European Online Journal of Natural and Social Sciences 2016;
Vol.5, No.3 Special Issue on Humanities and Social Sciences
ISSN 1805-3602

Computer Crime, Strategies and the ways to deal with them

Neda Peykanpour[1*], Fataneh Jalali[2]
[1]Department of Computer Science, Najafabad Branch, Islamic Azad University, Isfahan, Iran;
[2]Faculty of Computer Science, Islamic Azad University, Najafabad Branch
University Sq, Najafabad, Isfahan, Iran
P.O.Box: 85141-43131
[*]E-mail: n.peykanpour@gmail.com

Abstract

In order to use the cyberspace facilities, it is important to provide the security that is one of the rudimentary requirements and essential procedures. Therefore, if the security does not run over the Internet, not only the country but the entire world will be in trouble, as far as the atmosphere is very insecure and unusable. But, providing the security is not one person or organization's obligation but it necessitates an international collaboration among people and the governments. In this paper, we emphasis on a brief review of computer crimes and causes, and then, the solutions and the necessary measures to prevent and impede the occurrence will be discussed. The results show that it is vital for the people and government to fight together to stop cybercrimes and this does not take place without the cooperation of every one of them. Other necessities that need to be emphasized are education and culture among the general public, as many victims perish because of ignorance and lack of knowledge about the ways and means of computer crime. Diverse ways of dealing with these crimes are argued by people and governments.

Keywords: computer crime, Internet, strategies, crime prevention, security

Introduction

Desire to achieve computers and the Internet, and reap the advantages which is growing so fast every day is a universal trend. Although, data processing arranges community association background in the economic process, however, new crime phenomena will get advantage of these favorable conditions to increase the rise of new crimes in cyberspace (Beigi and Khoshyari, 2012). Cyber environment is a secret, free and unlimited place that needs to be organized otherwise each page of this environment can be a crime scene and confusion (Dibaji, 2012). The nature and characteristics of this category of crime somehow differs substantially from traditional crimes. Computer criminals are far from the places where the effects of their actions appear (Beigi and Abdi, 2012). According to the reports, there are now nearly 120 countries that are using Internet in spying and electronic money laundering is increasing significantly, due to the nature of the digital records that is temporary. In consequence of the public nature of newsgroups and online communities and even e-mails, publishing defamatory statements and occurring invasion of privacy will be easier. Internet is the best source of information for both traditional and electronic crimes such as stilling cars or even making electronic bombs; encrypted messages in emails give an opportunity to criminals to send their notes about producing, manufacturing and distributing their drugs simply. People used to produce computer viruses to gain reputation but now they do it to get financial incentive and according to Symantec's latest report, there are over one million computer viruses in the world (Haghgoo Jahromi et al., 2012).

The evolution of computer technology has gone a long way to reach its current form and it is still growing. In the early 50th, US Havan factory built the first generation of computers for the first time. In the 50's and 60's computer software was mostly related to accounting, distribution of goods, besides and accounts maintenance and it was shown very simple and modern.

In the 70's, computer programming developed and software developers were able to design and write software, calculate financial and commercial accounts by mainframes. 70s was the first time Iranian tried to utilize computers, for example, Sanjesh organization used computers for exams, they tried to record candidates' information and they took computers for reports correction and so on.

In the 80s, experts and computer science scholars proposed a new discussion about computer software and electronic payment. In the 90s, computers were the main part of banking systems for doing payments, information exchange, administration and financial matters, even in advanced academic centers and industrial research centers they had the first lead role. 90s was the perfect time for the cybercrime to shine since it was the time that telecommunication computer systems and satellites were vulnerable to vandalism, theft, forgery and changing data in criminals (Karam Ravan, 2012). The first cybercrime was committed by a man named Eldon Royce in 1963, he made changes in the application of the organization's costs and according to that, he sent a percentage of the fund to the specific accounts, however, he was arrested and the court sentenced him to 10 years in prison.

In Iran, talking about computer crimes started in the late 1370s, which was at the same time with public and personal documents forgery. The foremost mass was announced in June 1378 to which a computer science student and a café worker in Kerman, were forged guaranteed cheques (Sheikhloie and Tamjid Tash, 2012). In this paper, after a brief review of the causes of cybercrime, the strategies and the ways of standing and preventing against it will be discussed.

Concepts and basic definitions

Cyber: A prefix used in different cultures in the of term of literal meaning virtual and intangible. In the first time the word cyber was used by William Gibson author of science- fiction book named Neuromancer in 1984 (Majidi et al., 2012).

Computer crime: Any activity that uses computer or other tools, a target or even a place that the criminal activity happens can be in the class and group of the computer crime (Beigi and khoshyari, 2012).

