# Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (12): 1558-1565, 2007
ISSN 1812-5654


# Computer Crime and the Law from an Islamic Point of View

Mansoor Al-A'ali
Department of Computer Science, College of IT, University of Bahrain, P.O. Box 32038, Bahrain

**Abstract:** Information technology is facing waves of laws guarding the interest of people using the Web technology. These laws were derived from the common laws and legislations applied in general crimes. One of these laws is the law of the state is Texas in the United States in 1985. In a world which has more than one billion Muslims, it is time to consider proposing a law that is in line with their teachings. Several calls were also raised in the Islamic countries to establish a law suitable to handle computer crimes which matches the Islamic Shar'iah law. The main question to ask here is how can the Islamic law which was established in the seventh century handle crimes resulting from the use or abuse of the new technology and provide suitable laws for the protection of its computer users. To answer this question our research has analyzed the Adellah (الأدلة) (Shar'iah Evidences of Quraan, Hadith and Imams sayings) that match Texas computer crime law items to verify the outlook of Islam in computer crime. We set out to prove that computer crime with its high technology is not entirely a new type of crime that needs a new Islamic theory and thus is already covered by the general Islamic Shar'iah laws. Based on the available computer crime laws and our understanding of the Quranic verses, we propose to tackle this very difficult area by proposing a computer crime law from an Islamic point of view. We believe this research is the first of its kind and will open the discussion in this important area with the exception of one study which addresses the e-commerce from an Islamic view point.

**Key words:** Computer crime, computer crime law, texas law, Islamic law

## INTRODUCTION

With the spectacular growth of high-technology industry, computers and communication have become the backbone of our new life style. Consequently, computers have created a host of potentially new misuses and the computer-related crime has become a growing phenomenon that involves traditional criminal activities such as theft, fraud, forgery and mischief. In spite of the difficulties to determine when the first crime involving a computer actually occurred, in early 1974, David Stryker, John Shore and Stanley Wilson of the United States Naval Research Laboratory subverted operating system of a Univac 1108 computer using security violating Trojan horse techniques to obtain unauthorized and surreptitious access to classified information. US government figures show that money made by criminals through cyber crime now exceeds that from drugs and narcotics. Some reports claim that the cyber crime market is worth up to $1.6tr a year (Little, 2006; Zainul *et al*., 2004; Abu Bakar, 2003).

Computer security represents a growing concern for societies and organizations. A number of reports researchers have addressed the computer crime threat (ISO BS17799, 2005; Willson, 2006). However, there has been a lack of focus given to the relationship between the human behavior of offenders during the perpetration of computer crime and other relevant issues such as social and religious upbringing and behavior. Yet insights into this relationship could feasibly be used to address such dangerous risks. The goal would be to understand the offender behavior and look into other ways of bringing to the attention of the individual other benefits and punishments which are not necessarily related to man made criminal laws. Hence the computer security strategy should aim to support the criminal act through the implementation of safeguards which influence the offender's inclinations and wider fears (Al-A'ali, 2006).

Organizations can currently draw on a number of means for computer crime guidance. These include the use of risk assessment techniques (Peltier, 2004), international standards, such as ISO BS17799 (ISO BS17799, 2005), or the baseline security approach (Parker, 1998; Willison, 2006; Willison and Backhouse, 2006), where controls are selected based on best practice principles. However, the major question will always remain, is it enough to have standards and crime laws to prevent or reduce crime? Clearly unless we address the human behavior itself and appeal to the individual with other forces of control which should on the whole be self imposed, we shall continue to have computer crime.

We can define computer crime generally as a crime accomplished through special knowledge of computer technology. The law has been too slow to understand and react to the rapid changes in technology. We have recently witnessed that previous laws are unable to handle these crimes. The first comprehensive proposal for computer crime legislation was a federal Bill introduced in the US Congress by Senator Ribikoff in 1977 (Schjolberg, 2003). The Bill was not adopted, but this pioneer proposal created awareness all around the world.

