Knowledge Levels and Attitudes Toward Cybercrimes of Adolescents in Northern Cyprus

Fezile Ozdamli [1], Erinc Ercag [2]

[1]*Near East University, Department of Computer Information System, Nicosia, Cyprus, Mersin 10, Turkey*
[2]*Near East University, Department of Computer Education and Instructional Technology, Nicosia, Cyprus, Mersin 10, Turkey*

Abstract **– Besides the many positive effects of the use of information technologies, it also generates many problems. It is especially of great importance to determine the level of knowledge and awareness of individuals on the cybercrime. No studies have been conducted on this issue in the Turkish Republic of Northern Cyprus. Based on this, it was necessary to determine the knowledge level of adolescents who are frequent users of digital technologies regarding the cybercrimes and their attitudes toward them. This study is a descriptive survey model. The working group is composed of 407 adolescents in the TRNC. The data collection tool was "Concepts of Informatics and Student Opinion Survey on Cyber Crimes" developed by Gozler and Tasci (2015). The 5 point Likert scale questionnaire consists of 16 items. Frequency, percentage and mean analysis was applied during the data analysis. It is clear that cybercrime awareness in Northern Cyprus has to be increased.**

Keywords **– Young, cybercrime, attitudes.**

1. Introduction

The changes in information and communication technologies in the present era of technology have led to advancements in many areas of our lives [1].

DOI: 10.18421/TEM84-35
https://dx.doi.org/10.18421/TEM84-35

Corresponding author: Fezile Ozdamli,
Near East University, Department of Computer Information System, Nicosia, Cyprus, Mersin 10, Turkey
Email: fezile.ozdamli@neu.edu.tr

Received: 28 September 2019.
Revised: 05 November 2019.
Accepted: 11 November 2019.
Published: 30 November 2019.

There are hardly any businesses at present time that do not implement the use of information technologies. The developments in the field of information and communication technologies have a great impact on the social, political, economic, cultural and similar fields, and therefore the profile of manpower which is the essential component of information societies is changing day by day. Besides the many positive effects of the use of information technologies, it also generates many problems. The concept of informatics, which facilitates our lives by establishing the bridge between the world of information and the world of technology, provides a basis for the violation of human rights [2]. One of the bad uses of information technologies is the use of informatics for perpetrating crimes. According to Beceri (2006), cybercrimes do not share the same definition as ordinary crimes and that ordinary crimes are those committed before any cybercrime was ever committed. According to Katos and Bednar (2008) as well as having commonalities between them, cyber and physical crimes also have significant differences, making the topic of cyber-crime an important area of research. The main difference between cybercrimes and physical crimes is that the boundaries of the crime scene cannot be clearly drawn. Cybercrime may extend beyond a room, a city, a country or a continent [9]. Alaca and Ilbars state that cybercrimes are also referred to as "computer violation", "computer criminality", "malicious use of computers", "cybercrime" and" internet crime". Cyber Crime is illegal, unethical, unauthorized behaviour in a system that automatically processes or transmits information [4]. Ilbas (2009) indicates that terms such as computer-related crime, crimes committed via computers, high-tech crime, computer crime, and IT crime are ones which also mean cybercrime [12]. As more and more data is stored electronically, cybercrimes and environmental security have become agenda items [5]. The concept of what constituted Cyber Crime was identified under 12 headings in a doctrine in the United States, where the first crimes were

