University College of Takestan

Available online at **http://UCTjournals.com**

Iranian Journal of Social Sciences and Humanities Research

UCT . J. Soc. Scien. Human. Resear.(UJSSHR)

38-41 (2015)

Volume 3,Issue3

ISSN:2382-9753

Electronic theft and reduce its impact on the bank's security

Abolfazl Azizi[1] and Alireza Millanei[2]

1Department of Law, Electronic Branch, Islamic Azad University, Tehran, Iran
2Department of Law, Islamshahr Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Information technology affected all aspects of social, economic, cultural and deeply, including criminal law. Any change in today's world because of the complexity of human activities will have consequences. There is always the possibility of abusing in such a way of invention of new tools, as well as correct and legitimate use.

Cyberspace, the result of scientific and industrial progress in recent centuries is not an exception to the positive and negative effects on human life and the most important works was the emergence of cybercrimes. Computer crime of unauthorized use of computer technology to seize sensitive personal data and confidential information also applies to organizations. Advances in computer technology made it possible to create a new crime to forge compared to traditional methods, are much more technical.

Although most electronic thieves are doing it to show off, but the theft is done for the purpose of access to information of the banks, has created a major problem. The purpose of this study was to investigate the electronic theft and its impact on the bank's security. In this study, using documents and legal opinions and legal analysis of the data obtained will be discussed. It is optimized for the opinions of respected professors were used.

As we know, in the traditional banking as well as those with some threats faced these threats on electronic systems for others. To provide and enhance the security of electronic banking and the banks should reduce threats, while respecting security policies, including privacy, authenticity, integrity and ... Of security tools such as encryption, user code and password, digital certificates, digital signatures, software and security protocols to be used.

Original Article:

Received 12 Aug. 2015
Accepted 25 Sep. 2015
Published 30 Sep. 2015

Keywords:
electronic theft, bank data, bank security

Introduction

Introduction

Information technology, affected all aspects of social, economic, cultural, including criminal law deeply. Any change in today's world because of the complexity of human activities, and works inevitably will have consequences. In such a way, the invention of new tools, as well as correct and legitimate use of it, there is always the possibility of abuse.

Cyberspace, the result of scientific and industrial progress in recent centuries, is not an exception to the positive and negative effects on human life, which is the most important work has been the emergence of cybercrimes. Computer crime of unauthorized use of computer technology to seize sensitive personal data and confidential information also applies to organizations.

These legal and policy-related developments have forced to pause. In this regard the law as a supporter of justice and creating harmony in human society, whatever that cause the slightest damage to the balance, covered and try to fix it or prevent its adverse effects. For this purpose in this article, theft of a computer crime and security features and its impact on banks to is investigated.

Problem statement

One of the unavoidable realities of today's world is the Internet and, consequently, the electronic interactions and the Internet. Due to the very high computing capabilities such as high accuracy, high speed, high volume data storage, tirelessly, rapid exchange of information, easy access and countless other advantages, has brought great opportunities for man, one of the largest of which is the creation of a global village or transnational phenomenon. Despite all the useful applications that the Internet has brought, shattering the negative effects of the economic and social fields has brought.

Including crimes that may occur in the information and data can be things such as theft, fraud, embezzlement, Anthab and Astlab noted. Theft crime is oldest crimes against property in human societies. Nowadays with advances achieved in the field of technology and the emergence of electronic devices such as computers and the Internet, the exchange of goods and objects and keep them from traditional to electronic means has been turnover.

Electronic theft of this nature is an adult user, wise, knowledgeable and autonomy without the use of computer technology and telecommunications, is locked in a virtual environment web site or a file that is owned by the other, by enforcing password or files on the break and worth a quarter of a dinar, the data that has financial value, cut and use it.

Computer Crimes Act in article 12-store robbery and states: "Everyone is illegal to steal data belonging to another, if the same data is available to its owner, to a fine of one million (1,000,000), rials twenty million (20,000,000) rials and otherwise the imprisonment of ninety-one days to one year

or a fine of five million (5,000,000), rials twenty million (20,000,000) rials or both will be punished."

In Iran particular the 2001 Law on combating and dealing with computer crimes are special and specific and legislator a little late to the law, certain computer crimes and cybercrime to take action, and this legislation is now the basis for punishing the cyber criminals.