A number of western nations have long started their assessments of existing laws for their suitability or adaptability to computer crimes. The legislature of Texas-as example-passed the computer crime law in 1985. A great number of specialists in different law fields, information technology, politics and economics have participated to prepare this law and it has been modified several times during a short time. This law shows the efforts spent to achieve the law to win the battle of this growing threat. In a study by Bloombecker (1995), computer fraud, law, procedures and punishment in the USA is outlined in chart format showing the definitions, prohibitions, procedures and punishments of computer crime laws in the USA.

The question is: Do these laws work actively and do they provide the right punishment to fit the crime? The evidences show that the risk of a computer crime remains high and that despite deploying an enviable range of security technologies and new laws, people and organizations still fall victim to attacks that resulted in significant financial loss (CSI/FBI Survey, 2003). The Australian survey also shows that the total losses for 2003 are more than double quantified losses in 2002 (AUSCERT, 2002).

In the last two decades, the information technology has been reshaping how the world communicated and received information. Evidence of the eagerness on the part of some Muslims to embrace such technology, has been the proliferation of Islamic sites on the Internet, some of which are devoted to Islamic education and propagation, while others being of a more commercial or entertainment nature (Yousif, 2002).

One out of every four persons on the planet is a Muslim (Hassan, 1990) and for those who believe in perfecting justice through the Islamic law, it is very important to develop the Islamic outlook to computer crime especially since we know that most Islamic countries place it at the center of their legal codes like Saudi Arabia, Sudan and Iran (Crystal, 2001). Facts decide the importance of the Islamic law to minimize computer crimes, by providing a worldly punishment as well as that in the hereafter (Afifi, 2003). Researchers proved that computer crimes with high technology like money theft, information theft, or betrayal are not new. Computer crimes need a new Islamic theory (Ahmad, 2001).

Modern scholars have made advancement on several definitions for the concept of rights in various perspectives. Some of the definitions, viewed rights from the Islamic laws, while others tend to emphasize the concept of interest avoid. To avoid engaging in technicalities to overlap, a resaercher (Mohammed, 1994), made a conclusion to define rights as an exclusive appropriation or power over something, or demand addressed to another party, which the Islamic laws has validated in order to realize a certain benefit.

The questions are: What is the basis of the Islamic law for computer crime? When and where the Islamic law was established? How would the Islamic law that was established in the seventh century handle the new technology issues and provide a suitable law for computer crimes? How would the Islamic law compare with the western laws like Texas computer crime law? This research attempts to answer these questions in order to establish an introduction of the computer crime Islamic law and to prove that an Islamic computer crime law can contribute to the well being of humanity in parallel with the western law.

Before we start to propose a new Islamic computer crime law, we must describe the basic principles of the Islamic law in general. We will then compare the new Islamic computer crime law with the Texas computer crime law. Then we will survey the Quaranic verses and Prophet Mohammad sayings to find and analyze the Islamic evidences that can be related to computer crimes in Texas computer crime law. Present final objective is to propose the Islamic computer crime law.

Islamic law originated with the birth of Islam in the seventh century with the coming of Prophet Mohammad (Pbuhwa), as a common law. Islamic law is known as Shar'iah Law and Shar'iah means the path to follow God's Law. Shar'iah Law is holistic or eclectic in its approach to guide the individuals in most daily matters. Shar'iah Law controls, rules and regulates all public and private behavior (Denis *et al*., 1994; Mancuso, 2007). The theoretical assumption of the Islamic Law is to protect the five important indispensables in Islam: Religion, Life, Intellect, Offspring and Property. Islamic Law has provided a worldly punishment in addition to that in the hereafter (Madkoar, 1980). Islam has, in fact, adopted two courses for the preservation of these five indispensables:

- Through cultivating religious consciousness in the human soul and the awakening of human awareness through moral education.
- By inflicting deterrent punishment, which is the basis of the Islamic criminal system. Therefore, the limits or Hudud and retaliation (Qisas) and Discretionary (T'azir) punishments have been prescribed according to the type of the crime committed.