committed. These are; data or service theft, property theft, access violations, data fraud, personal errors, extortion, violation of sensitive information, sabotage, theft of tangible assets, fraud, theft of ATM cards, actions taken to obtain passwords of magnetic cards [6]. The joint report of EU and UN commission lists cybercrimes under the following headings are: unauthorized access and listening to computer systems and services" "computer sabotage" "computer fraud" "counterfeiting", "unauthorized use of a software protected by law" and "illegal publications" [2]. Koc and Kaynak classify cybercrime as follows: "unauthorized access to computer systems", "obstruction, destruction of information systems or modification of data", "unauthorized use of a software protected by law", "illegal publications", "obscenity-child pornography on the internet", "aggravated fraud committed through informatics", "insult, slander and blackmail via informatics", "illegal actions taken against electronic signature act" [11]. According to Henkoglu (2014), the first means to harm information systems and data is the use of harmful software. Some of the most commonly used malware are; Viruses, Scams, Rootkit, Spam, and Rabbits [5]. Spinello (2006) indicated that the worm "Blaster" and the virus "SoBig" exclusively caused approximately $ 35 million worth of damages in the summer of 2003 [7]. Kurt (2005) stated that it is possible to commit cybercrimes in many different ways. Some are as follows: scavenging, eavesdropping, data diddling, trojan horse, scanning, super zapping, salami techniques, trap doors, asynchronous attacks, network worms, viruses, piggybacking, spam, logic bombs, masquerading, credit card fraud and etc. [8]. Most fraud now involves technology in some way and networks are clogged with malicious traffic, including phishing emails, ransom ware, malvertising and other illegal methods of parting people from their money [10]. Meanwhile, Koc and Kaynak (2011) maintain that the constant advances in technology have led to the increase of cybercrimes; stating that "cybercrimes aim to inflict material or moral damage to people or institutions with the help of technology and often in a virtual environment". Moreover, violations which are also regarded as offenses are computer crimes, computer-related crimes, computer criminality, and informatics infringement [11]. In a National Computer Crime Squad (NCCS) study conducted in the United States of America by The Federal Bureau of Investigation cybercrime has been classified as a violation of the general telephone network, violation of major computer networks, violation of network integrity, violation of private life, industrial / corporate espionage, software piracy, and other crimes in which computers play a role [12]. Many researchers categorise cybercrime as crimes committed against informatics and informatics systems (Target information systems) and the crimes committed using informatics and informatics systems (Mode information systems). The aim of the target system is to prevent the confidentiality, integrity or accessibility of the information in the system. The services provided, the stored, received or sent data, or the hardware is damaged in target information crimes. Crimes committed by means of information systems are events such as cyber terrorism, fraud; intellectual property rights violations and online sales of illicit substances [13], [14]. Today, cybercrime is important problem which is increasing rapidly. Therefore, the need for legal actions combining law and technology has greatly increased [18].

Literature review reveals that a lot of research has been done into cybercrime. Research on cybercrime has been carried out in many areas. Some studies are related to cybercrimes involving bank accounts, while some studies are related to cybercrimes aimed at personal data in social networks [14], [15], [16]. One of the remarkable facts is that among the people exposed to cybercrimes, there are those who are highly educated. It may be said that individuals who do not have sufficient awareness about cybercrimes are highly likely to be victims [17]. It is clear that cybercrime is escalating day by day and the individuals and institutions are victims. While many suggestions have been put forth on how to prevent cybercrime, the number of studies on how to protect against cybercrime crimes, or on the level of awareness of cybercrime is very few. It is especially of great importance to determine the level of knowledge and awareness of individuals on the subject in the Turkish Republic of Northern Cyprus. No studies have been conducted on this issue in the Turkish Republic of Northern Cyprus. Based on this, it was necessary to determine the knowledge level of adolescents who are frequent users of digital technologies regarding cybercrimes and their attitudes toward them. It is important to examine the relationship between different variables of information crime level of adolescents. It is important to examine the relationship comprising knowledge levels of adolescents within different variables of cybercrime.

The purpose of this study is to determine the knowledge level of ICT crimes of individuals living in Turkish Republic of Northern Cyprus and their opinions on the subject.

The following sub-aims were developed and based on this aim:

• For what purposes do adolescents use the internet?

• What is the knowledge level of adolescents of ICT crimes committed on the Internet?

• What are the attitudes of adolescents towards cybercrimes?

2. Method

This study is a descriptive survey model. The working group is composed of 450 adolescents in the TRNC. The return rate was 90% and 407 usable questionnaires were available for analysis. 53.8% of the adolescents participating in the research are females.