A short time commit robbery, burglary, electronic and spatial extent of physical contact made with stolen property, according to a method commit theft, among the features of electronic theft.

According to before description, the electronic theft, the thief can get past the fire wall and security of electronic banking portals and by entering the password bank account a large amount of money from their account or accounts by other people to move. In this case the economic security of people affected feel the bank is lost? Do you still be willing to invest in banks?

On the other hand, theft of a different nature from ordinary theft is done in banks. So the question arises whether electronic theft is the theft of common legal? What the fulfillment of the conditions like? Is the reward of up password and break the lock, the case of violation of privacy?

Nowadays we are seeing new varieties electronic theft. Therefore, it is necessary to be transparent, electronic theft of known and unknown nature of the offense. Because without knowing the electronic theft and its variants, is not a suitable solution, valid for this type of crime was fighting and fighting. Hence purpose of this study is to explain the nature of the juridical and legal theft crime and theft e-mail, try to answer the questions come and the impact of this type of theft are reduced banking security law.

The importance and necessity

Advances in computer technology made it possible to create a new crime compared to traditional methods, are much more technical. Although most electronic thieves to show off this work they do, but the theft for the purpose of access to information are the banks, has created a major problem*. The biggest example of block internet is access to bank accounts for customers who have access to some Web sites known to impossible.

Banks to deal with the complex problems of the technology used to prevent unauthorized access to your financial information banks, and by identifying new risks, their systems continuously provide timely and updated. Obviously, the banks should be in close contact with law enforcement authorities to protect the country's financial infrastructure.

Electronic theft of such crimes is to explain the legal-criminal aspects of it, the nature and manner of its formation deserves to be examined thoroughly and carefully to punish the perpetrators, not to extremes and finally the objectives of the legislator was not far away. The necessity of this is in addition to legal compliance issues and legal issues, caused legislative consideration the importance of this issue and trying to prevent this type of crime in order to improve banking security are important effects. Perhaps with electronic occurring in the bank theft, security undermined banks and trust banks are depositing your funds to be withdrawn.

C. research history

Hazraty Shahindej (2010) studied the legal nature of the legal and electronic theft. In this study it was stated that the use of computers to commit theft is possible in different ways. If a computer is used as a means to commit a crime, its constituent elements, the elements of theft is common with its own characteristics due to the wide range of possible victims, as well as ease of the crime is concerned.

In this crime, criminal, recipes, information and computer data puts the main purpose of committing a crime. After this information thieves can use them to open accounts in the name of the victim and abuse, withdrawal from bank accounts, take advantage of online services and online or obtain financial benefits such as loan use.

Property characteristics of computer systems, as well as the work of criminals and perpetrators of crime are easy to commit successful work for the restitution of property of victims or accused tracing difficult. Especially in cases where theft is carried out in another country, in this case, access to him and for compensation to be hardly possible. †

Masjed Saraei and Taghavi (2012) studied "The concept and nature of the amulet with an approach to Internet piracy,". In this study, it was suggested that in the case of computer crimes listed several definitions, but in the context of Iranian law not the law of e-commerce and the cybercrime law does not provide a definition of this concept.

One of the areas of major crimes is cyber theft. In all religions and communities, theft was illegal and severe punishment. Theft such as other crimes related to the evolution and development of human societies evolved from primitive and simple to very complex way accordingly.

The nature of computer crime has become a complicated matter in this study considered the implications of theft and amulet and then the amulet in the context of cybercrime were evaluated according to the definitions and may or violation of some amulet on the Internet were discussed.‡

Mousavi Boroujerdi and Bani Hashim (2012) studied "legal review of computer theft (VoIP) with an emphasis on Imam Khomeini". In this study legal opinion addressed to the crime after criminal act described to compare it and theft part and concluded, despite the fact that the mutilation of security in terms of deterrence, can be a good idea to punish thieves; but since in many cases there are doubts in this type of theft cannot be far from the norm about these criminals be current. §

Izadifard and Pirdehi Hajikala (2010) studied "cyber theft" While explaining the nature of cyber theft, was sentenced finally, this type of theft. The only reason for mandatory

* McLean, Jean, 1380, a new era of banking security in today's highly technical world, the fight against crime banking, numerous fronts, translation Kamran Sepehri, the banks and the economy, (18), Ss29-31