Methodology

Computers and the Internet in the era of communications and technology, are able to quickly spread between homes and agencies. Human can reach a numerous great services in the shadow of this technology, on the other hand, this technology is always open to sabotage, espionage, fraud, etc., in order to verify and prevent that, it is vital to identify crime platforms in cybercrime. In this study, we emphasis on library method and articles written in this field that are used as resources in which the researchers are trying to answer the specific questions:

a. What are the causes of cybercrime?

b. What are the methods of dealing with cybercrime and how we are able to deliver a safe atmosphere in the vital space?

c. Is the government the only place that is in charge to control the cybercrime or it is a public duty?

Requirements for cybercrimes prevention

Preventive measures related to cybercrimes are divided into two sections, one is the aspects and the method of the crime action and the other one is the actions in order to stop and limit the risk of the crime commitment. In this situation, we have to first recognize the crime and then deal with it. It is clear that it is impossible to face with a threat that is not clear how to act with it.

a. Finding the ways of crime: The first step in the battle against cybercrime is to detect gaps and holes that affect the crime.

b. Trying to bound the probability of crime: After understanding the crime factors, measures prevention needs to be taken.

Causes of cybercrime

It is obvious that the awareness about the effective background of the crime supports us to prevent and forbid it. By focusing on diverse kind of crime and getting them together, we can have three general factors that impressively increase the incidence of the crime:

a. The lack of supervision: this helps the wrongdoer to do the crime in different places easily without recognizing to be guilty.

b. The availability of escape: this makes it conceivable for the wrongdoer to disappear quickly from the crime scene after crime occurs.

c. Alienation and anonymity: People cannot diagnose the criminals (Farokhi and Kalantari, 2012).

Strategies and plans to inhibit from cybercrime

Cybercrime is not the problem that only the organizations, institutions or the specific class have to deal with it but facing with it requests a grand cooperation and coordination between the government and the public. In figure 1, strategies and the actions against the cybercrime is shown.

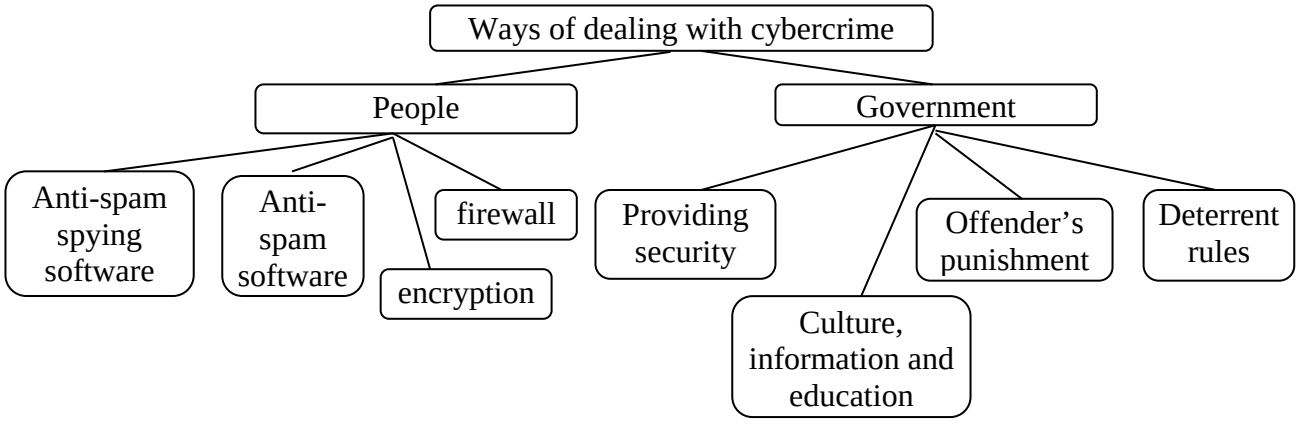

Figure 1: Strategies and measures to deal with cybercrime flowchart

Government duties against the cybercrime

Cybercrime is still expanding in the physical and spiritual aspects caused by misuse of the computer and specially the Internet. The average age of people utilizing the Internet are youth and this raises the possibility that these people might fall into the hand of the criminals or they will be one of them in the future. This problem is a multifaceted phenomenon that influences all aspects of the communities mainly the developing countries such as Iran (Farokhi and Kalantari, 2012). But, the only tactic people can assist the government is by making them aware of the circumstances of these crimes, and training them the ways to deal with it. The government is in charge of codifying the crime deterrent laws, offender's punishment in order to prevent the spread of crime, controlling and providing the security in cyberspace through monitoring circadian activities, filtering, and so on. In addition, they have to focus on culture, information and education through unalike kind of tools and media they have. Education has a magnificent role. The lake of technology awareness and knowledge and the existing different ways of abuse and fraud cause victims falling prey to cyber criminals.