Instrument and Procedure

The data collection tool was "Concepts of Informatics and Student Opinion Survey on Cyber Crimes" developed by Gozler and Tasci (2015). The 5 point Likert scale questionnaire consists of 16 items. Cronbach Alpha internal consistency coefficient was 0.84 in the study in which the data collection tool was developed [17]. The Cronbach Alpha internal consistency coefficient was calculated as 0.89. The following limits were taken into account when evaluating the statements in the data collection tool:

Table 1.Limits for Evaluation

Degree / Option	Score Limit
I strongly disagree	1.00 – 1.79
I do not agree	1.80 – 2.59
I am undecided	2.60 – 3.39
I agree	3.40 – 4.19
I strongly agree	4.20 – 5.00

The statistical package program SPSS 25 software was used in analysing the obtained data. During the analysis of data; f, %, mean, t-test analysis was used and the significance level was determined as .05

3. Results

Internet use objective of adolescents

When the daily internet usage habits of the adolescents who participated in the study were examined, it was established that 10% of them used the internet for at least one hour, 22% for 2-3 hours, 25.3% of them used internet for 4-5 hours and 42% of them used internet for more than 6 hours. A frequency test was used to determine the reasons for adolescents' internet use. The findings are presented in the table below:

Table 2. The main reasons why adolescents use the internet

Reason	f	%
To listen to music	347	85.3
To use social networking sites	342	84.0
To watch films	332	81.6
To chat	306	75.2
To scan for sources	253	62.2
To play games	216	53.1
To learn	204	50.1
To meet new people	135	33.2
To install software	106	26.0
To share information	100	24.6
To access online news	91	22.4
To share ideas or fantasies	89	21.9
Other	89	21.9

As seen in Table 2, adolescents mainly use the Internet to listen to music, access social networking sites, watch movies and chat. The study is conducted with university students by Gozler and Tasci revealed that the main reason why students go on line is to do homework and research. 17]. This difference is thought to be from the age of the participants.

Levels of Knowledge Adolescents have about Cyber Crimes

The awareness of cybercrimes among adolescents participating in the study is discussed at 3 levels; "those who know about this concept, "those who have only heard about the concept" and "those who have no idea about this concept". The frequencies and percentages for these 3 levels are presented in Table 3.

Table 3. Levels of Knowledge Adolescents have about Cyber Crimes

	I know what this concept is		I only heard of the concept		I have no idea about this concept	
	f	%	f	%	f	%
Worms	28	6.9	102	25.1	277	68.1
Network security	274	67.3	114	28	19	4.7
Hacker	96	23.6	217	53.3	94	23.1
Cracker	41	10.1	60	14.7	306	75.2
Child porn	289	71	99	24.3	19	4.7
Digital sign	145	35.6	207	50.9	55	13.5
Hacking	139	34.2	163	40	105	25.8
Logic bombs	9	2.2	37	9.1	361	88.7
Masking	28	6.9	53	13	326	80.1
Phishing attack	11	2.7	35	8.6	361	88.7
Phreakers	7	1.7	22	5.4	378	92.9
Trap doors	10	2.5	36	8.8	361	88.7
Salam technique	7	1.7	33	8.1	367	90.2
Cyber fraud	27	6.6	98	24.1	282	69.3
cyber gambling and betting	40	9.8	102	25.1	265	65.1
Cyber blackmail and threat	36	8.8	100	24.6	271	66.6
Spam	26	6.4	89	21.9	292	71.7
Trojen	12	2.9	45	11.1	350	86.0
Warez	9	2.2	29	7.1	369	90.7
Web page theft	93	22.9	220	54.1	94	23.1

As seen in the table above, 71% of adolescents know about child porn and 67.3% know the concepts of computer and network security. More than half of the adolescents know these concepts. Digital sign and hacking are the next most commonly known concepts among adolescents. Gozler and Tasci's similar study which was carried out in Turkey determined "Computer and network security" and "child pornography" as the most well-known concepts. [17]. Solak and Topaloglu stated that the most known concepts are child pornography and cyber fraud. [18].

Web page theft (54.1%), hacker (53.3%), and Digital sign (50.9%) are concepts that more than half of the adolescents have heard of, but have no knowledge about what they are. Half of adolescents have heard about the concept of hacker, but do not know exactly what it involves. A study on cyber bullying in Turkey revealed that the main crime adolescents either commit or are victims of is the hacking of friends' mail accounts. [19], [20].