In this research we address the major issues of human behavior in relation to Islamic religion and computer crime. This research presents a new computer crime law based on Islam. To present knowledge, there is no Islamic Computer Crime law till now and hence our proposed new Islamic Computer Crime law is the first. We, evaluate the leading computer crime law which is the Texas Computer Crime law in relation to our newly proposed Islamic Computer Crime law. The Texas Computer Crime law and other existing similar laws are conclusive and pioneering by all accounts, but, it is our belief that they actually do not trigger the emotions of Muslims and hence can only be applied in the court of law. It is our belief that once a crime is in the court of law then the damage had been done and the court will keep busy with a constant stream of a wide variety of cases if they are discovered. If we appeal to the Muslim before he/she commits the crime and put the issue of computer crime in perspective, then we are more likely to succeed in stopping crime.

## TEXAS COMPUTER CRIME LAW

We have selected the Texas computer crime law because it was the first of its kind in the world. The aim of this research is not to make a survey of western computer crime laws, but rather to argue for the benefits of proposing a new computer crime law based on Islamic values and beliefs. The Texas computer crime law serves as a good comparison platform with our proposed Islamic computer crime law. The full Texas Computer Crime law is given in the Appendix 1 for easy reference. Section 33.02. in Texas computer crime law defines the breach of computer security in four points (Texas Computer Crime Law, 1994):

- A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
- A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.
- An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:
  - A state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or
  - A felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.
- A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

## SELECTED SHAR'IAH EVIDENCES RELATED TO COMPUTER CRIME

In Islam, the basis of law is the Quraan (Islam Holy Book) and Hadith (Prophet sayings). In this section we have collected and presented the Adellah (Shar'iah Evidences) of Quraan and Hadith which relate to the three points of the breach of the computer security in relation to the Texas computer crime law. We use the Quraan translation by F. Malik. Here we have simply collected a few of the Quranic versis from the wholly Quran and a few of the Prophet sayings in preparation for the next sections.

- A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

This section dedicates the importance of privacy. The computer hardware or software is a property of someone. Access would be unauthorized if an offender:

- Is not himself entitled to control access of the kind in question to the program or data.
- Does not have consent to access the program or data from a person who is so entitled.

**Allah (God) said:** O believers! Do not enter houses other than your own until you have sought permission and greeted their inmates(Ayah, An-nur, 27). In this Ayah,

Allah decides: If you wanted to enter a house other than your own ask the owners permission beforehand. So from the Islamic principles you can not access the properties of others without their permission, this is the Islamic approach to the rights of privacy.

**Allah said:** O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, Do not spy on one another (Al-Hujurat, 12). In this Ayah, Allah command: Do not spy on one another. Therefore, from the Islamic principles you can not spy on the secrets of others including those hidden or stored inside computers despite your suspicion.

**Prophet Mohammad (peace be upon him) said:** It is better for a Muslim to mind his own business (Al-Muatta, 1604). In this Hadith, the Prophet tells us that we are good Muslims if we leave other peoples' business alone. Therefore, from the Islamic principles you can not allow your curiosity on other peoples' business to delve in their property including the information in their computers.

**Prophet Mohammad (peace be upon him) said:** Permission is for having a look (Al-Bukhari, 5887). In this Hadith, the Prophet tells us that the main aim of permission is for having a look. Therefore, from the Islamic principles you can not have a look inside other persons properties if they did not allow you and the computer is a property.

- A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data. This section dedicates the importance of trust. The computer system password, identifying code, personal identification number, debit card number, bank account number, or information that may be given on trust. To give any confidential information to another person without effective permission is a betrayal of trust.

**Allah said:** Allah commands you to give back the trusts to their rightful owners (An-nessa, 58). In this Ayah, Allah commands: give back all the trusts to their owners. Therefore, from the Islamic principles you can not access other persons properties without their permission. This is the Islamic approach to privacy right.

**Allah said:** O believers! Do not betray the trust of Allah and His Prophet, nor violate your trusts knowingly (Al-Anfal, 27). In this Ayah, ALLAH commands: Do not betray the trust. The security information given to other people without a permission is a betrayal.

