4th WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES, WCETR-2014

The Perception Analysis of Cyber Crimes In View of Computer Science Students

Duygu Solak[a]*, Murat Topaloglu[a]

[a]Trakya Uiversity, Kesan Yusuf Capraz School of Applied Sciences, Edirne

Abstract

Computer Technologies growing rapidly has become an indispensable part of modern life. While making social life easier, the changes that technology has brought also bring forth some security issues. Thus, it is easier to commit crimes and we are faced with cyber-crimes. This study examines the differences among the cyber-crime perceptions of undergraduate students at Trakya University in terms of demographic factors. The method of the study was a questionnaire that was given to lecturers and students at Trakya University sample and it was designed to measure and assess the levels of interest in technology, the severity of cyber-crimes and the individuals' perceptions of cyber-crimes in terms of ethics and law. The findings of the study can help us define the level of common perception of cyber-crimes and the meaningful differences between separate groups.

Keywords: Information Technologies, Cyber Crimes, Information Technology Law, Perception Analysis

1. Introduction

Informatics has been defined as the science of processing of the information used in technical, economic and social communication areas, and on which science has its own basis, properly and logically via electronic machines in particular (Koksal, 2006). The developments in computer and information technologies have penetrated into anything in everyday life. Globalization has gained speed with the internet becoming more popular and the physical

* Duygu Solak. Tel.: +905418713106
  E-mail address: nduygusolak@trakya.edu.tr

boundaries have disappeared. This popularity of the internet has brought forth the issues like storing and processing information. The developments in informatics have both pros and cons for humanity. Since the economic, social and political value of the information has increased, the people who want to cut corners to gain power and money have begun to tend towards using information technologies to commit crimes, sometimes targeting the technology itself. Herein, the term "cybercrime" becomes evident.

Cybercrime is "any kind of illegal, unethical and unauthorized behavior in a system which processes information automatically or transfers data" (Keskin, 2009). Cybercrime can be divided into two main categories where the computer is used as a tool or as a target. Harassing and threatening people on the internet or mobile phones, and publishing music or books without having the copyrights are two examples of cybercrime. The authorities prefer to extend the scope of the punishments for classic crimes instead of adding cybercrime clauses to the present codes. On the other hand, acts like distorting, replacing data and blocking access to a system are crimes where the information systems are targeted directly and there are independent codes and regulations in law defining the scope of these crimes.

Today cybercrime is an important problem growing rapidly. Therefore, the need for legal acts combining both law and technology has risen dramatically. However, there is much to be done to reduce the number of cybercrimes. The first recorded cybercrime was released to the public in a Minneapolis Tribune article "Computer Expert Accused of Cooking the Account Books" on October 18th, 1966. In 1973, one of the classic early data diddling frauds was "Equity Funding" with 64,000 fake client records in Los Angeles (Johnson, 2005)

The first legislative proposal was delivered by Head of Operations Committee, Senator Abe Ribicoff in February 1977. Although the proposal was declined, it helped the concept of computer crime to be discussed in the U.S.A. and other international platforms (Cybercrime Law, 2012). Council of Europe started to work through the electronic data banks to determine the principles to protect the privacy of the individuals. As a result, Committee of Ministers of Council of Europe affiliated two recommendations showing the principles to be applied in electronic data banks in public and private sector and member countries like Germany, France, Austria, Denmark and Norway acknowledged certain codes for data protection. "The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" was ratified on January 28th, 1981.

The most comprehensive regulation is The Convention on Cybercrime realized within Council of Europe which took four years to issue. It was opened for signature in Budapest, on 23 November 2001. As of October 2014, 44 states have ratified the convention, while a further nine states had signed the convention but not ratified it. Turkey has not ratified the convention yet (Avrupa Konseyi Siber Suclar Sozlesmesi Taslagı, 2007).

2. Materials and Method

2.1 Problem Statement

Do the survey scores of the students studying at the Department of Computer Technologies and Information Systems at the School of Applied Disciplines differ by gender and year of study?

2.2 Method

In order to describe the attitudes of Computer Technologies and Information Systems students towards cybercrime from on moral and legal grounds, descriptive survey model was used as the method as descriptive studies help define the related situations as they are in reality (Karasar, 2008).

Relational screening model is also used to determine the relationship between two or more variables. Screening research is a type of research conducted using larger samples which identifies the attitudes, interests, skills in certain areas (Buyukozturk et al., 2008).