Hazrati Shahindej, Samad., 1391, jurisprudence and legal nature of electronic theft, Association Journal, No. 128, Ss75-94

Anonymous, 1382, cybercrime and theft from banks, the banks and the economy, (43), Ss48-51

† Hazrati, Shahin Dez, Samad, 2012, Juridical Nature Of Electronic Theft, Focal Journal, No. 128, Page 75-94

‡ Sajd saraei, hamid, taghavi, seyed abbas, 2012, nature of internet theft, seman journal, third year, no. 7, page 43-54

§ Mosavi bojnordi, seyed mohammad, banihashem, maryan, 2012, juridical study of internet theft with imam khomein approach, matin journal,no 1, no. 60, page 29-40

knowledge of cyber theft is failure to fulfill one of the conditions for obtaining the physical theft and providing new ways and new security user's punishment.

After theft the store and match it with theft some nature, this turns out that both the definition of cyber theft and the theft condition is expected, according to the same physical coach getting stolen in the theft but the extent and in the outside world, but in the discovery of cyber theft and other data at its disposal to put them through the electrons in cyberspace.

Hence, the implementation of the theft the problems facing the prison sentence as punishment appropriate user security can be raised. The purpose of this study was to investigate theft of mail and its impact on banks.

Methods and tools to analyze the data:

Using documents and legal opinions and legal analysis of the data obtained will be discussed. It is optimized for the opinions of professors will be used.

First Speech: Privacy Policy and Security

In general, the privacy protection of personal information and the exact dates, Clark privacy as the right to privacy only with regard to different aspects of the body, behavior, communication and defines personal data. As far as the Internet is concerned, the privacy aspects such as the acquisition, distribution or unauthorized use of personal information affects, the growing capacity of new technology for the processing of information as well as its complexity, privacy has become a very important issue.

The fact that personal data are collected and how the Exchange store how to come on stream, can enhance customer confidence and, consequently, as a major obstacle to be placed on the development of e-commerce, which is mainly the lack of user control over the use of personal data supplied by the vendors.

In addition to the problems that arise due to the lack Privacy Policy, lack of security which is viewed by consumers is one of the main obstacles to the development of electronic commerce. In the field of Internet, security returned to observations in relation to the means of payment security mechanism to store and transfer data.

So, what we are here talking about it, the technical aspects of the integrity, reliability, validity and other aspects of diagnostic relations is reassuring in a nutshell, this entry expressed the Privacy Policy, to a set of legal requirements and practices regarding the use of private data points. As security, the technical guarantees for the effective fulfillment of these legal requirements and practices regarding privacy are reassuring.

But these two variables are related to each other and clearly in three distinct areas should be focused on this issue in the minds of consumers, there is a close relationship between the two of them together and usually they are wrong. Organizations also tend to apply both concepts jointly. Public institutions also consider both concepts to run together. Thus, the actions of regulators, including batch-type process measures (e.g., collect and use and transfer of personal data) and those who are generally technical type.

Therefore, it seems fair to say that the properties of variables privacy and security should be applied as distinct concepts, but as we see, not only consumers, but also organizations and legislators have found that these two concepts are closely related to each other. This fact suggests that these variables must be the size of a projection. (Construction)

This plan called security observed in working with private data and consumer understanding of the ways show that was about the protection of private data by financial services and information systems.

Second speech: Electronic banking security

Similar to many electronic review that information security is primarily for business customers cite the importance of this issue (as well as the reliability of the processing of personal data) By users and potential users with regard to the security and privacy of Internet banking transactions challenged.

There is a close relationship between e-commerce and internet banking, internet banking, which is meant to limit the duration of the implementation of the security requirements that must be listed below, are met:

1. Identify and authenticate the user's unique ability to determine the identity of a person or it proved
2. to possess: the ability to control the actions of a person's identity based on characteristics
3. Reliability: the ability to prevent unauthorized groups in the interpretation or understanding of data
4. Integration: the ability to ensure that data on accidentally or by unauthorized groups will not change.
5. Undeniable: the ability to prevent denial or denied actions by a person or entity
6. Availability: ability to provide uninterrupted service
7. Privacy: the ability to prevent illegal or unethical per use of information or data
8. Ability to handle: the ability to maintain an accurate record of all transactions for the next eight goals of security requirements, as a basis for the security of electronic commerce have continued, user authentication mechanisms must also provide the cornerstone of authentication for Internet banking framework considered and this entry includes the use of smart cards and biometrics is perhaps science. (Faculty of Biomedical Engineering to identify humans)[**]

Second topic: general security requirements for a banking environment

First speech: electronic payment system

Payment is main part of trade. There was no deal without full payment. Nowadays with the development of e-commerce needs to be appropriate electronic payment methods is strongly recommended. Payment system is a set of complex procedures, institutions and mechanisms that lead to the transfer of money and funds. In other words, payment of the sum of the funds from one account to another account in a bank in another bank transfer.