**Prophet Mohammad (peace be upon him) said:** The signs of a hypocrite are three: Whenever he speaks, he tells a lie. Whenever he promises, he always breaks his promise. If you trust him, he proves to be dishonest. If you keep something as a trust with him, he will not return it (Al-Bukhari, 1010).

**Prophet Mohammad (peace be upon him) said:** Give back what you have been trusted with and do not betray those who have betrayed you (Al-Hakeem, 1990).

**Allah said:** O believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent (An-nessa, 24).

**Allah said:** Male or female, whoever is guilty of theft, cut off their hand (that was used in theft) of either of them as a punishment for their crime. This is exemplary punishment ordained by Allah (Al-Maaeda, 38).

**Prophet Mohammad (peace be upon him) said:** It's prohibited to take the Muslim wealth without his complete permission (Al-Baihaqi, 11325).

## ISLAMIC COMPUTER CRIME LAW PROPOSAL

Here, we have put together a proposal for an Islamic computer crime law which we hope will initiate further future research by computer security specialists, law makers and theologians alike. It is an arguable discussion whether to call this a computer crime law or a computer crime ethics law; it is our belief that the latter applies more since the aim is to work on the human being to stop him or her from committing the crime rather than handing out the punishment. There is no disagreement that punishment can be a deterrent but prisons are never and will never be empty. Our proposed computer crime law is more of prevention rather than a cure for many in society in general rather than a deterrent to an isolated individual.

**Privacy:**

"الـمـاجعل الاِستئذ ان لاَجل النظر". لا يصح الاِقراب (مادىَ أو اِفتراضيا) مـن اَجهزة الكمبيوتر اَو ملحقاتها للتطفل اَو محاولة النظر اِلى مهتو يتها اِلا بعد الحصول على اِذن صريح من مالكها مع مراعاة حدود ذلك الاذن.

A person should have a permission before having a look. It is prohibited for any person to come (physically or logically) near to any of computers or their accessories for curiosity or to look at their contents without a prior permission of the owner and he should be aware of the limit of the given permission.

This item presents issues which are related to the fundamental nature of the human being. The item states that even having a look can only be done after gaining permission and this puts a stop to many attempts to invade any kind of information privacy. The restriction is placed on a person not to come even close to a computer or its accessories physically or logically without permission and even if such permission is granted then one has to make sure that he/she is aware of the limitations of this permission. This item supersedes the Texas law for example, which concentrates on a person committing harm or damage rather than just having a look.

**Trust:**

"اد الاَ مـانة اِلى مـن اتـمـنـك ولاتخن من خنك". فلا يجوز لمن هصل عـلـى مـعـلـومـات سـرية اَوشيـفرات تتيح الدخول اِلى انظمة كمبيوتر اَن يسـربهـا عـمداً لاي شخص كان اِلا بعد الحصول عليالاِذنالصريح بذلك مـنـالـمـالـك. وليـعتبـر اِلاخلال بذلك خيانة للامانة، ويستوي في ذلك المسلمون و غيرهم.

A person should be trust worthy even with a betrayer. Any person who receives some confidential information or a password to access a computer should not give them deliberately to any person without a prior permission from the owner. Muslims and none-Muslims are equal to be trust worthy.

It is interesting here that this item states that one cannot betray someone else who had betrayed them beforehand. Further, this item states that Muslims and none-Muslims are equal in trust worthiness.

**Theft:**

"يـحـرم اكـل امول الناس بالباطل". فلا يجوز محولة الاِستفادة المادية من مـحـتـويات الكمبيوتر او من خلاله اِلابإذن صاحبه، وأيِ انتهاك لهذا المنع يعتبر سرقة محرمة.

It is prohibited to get other persons properties illegally. It is not permitted to get benefits of the contents of a computer or through it without permission. Any action like this is considered a theft.