Questionnaire forms were given to describe the internet use habits and the attitudes of Computer Technologies and Information Systems students at Trakya University, Kesan Yusuf Capraz School of Applied Disciplines towards cybercrime from on moral and legal grounds and to obtain demographic information.

2.3 Study Group

182 students studying at Trakya University, Kesan Yusuf Capraz School of Applied Disciplines, Department of Computer Technologies and Information Systems during the academic year in 2014-2015 make up the study group of this research.

2.4 Data Collection

The survey used in this study has three subdimensions to obtain demographic information, to assess the internet use and the examples of cybercrimes. The first part includes personal information, such as gender and year of study. In the second part aims to describe the internet use habits of the students. The last part includes Cybercrime Examples Scale with five point likert scale with "Strongly agree (1), Agree (2), Not Sure (3), Disagree (4), Strongly disagree (5)". To examine the attitudes on legal grounds, the statements "Definitely a crime (1), Crime (2), Not Sure (3), Not a Crime (4), Definitely Not a Crime (5)" are used whereas "Certainly right (1), Right (2), Neutral (3), Wrong (4), Definitely wrong (5)" statements are used to examine moral attitudes towards cybercrime. The questionnaire form was taken from the masters' thesis "The Perception Analysis of Computer Crimes With respect to Socio-Cultural Levels" by (İlbas, 2009) and applied to the study group.

2.5 Data Analysis

SPSS 20 (Statistical Package for Social Sciences) was used for the analysis of the data. Percentage and frequency analysis were used to determine the perceptions analysis of cybercrime in computer students. The reliability coefficient for the whole scale was found .88.

3. Findings

In this section, frequency and percentage distributions of the students' genders and years of study are presented. %35,2 (64 students) of the participants were females and % 64,8 (118 people) were males; %14,8 (27 students) were freshmen; %20,3 (37 students) were sophomores; %20,9 (38 students) were juniors; and %44,0 (80 students) were seniors.

According to the frequency analysis results for the interest in computers and technology and following the latest developments in the field; %6 (11 students) of the students reported they are not interested in the subject and do not follow the latest developments with %9,9 (18 students) who are not interested but following the updates in written and visual media. %24,2 of the participants (44 students) said they are interested in the subjects without following the updates with %59,3 (108) reporting their interest in both the subject and latest developments. The results show that majority of the students have interest in computers, technology and the internet following the updates and developments closely.

According to the frequency analysis for how long the students have been using the internet; %0,5 (1 students) said "I don't use"; %0,5 (1 students) said they have been using information technologies for "less than a year"; %10,4 (19 students) 2-5 years; %59,3 (108 students) 6-9 years; %29,1 of the students reported that they have been using the internet more than 10 years. Most of the students have been using the internet for 6-9 years according to the results.

The frequency analysis for the place where the students get connected to the internet show that %31,3 (57 students) can access to the internet at home and %8,2 (15 students) use the internet at work or at school while %0,5 (1 student) goes to internet cafes. %1,6 (3 students) reported using common access areas. Most of the students have been using the internet at home according to the results.

According to the frequency results, the internet is used by students for doing research for work and school with %31,3 (57 students); for doing research for personal interests with %37,4 (68 students); for reading news and current affairs with %14,3 (26 students), for communication purposes with %8,8 (16 students), for forming social relationships %1,1 (2 students); and for entertainment and games %7,1 (13 students). Most of the students seem to use the internet to do research on their personal interests.

According to the frequency analysis results for the average internet use, %4,9 of the participants (9 students) reported not using the internet out of work and school ours while %2,2 (4 students) said they use the internet less than a day in a week. %1,6 (3 students) of the participants told they use the internet one day a week whereas %4,4 (8 students) use the internet several days a week. Overwhelmingly, %86,8 (158 students) of the participants reported that they use the internet almost every day.