The electronic payment is transfer electronic value from the payer to the payee's payment through electronic payment mechanisms. Electronic payment service that enables customers to remotely manage their accounts and transactions have access to them, in general, there are three methods of electronic payment:

Electronic cash, electronic check and electronic cards (credit cards, debit cards and prepaid card) Security means freedom from danger or fear and protect against threats that cause

[**] Abed, rasoul (2012), regulation for difference of crimes in the material of crim, journal of education message, no. 54

financial damage and injuries or network resources in the form of destruction, disclosure, alteration and destruction. Information security is a process through which the organization of systems, equipment and networks, including the protection of vital information, is safe and secure electronic transactions depends on these factors.

- Systemic factors: technical infrastructure;
- Transactional factors: Secure payment according to defined rules;
- Legal factors: legal framework ††

Second speech: confidence in electronic payment systems

Trust means the willingness to rely on an exchange partner confidence. According to social exchange theory of relationships based on trust form the exchange and may cost more than the value of the exchange and the potential benefits are to be avoided. On the Internet customers generally because of the distance, virtual identity and the lack of regulation, higher risks compared to traditional feel of traditional media.

Trust sub-structures rely such as secure electronic payment, usually on the interface or a third party on behalf of both well-known and reliable. Vendors or suppliers to ensure customers' trust must be higher than procedural and technological tools to make them. Procedure means a set of steps that the consumer is required for something that will make them travel.‡‡

Conclusion:

As we know, in the traditional banking as well as those with some threats faced these threats on electronic systems for others. Banks, to ensure and enhance the security of electronic banking and reducing threats while respecting security policies should like confidentiality, authenticity, integrity and ... Of security tools such as encryption, user code and password, digital certificates, digital signatures, software and security protocols to be used.

Reference

Abed, rasoul (2012), regulation for difference of crimes in the material of crim, journal of education message, no. 54

Abed, Rasoul, (2012), the criterion for applying this rule, a plurality of different crimes, crime, education, the judiciary monthly messages Department of Education, Issue 54

Anonymous, 1382, cybercrime and theft from banks, the banks and the economy, (43), Ss48-51

Fariborzi, Elham, (2011), the evolution of cybercrime laws in Iran, Journal of jurisprudence and the history of civilization, the seventh year, No. 27

Hazrati Shahindej, Samad., 1391, jurisprudence and legal nature of electronic theft, Association Journal, No. 128, Ss75-94

Hazrati, Shahin Dez, Samad, 2012, Juridical Nature Of Electronic Theft, Focal Journal, No. 128, Page 75-94

McLean, Jean, 1380, a new era of banking security in today's highly technical world, the fight against crime banking, numerous fronts, translation Kamran Sepehri, the banks and the economy, (18), Ss29-31

Mosavi bojnordi, seyed mohammad, banihashem, maryan, 2012, juridical study of internet theft with imam khomein approach, matin journal,no 1, no. 60, page 29-40

Norian, Ali Reza, 2012, FATA, police specialized professional or a trusted ?, week, the security forces of the Islamic Republic of Iran, (23)

Sajd saraei, hamid, taghavi, seyed abbas, 2012, nature of internet theft, seman journal, third year, no. 7, page 43-54

†† Abed, Rasoul, (2012), the criterion for applying this rule, a plurality of different crimes, crime, education, the judiciary monthly messages Department of Education, Issue 54
Fariborzi, Elham, (2011), the evolution of cybercrime laws in Iran, Journal of jurisprudence and the history of civilization, the seventh year, No. 27

‡‡ Norian, Ali Reza, 2012, FATA, police specialized professional or a trusted ?, week, the security forces of the Islamic Republic of Iran, (23)