complaint) • if securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint) • Internet Crime Complaint Center
Internet harassment	• FBI local office
Internet bomb threats	• FBI local office • ATF local office

Table 1: Federal Investigative Law Enforcement Agencies

3.1.2. China

Statistics show that computer crimes are increasing every year in China. In 2002, nearly 6633 offences, in 2003 about 11614 offences and in 2004, 13654 offences were reported. Most computer crimes in China respectively include fraud, identity theft and dissemination of immoral information [16]. Since 1994, China has enacted several laws to monitor the Internet, such as: Security of Computer Information Systems, Copy Right, Monitoring the Internet Information System and Internet Publishing Right [17]. Computer crimes in China can be divided into 5 categories:

- Using computers for production and distribution of pornographic materials
- Economic crimes committed via the Internet
- Dissemination of computer viruses and hacking
- The citizens’ personal rights abuses, such as insulting and attacking people via the Internet
- Endangering national security [18].

3.1.3. Canada

Canada was the first country that specifically addressed computer crimes in its federal law in 1983 and enacted several laws [19], including Unauthorized use of computers, Mischief to Data, Sale of Copyright Infringing Material [20].

There is information about Internet crime on www.antifraudcentre-centreantifraude.ca. If more information is needed or you want to report a crime, you can contact The Canadian Anti- Fraud Centre: info@antifraudcentre.ca [21].

3.1.4. Sweden

Article 143 of the Penal Code of Switzerland (Unauthorized access to data processing system), mentions: Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.

Article 144 (Damage to Data) mentions: Anyone, who without authorization alters, erases, or renders useless data which is stored or transferred by electronic or similar means, shall be punished by imprisonment for a term of up to three years or a fine of up to forty thousand Swiss francs if a complaint is made [22].

The National Coordination of the fight against crime on the Internet (CYCO) is the central point of contact for people wishing to report the existence of suspicious Internet sites or content. After an initial examination and a backup of data, the report forward the information received to the competent criminal prosecution authorities in Switzerland and abroad [23].

3.1.5. Iran

Computer Crimes law was enacted in 2009 with 56 articles and 25 amendments [24]. According to Omidi [25], deputy director of police, the most common computer crimes are: Unauthorized withdrawals from the account, unauthorized access to computer data, Internet Scams and others.

To report a crime, you can refer to courthouse or contact shora@isp.ir. Since 2009, there is a specific section in courthouse to investigate computer crimes. Unfortunately, there is no website to report and investigate computer crimes due to lack of financial support [26]. Adolescents and youth are the most frequent users of the Internet. Educating users about the good and bad consequences of their behavior in cyberspace is very effective in preventing computer crimes.

4. Conclusion

Since computer crimes are growing every day, we must first think of prevention. Perhaps the first step to prevent these crimes is to educate people and then strengthen the security of computer systems. In addition, restrictive legislation can be effective to prevent such crimes. In many western countries, the rules are so strict that these crimes occur less often. Since e-government in Iran has been on the agenda, more laws should be enacted to reduce these crimes. Moreover, we should ensure that these laws are fully and correctly implemented. At the same time, there should be specific references in all cities, not just big cities, to report the crimes. Yet, it is not enough. People should be informed that such places exist, so that they can easily refer to and report the crime. Considering the laws in other countries, such as America, better solutions can be adopted. For instance, computer crimes can be divided into categories and assign experts to each category, so that people's complaints can be easily addressed. As a result, complaints will be more efficiently and quickly handled.

In Iran, there are some places to investigate computer crimes. But they are neither sufficient, nor efficient and the process of investigating the crimes is really time-consuming. Thus, it is needed to implement a website, so that people can report computer crimes without referring to any place.

It is recommended that other researchers do comparative studies about legal authorities to realize the weaknesses of the current system in Iran.

5. References

[1] Gaines. L. K, Miller. R. L. (2008). *Criminal justice in action:The Core* (p. 7).USA: Cengage Learning

[2] Walston-Dunham. B. (2008*). Introduction to law* (p. 499). USA: Cengage Learning

[3] Omoneye Olufunke. (2010). *Computer Crimes and Counter Measures in the Nigerian Banking Sector.* Journal of Internet Banking and Commerce.

[4] Moon. B, McCluskey. J. D, McCluskey. C. P. (2010*). A general theory of crime and computer crime: An empirical test*. Journal of Criminal Justice.

[5] UN, International Journal of criminal policy. p 118. 1998. Office of Legal Affairs, *Computer Crime Laws*.

[6] Martin.C, Hlubik Schell. B. (2004).*Cyber crime: a reference handbook* (p. 2).USA: ABC-CLIO, Inc.

[7] Sen, Osman N. (2001*). Criminal justice responses to emerging computer crime problems*. UNT dijital library. University of North Texas.

[8] The secretary of state for the Home Department. (2010*).Cyber crime strategy*. Presented to Parliament.

[9] Kunz. M, Wilson .P. (2004). Computer *crime and computer fraud*. University of Maryland. Department of Criminology and Criminal Justice.

[10] Littell, J.H., Corcoran J & Pillai,V.(2008).*Systematic reviews and metaanalysis*. New York: Oxford University Press.

[11] Ellen S. Podgor. (2011). Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Accessed from http://www.enotes.com/

[12] Hao. W, Yong. J, Mia Hao. T. (2009). *Analysis of Computer Crime in Singapore using Local English Newspapers*. Singapore Journal of Library & Information Management

[13] Richmond. R. (2010*). Internet Fraud Declined in 2010*. The New York Times. Accessed on 25 Feb 2011, from http://www.nytimes.com

[14] The California Highway Patrol. (2011). *Computer Crime Reporting For State Agencies*. Accessed on 10 Apr 2011, from http://www.chp.ca.gov/programs/computercrime.html

[15] United States Department of Justice. Reporting Computer Hacking. Fraud and Other Internet-Related Crime. Accessed on 2 Apr 2011, from http://www.justice.gov/criminal/cybercrime/reporting.htm

[16] Jianzhuo. X. (2005). *Current situation of cyber crime in China*. Ministry of Public Security of P.R.C

[17] Chinese State Council's Information Office. *The Internet in China*. Accessed from http://www.gov.cn/

[18] Grabosky. P, Broadhurst. R. (2005). *Cyber-Crime:The Challenge in Asia*, Hong Kong: Hong Kong University Press

[19] Casey. E. Dijital. (2004). *evidence and computer crime* (p. 26). UK: Academic Press

[20] Millar Carroll. J. (1996). *Computer security* (p. 38). USA: Butterworth-Heinemann

[21] Antifraud centre. (2011). Canadian Anti-Fraud Centre. Accessed on 20 Mar 2011, from http://www.antifraudcentre-centreantifraude.ca/english/reportit_howtoreportfraud.html

[22] Cybercrimelaw. Switzerland Penal Code. Accessed on 20 Apr 2011, from http://www.cybercrimelaw.net/Switzerland.html

[23] Federal Office of Police. (2006). *Cyber crime*. Accessed on 20 Feb 2011, from http://www.kobik.ch/

[24] Office of Legal Affairs. (2011). *Computer Crime Laws*. Accessed From http://lawoffice.mohme.gov.ir/laws/general_law/laws.jsp

[25] Omidi. M. *Most computer crimes in Iran*. From nicenews.ir. 2011.

[26] Afkhami. B. Judicial Complex 34. *Internet special claims*. From http://www.citna.ir/4467.html. 2010.