This item focuses on two main issues. The first is that other persons property is prohibited. This means that we do not have to make numerous legislations stating what is legal, rather, what is not yours is illegal to you. The second point is that the contents of a computer are illegal and this covers software, hardware, ideas, methods, etc. This places restrictions on gaining any kind of benefit from someone elses computer no matter what form it is stored in.

**Promise:**

"الـمسـلـمـون عـلـى شـروطهم". وهـذه الانـظمة تحـرم اِلاعتداء على كـمبيـوترات الاَخرين اَو اِستعمالها اَو اَخذ مافيهما من بر امج او معلومات ذات قيمة بدون ، و يستوي في ذلك المسلمون و غيرهم

Muslims should respect their terms. This condition states that it is prohibited to use other person's computers or get what is recorded on them of worthy programs or information without a prior permission. Muslims and none-Muslims are equal at that condition

This item re-emphasizes the previous point in that all kinds of contents inside a computer is prohibited no matter who is the owner of this computer.

## COMPARISON BETWEEN ISLAMIC COMPUTER CRIME LAW AND TEXAS COMPUTER CRIME LAW

To define the difference between the Islamic computer crime law and Texas computer crime law, we show the relation between both laws in next Table 1.

## CONCLUSION

The international community is facing and will increasingly continue to face crimes committed with the use of computer technology. Although advanced computer crime laws exist in the advanced nations today, but for the one billion Muslims, it is questionable whether these laws will have real effect. We argued the case for a proposed computer crime law based on Islam which addresses the individual before the crime is committed and hence is more of prevention than cure. The paper presented the proposed law and its analysis with the argument that the leading Texas computer crime law can be rewritten with Islamic flavor and would appeal to Muslims more.

Table 1: Comparison between Islamic computer crime law and Texas computer crime law

| Islamic computer crime law proposal | Texas computer crime law | Comparing |
|---|---|---|
| A person should have a permission before having a look It is prohibited to any person to come (physically or logically) near to any of the computers or its accessories for curiosity or try to look at their contents without a prior permission of the owner and he should be aware of the limit of the given permission. | A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner. | The Islamic article is more precise as it makes the mere looking at a single piece of information on the screen or the access to a computer even from a remote place deserves punishment. |
| A person should be trust worthy even with a betrayer Any person who got some confidential information or a password to access a computer should not give them deliberately to any person without a prior permission from the owner. Muslims and none-Muslims are equal to be trust worthy. | A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data. | The Islamic article makes the betraying of the trust is prohibited even if the matter concerns somebody who has betrayed the same person before. |
| It is prohibited to get others properties illegally. It is not permitted to get benefits of the contents of a computer or through it without permission. Any action like this is considered a theft. | An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is a state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or a felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more. | The two articles agree that getting any benefit of the computer contents without a prior permission is a crime. But Texas law imposes a financial fine but the Islamic law neglects the financial fines. |
| Muslims should respect their terms. This condition states that it is prohibited to use others' computers or get what is recorded on them of worthy programs or information without a prior permission. Muslims and none-Muslims are equal at that condition. | A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections. | The two articles are different as Texas law gives multiple punishments for multiple crimes. |
| The Islamic punishments are material or abstract in our world and the real and long lasting punishment is in the hereafter. | The law talks about the material punishment as the law is concerned with materials not the soul of the crime. | The Islamic law talks to the conscience of the criminal even if his bad deeds were not discovered, he will suffer his and his fear of God from conscience to be tortured in the hereafter. |

## APPENDIX 1

**Texas Computer Crimes Statute**
**Section 1. Title 7, Chapter 33, Texas Penal Code**
**Section 33.01. DEFINITIONS:**

In this chapter:

(1) Access means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network.

(2) Communications common carrier means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(3) Computer means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(4) Computer network means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(5) Computer program means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(6) Computer security system means the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(7) Computer services means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing and storage functions.