Table 1. Item Distributions for Cyber Crime Perceptions on Legal Grounds

		Legally		Morally	
		$\overline{X}$	Standard Deviation	$\overline{X}$	Standard Deviation
1	Using others' Wi-Fi connection with no password.	3,500	1,507	3,593	1,448
2	Reading husband/wife, children or friends' e-mails.	3,912	1,363	4,049	1,305
3	Using software to monitor and control children's internet use.	2,417	1,512	2,412	1,519
4	Visiting websites with sexual and adult content.	3,978	1,341	3,961	1,347
5	Sending spam e-mails for advertising.	3,923	1,364	4,005	1,310
6	Sending e-mails including personal information and notice to more than one	2,939	1,379	2,928	1,362
7	Adding misleading information to forums and online encyclopedias.	4,126	1,300	4,044	1,393
8	Providing and obtaining movie files that are still showing via sharewares.	3,406	1,444	3,263	1,428
9	Providing and obtaining new-release music albums via sharewares.	3,456	1,431	3,296	1,414
10	Providing and obtaining old-dated movies and music albums via sharewares.	2,747	1,449	2,697	1,411
11	Searching for the security weaknesses in an information system that belongs to	3,483	1,440	3,296	1,448
12	Using sniffers to monitor the internet traffic of others.	3,950	1,262	3,824	1,275
13	Using software with open source codes to make profit.	3,181	1,532	3,087	1,495
14	Using operation systems (Linux, etc.) with general public license for individual	2,818	1,469	2,708	1,455
15	Using techniques to ban access to a website.	3,544	1,368	3,494	1,373
16	Decrypting an e-mail password that belongs to another person and using the	4,314	1,113	4,164	1,219
17	Decrypting and changing an e-mail account password that belongs to another	4,318	1,140	4,175	1,317
18	Gathering personal information from internet users and leaking them to third	4,373	1,162	4,214	1,310
19	Obtaining a serial number of a paid software and using it for free.	3,428	1,442	3,225	1,405
20	Coding and spreading viruses and Trojans.	4,192	1,235	3,945	1,409
21	Creating and using fake accounts on free services like SKYPE and Facebook.	4,236	1,205	4,208	1,203
22	Forwarding offensive e-mails insulting individuals or companies to others.	4,104	1,158	4,082	1,216
23	Declaring personal opinions about securities (stock certificates, etc.) on the	3,505	1,432	3,500	1,444

According to the table above, the three statements with the highest percentages that evaluate the legal perspectives of the students are as follows:

1.	127 of the students said "definitely agree" in addition to 26 students who told they "agree" with the statement "Gathering personal information from internet users and leaking them to third persons." According to the descriptive analysis results, it has the highest mean with 4,373.
2.	120 of the students said "definitely agree" in addition to 27 students who told they "agree" with the statement "Decrypting and changing an e-mail account password that belongs to another person." According to the descriptive analysis results, it has the second highest mean with 4,318.
3.	115 of the students said "definitely agree" in addition to 33 students who told they "agree" with the statement "Decrypting an e-mail password that belongs to another person and using the account without changing it." According to the descriptive analysis results, it has the third highest mean with 4,314.

According to the table above, the three statements with the lowest percentages that evaluate the legal perspectives of the students are as follows:

1.	75 of the students said "definitely disagree" in addition to 45 students who told they "disagree" with the statement "Using software to monitor and control children's internet use." . According to the descriptive analysis results, it has the lowest mean with 2,417.

2.   46 of the students said "definitely disagree" in addition to 46 students who told they "disagree" with the statement "Providing and obtaining old-dated movies and music albums via sharewares." According to the descriptive analysis results, it has the second lowest mean with 2,818.

3.   46 of the students said "definitely disagree" in addition to 40 students who told they "disagree" with the statement "Using operation systems (Linux, etc.) with general public license for individual purposes." According to the descriptive analysis results, it has the third lowest mean with 2,747.

According to the table above, the three statements with the highest percentages that evaluate the moral perspectives of the students are as follows:

1.   119 of the students said "definitely agree" in addition to 25 students who told they "agree" with the statement "Gathering personal information from internet users and leaking them to third persons." According to the descriptive analysis results, it has the highest mean with 4,214.

2.   108 of the students said "definitely agree" in addition to 37 students who told they "agree" with the statement "Creating and using fake accounts on free services like SKYPE and Facebook." According to the descriptive analysis results, it has the second highest mean with 4,208.

3.   116 of the students said "definitely agree" in addition to 26 students who told they "agree" with the statement "Decrypting and changing an e-mail account password that belongs to another person." According to the descriptive analysis results, it has the third highest mean with 4,1758.

According to the table above, the three statements with the lowest percentages that evaluate the moral perspectives of the students are as follows:

1.   73 of the students said "definitely disagree" in addition to 44 students who told they "disagree" with the statement "Using software to monitor and control children's internet use." According to the descriptive analysis results, it has the lowest mean with 2,412.

2.   47 of the students said "definitely disagree" in addition to 45 students who told they "disagree" with the statement "Providing and obtaining old-dated movies and music albums via sharewares." According to the descriptive analysis results, it has the second lowest mean with 2,697.