Interestingly, most of the adolescents had no idea about Phreakers (92.9%), Warez (90.7%), Salam technique (90.2%), Logic bombs (88.7%), phishing attacks (88.7%), trap doors (88.7), trojans (86%), masking (80.1%), cracker (75.2%), spam (71.7%), cyber fraud (69.3%), worms (68.1%), cyber gambling - threat (66.6%) and cyber gambling - betting (65.1%).

Attitudes of adolescents on cybercrimes and those who commit cyber crimes

In addition to the importance collecting data about how aware adolescents are of cybercrimes, it is also important to examine their views on cybercrime and cyber criminals as contribution to the study.

Therefore, a 5-point Likert scale data collection tool prepared by Gozler and Tascin was applied. Adolescents were asked to choose the expression that best represented their thoughts. The mean and standard deviations were calculated and the opinions of adolescents about cybercrimes were determined and interpreted. The results obtained of the analyses are presented in Table 4.

Table 4. Attitudes of adolescents on cybercrimes and those who commit cyber crimes

No	Opinion statements on cybercrime	X	S
1	I know what to do if my passwords are hacked	1.953	.865
2	Information about cybercrimes should be provided in ICT courses	3.941	.837
3	My best friends know my passwords	1.825	.801
4	I don't have enough knowledge about internet fraud	3.850	.818
5	It would upset me if my email or other accounts were to be hacked	4.076	.753
6	I recognize emails that are potentially dangerous when I receive them	2.334	1.012
7	I don't add people I don't know to my email contact list and social media pages	3.884	.808
8	I shop online with my credit card without concern	1.889	.787
9	My computer is protected against viruses	3.852	.826
10	Press and media do not inform people about cyber crimes	3.75	.828
11	I know what to do when I witness any sort of cyber crime	2.063	.842
12	Penalties for cybercrimes should be severe	4.132	.703
13	Information on cybercrimes should be given from the start of primary school	3.990	.742
14	Cybercrimes are not as dangerous as they are made out to be	1.879	.795
15	Conferences and seminars about cybercrimes should be organized	4.196	.719
16	People who commit cybercrimes are very intelligent	3.643	.864

The analysis of the study determined that adolescents agreed on the importance of participating in conferences and seminars on cybercrimes, and that education on the subject should start during the primary education. Moreover, adolescents felt that they were distraught when their email and other social account passwords were hacked that not even their closest friends knew their passwords. In addition, not favouring the idea of online shopping adolescents' state that cybercrime is a dangerous situation. According to the findings, adolescents do not have substantial knowledge about password hacking and what they should do when they are exposed to viruses.

4. Discussion and Conclusion

According to the results, almost half of the adolescents use the Internet for at least six hours. Similarly, in a report prepared by the English Education Policy Institute (EPI) in the UK, more than one third of the UK's adolescents use the internet for at least six hours per day, and they are therefore classified as 'excessive internet users'. In addition, adolescents mostly go online to listen to music, use social networking sites, watch movies and chat. In the study conducted by Pew Research Center in the US in 2017, it was stated that almost all of the adolescents used social networking sites actively, and that especially YouTube, Instagram and Snapchat were popular among adolescents [3].

These results provide us an insight into the degree at which adolescents are exposed to cybercrimes.

Moreover, the results show that the majority of adolescents were familiar with concepts such as 'child pornography' and 'computer and network security'. While child pornography and cyber fraud are often emphasized as cybercrimes, while other types of cybercrimes are often overlooked in the media. In addition, there are still legal objections and obstacles to the definition and determination of the behaviours that are regarded as cybercrimes in the law.

Warez, which is one of the concepts that are unknown to adolescents, is the name for all pirated software in general. Due to the lack of copyright laws and related laws in Northern Cyprus, pirated software is used in many corporate and personal computers. However, adolescents do not know about this concept.

Other results obtained from the study show that adolescents are trying to protect themselves by taking precautions such as not sharing their account information with others and refraining from shopping online. Training sessions or seminars can be organized and presented by experts to give vital information as to what one needs to pay attention to while shopping on the internet. By teaching them informatics concepts they are unfamiliar with, adolescents may become better equipped to protect themselves.