People duties against the cybercrime

Today, due to the technology and science development, people have to communicate with the virtual world to do their daily activities. Considering a few tips will help them to increase security and protection that are: firewalls, encryption, antispam software, anti-spyware software, etc. firewalls, encryption that are the most key items for security and protection will be explained.

Firewall

It is one of the security mechanism to deal with unauthorized access of abuser, digital pests and disclosure of confidential information (Alamolhoda, 2012). In general, the firewall can be summarized in three sentences:

1. It controls input data.

2. It prevents the exchange of dubitable information and it doesn't allow access to the sensitive parts of the operating system or even information.

3. It escorts the output data(Mousavi, 2012).

Encryption

Experts, computer users and the Internet concern about high speed data transfer, taking advantage of the lower cost of data and electronic technology benefits and on the other hand, security and privacy and data communications must inevitably pass through the global communication network. Therefore, the former security practices for the mass media and documents such as sealed envelopes, files and strongboxes are substituted by encryption security technology (Mousavi, 2012). Changing the primary data to the incomprehensive information is called encryption. There are different cryptography techniques such as private key encryption, public cryptography and digital signature and they implement diverse security services like authentication services, access control services, non-repudiation services and data integrity service. Security in the stored information and transition is the most important encryption purpose that desires to be done (Alamolhoda, 2012).

Repairing damages and restoring the system to its original condition

So far, we discussed about the activities in order to prevent cyber-attacks. But, the steps mentioned below are the necessary actions if the cyber-attacks occur with the intention of repairing the damages of the system.

- Destroying any kind of malware that remains in the system.
- Replacing or abandon the vulnerable parts.
- Reconfiguring and apply patches for the equipment or software.
- Reconfiguring the accesses.
- Updating network security (Fakhori Tabrizi and Fakhori Tanrizi, 2012).

Conclusion

We are living through the particular era in human history that the boundaries of science and technology are intertwined that life without it is very tough. Computer science and the Internet, which creates a space called the global village, is one of those inventions that infiltrated to human life and even houses very fast, even today, children under seven years are using it simply. Many valuable services such as e-banking, e-commerce and scientific activities are based on them. But this beneficial environment has always been disposable to threats and sabotage. Security in cyberspace is one of the basic requirements and necessary usages of its facilities, so that if the security is not provided by the person and the country not only them but the whole world will be in anxiety, as far as the atmosphere will be very unsafe and unusable. Offering the security is not only the person or the government's duty but it is required to have an international collaboration between them to

stablish the security. Since these sorts of crime commitments are not affected by geographic boundaries, each offender anywhere in the world can apply to this criminal acts. Therefore, without having a global cooperation between the countries, it is very difficult and sometimes impossible to track and punish the guilty person. As a result, it is important to have some safety tips to create difficulties for the crime. Governments have to codify to punish the criminals and monitor all the activities through security devices, in addition, they have to educate the public to obey the security principles and so forth. Many computer crimes occurred in the lack of safety awareness, carelessness and transpired in the shadow of citizens that are not observing the security issues. As a result, it is desired that people use the facilities like firewalls, encryption, digital signature, anti-spy software and software against spam emails to stop crimes and make complications for the offenders.

References

Alamolhoda, H. (2012). The impact of cybercrimes on e-commerce. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Beige, J. & Abdi. R. (2012). Situational prevention of computer crimes and the challenges against it. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Beige, J. & Khoshyari, R. (2012). Computer crime and dealing with it in international documents. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Dibaji, S. (2012). Insulation in cybercrime. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Fakhori Tabrizi, B. & Fakhori Tabrizi, A. (2012). Industrial control systems protection against cyber-attacks. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Farokhi, M. & Kalantari, M. (2012). Electronic city and Strategies to control and reduce cybercrime. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Haghgoo Jahromi, V., Nouri Motlagh, M. &Hoshyar, A. (2012). Electronic crimes and the challenges of enforcement in the community. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Karam Ravan, F. (2012). Cybercrimes and their preliminary investigation. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Majidi, A. Jahanbakhsh, N. & Mahdavi, Behzad. (2012). Security in information exchange space. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Mousavi,R. (2012). Situational prevention of cybercrime in the form of technical measures and limitations against it. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.

Sheikhloie, H. & Tamjid Tash, S. (2012). Today and the future of cybercrime. Regional conference on the challenges of cybercrimes in this decade. Islamic Azad University of Maragheh.