3.   53 of the students said "definitely disagree" in addition to 35 students who told they "disagree" with the statement "Using operation systems (Linux, etc.) with general public license for individual purposes." According to the descriptive analysis results, it has the third lowest mean with 2,708.

Table 2. Students' Legal and Moral Perceptions of Cyber Crime by Gender and T-Test Results

Total	Gender	N	$\overline{X}$	F	Sig.
On Legal Grounds	Female	64	87,25	.035	.017*
	Male	118	82,03		
On Moral Grounds	Female	64	84,89	1,89	.051
	Male	118	80,71		

* p<.05

In Table 2, the statistical value for students' legal perspectives of cybercrime by gender was found p<0,05 which means that gender can play an important part on legal grounds. Also, the statistical value for students' moral perspectives of cybercrime by gender was found p>0,05 which means that gender can play an important part on legal grounds which was thought more and less meaningful. The total score for cyber crime from a legal perspective by gender was found X = 87,25 points for female students and X=82,03 points for male students while the total score for cyber crime from a moral perspective by gender was found X = 84,89 points for female students and X=80,71 points for male students.

Table 3. One Way Variance Analysis Results for Students' Legal and Moral Perceptions of Cyber Crime by Year of Study

Total		N	$\overline{X}$	F	Sig.
On Legal Grounds	Freshmen	27	81,22		
	Sophomore	37	84,40		
	Junior	38	84,84	.395	.757[*]
	Senior	80	84,01		
	Total	182	83,85		
On Moral Grounds	Freshmen	27	81,96		
	Sophomore	37	82,43		
	Junior	38	80,07	.423	.737[*]
	Senior	80	83,13		
	Total	182	82,18		

* p>.05

In Table 3, p > .05 was found for students' both legal and moral perceptions of cybercrime by year of study and there was not a meaningful difference between them by year of study.

3.Conclusion

In the light of the findings of and the results obtained from this study, the recommendations are as follows; there were 64 female and 118 male participants. The largest group was senior students with 80 participants. Participants definitely agreed that gathering personal information of internet users and leaking them to third persons is a cybercrime while they indicated that sharing old-dated movies and music on the internet is not a bad thing. There was no significant difference between the legal and moral perspectives of the students. As most of the students reported disagreement with gathering personal information of internet users and leaking them to third persons, they are responsive to privacy on legal grounds. They also supported the monitoring of children's internet use by saying using parental control software is not a crime.

All in all, the number of interdisciplinary undergraduate programs like information technology law is not sufficient. Child pornography and cyber fraud are generally more emphasized as cybercrimes while other types are neglected most of the time in media. Besides, there are still objections and obstacles regarding the definition and determination of the behaviors that are described as crimes in law.

It is clear that the police and governments alone are not likely to prevent and solve cybercrimes that have become one of the biggest problems in modern world. For that reason, individuals as internet users should be informed and aware of cybercrime by perceiving cybercrimes as classic crimes and social phenomena.

References

Avrupa Konseyi Siber Suclar Sozlesmesi Taslagı (2007). Ankara Barosu Bilgi Islem Merkezi Yayınları.

Buyukozturk, S., Kılıc Cakmak, E., Akgun, O.E., Karadeniz, S., & Demirel F. (2008). *Bilimsel Arastırma Yontemleri*. Ankara: Pegem Akademi.

CyberCrime Law. (2012). Retrieved from: http://www.gov.ph/2012/09/12/republic-act-no-10175/

Elektronik Ticaret Hukuk Calısma Grubu Raporu. (1998). Erisim: http:// enoter_hukuk.tripod.com/ icelnoterodasicjb/tic.htm

Ilbas, C. (2006). *Bilisim Suclarının Tespitinde Kablosuz Internet Engeli, Bilisim ve Hukuk*. 1(1):34.

Ilbas, C. (2009). *Bilisim Suclarının Sosyo-Kulturel Seviyelere Gore Algı Analizi*. Phd Thesis.

Johnson, T.A. (2005). *Forensic Computer Crime Investigation*, CRC Press.

Karasar, N. (2013). *Bilimsel Arastırma Yontemi*. Ankara: Nobel Yayın Evi.

Kececi, O. (2011). *Siber Sucar Ve Siber Terorizm*.

Keskin, İ. (2007). *Bilisim Sucları*. Adalet Dergisi, Adalet Bakanlıgı Yayın Isleri Baskanlıgı, 29:6.

Koksal, A. (2006) *ENIAC'ın 60. Yılında TBD 35 Yasında*. TBD, Ankara. Yıl:35 sayı:93