Furthermore, educators in primary education and universities and decision makers have important duties in this regard. Researchers should work across the country to recognize cyber-crime profiles and training needs. Researchers should work across the country to recognize cyber-crime profiles and to determine training needs. This study can be used as a reference for assessing adolescents' awareness of cybercrimes, setting training needs and organizing relevant activities.

As with every study, this study has some limitations. Only one of these adolescents has been involved in the study, and it can be included in future studies by child and adults in Northern Cyprus. In addition, future studies can be conducted through qualitative interviews, and in-depth results can be obtained as well.

References

[1].Fasli, E., & Ozdamli, F. (2018). Teacher Candidates' Opinions Regarding Instructional and Safe Use of Social Networks and Internet Addiction Risk Levels,*Technology Education Management Informatics,7*(2), 405-410.

[2].Altunok, E.,& Vural, F.,A. (2011). Bilişim Suçları. Denetişim, (8), 74- 84.

[3]. Campbell, D. (2017). British teenagers among world's most extreme internet users, report. Theguardian. Retrived on 27 November 2018 from: https://www.theguardian.com/technology/2017/jun/30/british-teenagers-among-worlds-most-extreme-internet-users-report-says

[4].Alaca, B. (2008). Ülkemizde bilişim suçları ve internetin suça etkisi (Antropolojik ve hukuki boyutları ile). *Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi. Ankara*..

[5].Henkoglu, T. (2014). Adli Bilisim. Istanbul: Pusula Publishing.

[6].Avsar, B.Z.,& Ongoren, G. (2009). İnternet Hukuku. P,96. Ankara: TOBB Publishing.

[7].Spinello, R. A., (2006). Cyberethics Morality and Law in Cyberspace, London: Jones and Barlett Publishers.

[8].Kurt, L. (2005). Tüm yönleriyle bilişim suçları ve Türk Ceza kanunundaki uygulaması. P.60-77. Istanbul: Seckin Publishing.

[9].Katos, V., & Bednar, M. P. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces*, *30*, 223-228.

[10]. Moskowitz, L.S. (2017). Cybercrime and Business. Elsevier Science: Butterworth-Heinemann.

[11]. Koç, S., & Kaynak, S. (2010). Bilişim suçları bağlamında yeni medya olarak internet ve kişisel güvenlik. *Akademik Bilişim, 10*, 10-12.

[12]. İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi* (Master's thesis, Başkent Üniversitesi Fen Bilimleri Enstitüsü).

[13]. Gönen, S., Ulus, H. İ., & Yılmaz, E. N. (2016). Bilişim alanında işlenen suçlar üzerine bir inceleme. *Bilişim Teknolojileri Dergisi*, *9*(3), 229-236.

[14]. Yalcın, N. & Gurbuz, F. (2015). Sosyal ağlarda islenen suclar, Facebook Sosyal Agı Ornegi. Akademik Bilisim Konferansı. Eskisehir: Anadolu University.

[15]. Yurtsal, S.E. (2016). Fear of Crime in Social Networks: Facebook Example. Güvenlik Bilimleri Dergisi, *5*(2), 93-112.

[16]. Hutchinson, D., & Warren, M. (2003). Security for internet banking: a framework. *Logistics information management*, *16*(1), 64-73.

[17]. Gözler, A., & Taşçi, U. (2015). Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları. *International Journal of Informatics Technologies*, *8*(3), 147-157.

[18]. Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia-Social and Behavioral Sciences*, *182*, 590-595.

[19]. Kavuk-Kalender, M., & Keser, H. (2018). Cyberbullying Awareness in Secondary and High Schools. *World Journal on Educational Technology: Current Issues*, *10*(4), 25-36.

[20]. Kavuk, M. Y., & Keser, H. T. D. (2011). *İlköğretim öğrencilerinin sanal zorba ve sanal kurban olma durumlarının incelenmesi* (Doctoral dissertation, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı (Eğitim Teknolojisi Programı)).