(8) Computer system means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) Computer software means a set of computer programs, procedures and associated documentation related to the operation of a computer, computer system, or computer network.
(10) Computer virus means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.
(11) Data means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media and punchcards, or may be stored internally in the memory of the computer.
(12) Effective consent includes consent by a person legally authorized to act for the owner. Consent is not effective if:
    (A) Induced by deception, as defined by Section 31.01, or induced by coercion;
    (B) Given by a person the actor knows is not legally authorized to act for the owner;
    (C) Given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;
    (D) Given solely to detect the commission of an offense; or
    (E) Used for a purpose other than that for which the consent was given.
(13) Electric utility has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).
(14) Harm includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or ' any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.
(15) Owner means a person who:
    (A) Has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;
    (B) Has the right to restrict access to the property; or
    (C) Is the licensee of data or computer software.
(16) Property means:
    (A) Tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or
    (B) The use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

**Section 33.02. BREACH OF COMPUTER SECURITY:**

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.
(c) An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:
    (1) A state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or
    (2) A felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.
(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

**Section 33.03. DEFENSES:** It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Sec. 33.04 and amended by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

**Section 33.04. ASSISTANCE BY ATTORNEY GENERAL:** The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Sec. 33.05 by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

## REFERENCES


Afifi, A.K., 2003. Computer Crimes and the Author Copyright, Alhalabi Publishing, Lebanon, (In Arabic).

Ahmad, A.M., 2001. The Economic crimes adjudgments in the computer.

Al-A'ali M., 2006. Islamic computer ethics via the ACM computer ethics. International Arab Conference on Information Technology (ACIT'2006), Yarmouk University, Jordan, pp: 19-21.

AUSCERT, Deloitte Touche Tohmatsu and the NSW Police, 2002. Australian Computer Crime and Security Survey, pp: 1-36.

Bloombecker, J., 1995. Simplifying the state and federal computer crime law maze in the USA. Inform. Manage. Comput. Security J., 3: 18-20.

Crystal, J., 2001. Criminal Justice in the Middle East. J. Crimin. Justice, 29.

CSI/FBI Computer Crime and Security Survey, 2003. Computer Security Institute (CFI), San Francisco Federal Bureau of Investigation's Computer Intrusion (FBI), http://www.gocsi.com

Denis, W.J., J.D. Kendall and M.K. Azarian, 1994. Islamic Law Myths and Realities, University of Illinois.

Hassan, R., 1990. Muslims in America: A Living Presence, Horizons.

ISO BS17799, 2005. Information technology-security techniques-codes of practice for information security management. Switzerland: International Organization for Standardization.

Kamali, M.H., 1994. Freedom of Expression in Islam. 1st Edn., Berita Publishing Sdn Bhd, Kuala Lumpur.

Little, B., 2006. Protect and survive-against cyber crime Source. Train. Technol. Hum. Resour., 19: 11-12.

Madkoar, M.S., 1980. The Effect of Islamic Legislation on Crime Prevention in Saudi Arabia, Ministry of Interior, Kingdom of Saudi Arabia, (In Arabic).

Mancuso, S., 2007. Consumer protection in e-commerce transactions: A First Comparison between European Law and Islamic Law. J. Int. Commercial Law Technol., 2.

Parker, D., 1998. Fighting computer crime: A new framework for protecting information. New York: Wiley Computer Publishing.

Peltier, T., 2004. Risk analysis and risk management. Inform. Syst. Security, 13: 44-56.

Schjolberg, S., 2003. The legal frame work-penal legislation in 44 countries. Available from http://www.mosstingrett.no

Texas Computer Crime Law, 1994. Available from: http://suefaw.home.texas.net/

Willison, R., 2006. Understanding the offender/context dynamic for computer crimes. Inform. Technol. People, 19: 170-186.

Willison, R. and J. Backhouse, 2006. Opportunities for computer crime: Considering systems risk from a criminological perspective. Eur. J. Inform. Syst., 15: 403-414.

Yousif, A.F., 2002. Information Technology in 21st, Century: An Islamic Perspective.

Zainul, N., F. Osman, S.H. Mazlan, 2004. E-Commerce from an Islamic perspective. Electronic Commerce Res. Applic., 3: 280-293.