International
SMART Journal
International SOCIAL MENTALITY AND RESEARCHER THINKERS Journal
e-ISSN: 2630-631X

RESEARCH ARTICLE
COMPUTER AND INSTRUCTIONAL TECHNOLOGIES

Determination of Cyber Security Knowledge Level of Vocational High School Students in the Field of Information Technologies *

Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi

Ahmet Naci Çoklar [1]
Selim Aslan [2]

ABSTRACT

It is seen that today's education policy has changed, and the cyber security education in the curriculum recorded for the Information Technologies field of Vocational and Technical Anatolian High Schools is included in a condensed course module in Network Operation and a course module within common courses. It is explained that it is valuable to inform those who use the field's information technologies the most and to be the individuals who will develop these technologies in the future, and to what extent it is valuable to examine cyber security information within the scope of training in the field of Information Technologies. The purpose of the research is to determine the level of knowledge regarding personal cyber security in the development of information technologies in vocational high schools. In this context, data was collected from 305 students in the field of Information Technologies at vocational high schools in the central districts of Meram, Selçuklu and Karatay in Konya province. In order to collect data, the Personal Cyber Security Ensuring Scale was used. The results of the analysis of the data show that general cyber security knowledge is at a medium level. There was no significant change in general cyber security knowledge levels according to the grade levels of students. And also there is no significant difference in general cyber security knowledge levels depending on the situations of cyber victimization. It has been suggested that students should be given more cyber security training.

Keywords: Cyber Security, Information Technologies, Vocational High School, Cyber Security Training, Information Security.

ÖZET

Günümüzde eğitim politikasının değiştiği, Mesleki ve Teknik Anadolu Liselerinin Bilgi Teknolojileri alanına yönelik kaydedilen müfredatlarda siber güvenlik eğitiminin, Ağ İşletmeciliği alanında yoğunlaştırılmış bir ders modülü ve ortak dersler içerisinde bir ders modülü içerisinde yer aldığı görülmektedir. Alanın bilişim teknolojilerini en çok kullananların bilgilendirilmesinin ve gelecekte bu teknolojileri geliştirecek bireyler olmasının değerli olduğu, siber güvenlik bilgilerinin eğitim kapsamında incelenmesinin ne ölçüde değerli olduğu anlatılmaktadır. Bilgi Teknolojileri alanı. Araştırmanın amacı meslek liselerinde bilişim teknolojilerinin geliştirilmesinde kişisel siber güvenliğe ilişkin bilgi düzeyinin belirlenmesidir. Bu kapsamda Konya ili Meram, Selçuklu ve Karatay merkez ilçelerindeki meslek liselerinde Bilişim Teknolojileri alanında öğrenim gören 305 öğrenciden veri toplandı. Verilerin toplanması amacıyla Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır. Verilerin analizi sonuçları genel siber güvenlik bilgisinin orta düzeyde olduğunu göstermektedir. Öğrencilerin sınıf düzeylerine göre genel siber güvenlik bilgi düzeylerinde anlamlı bir değişiklik görülmedi. Ayrıca siber mağduriyet durumlarına bağlı olarak genel siber güvenlik bilgi düzeylerinde de anlamlı bir farklılık görülmemektedir. Öğrencilere siber güvenlik eğitimlerinin daha fazla verilmesi önerisi getirilmiştir.

Anahtar Kelimeler: Siber Güvenlik, Bilişim Teknolojileri, Meslek Lisesi, Siber Güvenlik Eğitimi, Bilişim Güvenliği.

How to Cite This Article
Çoklar, A. N. & Aslan, S. (2023). "Determination of Cyber Security Knowledge Level of Vocational High School Students in the Field of Information Technologies", International Social Mentality and Researcher Thinkers Journal, (Issn:2630-631X) 9(78): 5207-5213. DOI: http://dx.doi.org/10.29228/smryj.73684

Arrival: 15 September 2023
Published: 25 December 2023

INTRODUCTION

The Internet has become a part of daily life in many areas, from communication to education, from health to entertainment. In all kinds of transactions, information from personal information to bank card information is shared on the internet via digital media, which makes the issue of security in the cyber world important. Because the Internet provides both users and malicious individuals with the opportunity to access a computer anywhere in the world. This ability to reach is not always used in good faith. If the accessed computer system does not have sufficient security, there is a possibility of accessing the data in the system, changing these data or even corrupting the system (Alqahtani, 2022). In this context, the concept of cyber security gains importance.

* This study was produced from the thesis prepared by Selim ASLAN and supervised by Prof.Dr. Ahmet Naci Çoklar.

[1] Prof. Dr., Selçuk University, Faculty of Education, Department of Educational Sciences, Konya, Türkiye
[2] Teacher, Ministry of Education, Information Technologies Teacher, Konya, Türkiye

Cybersecurity is an organization and collection of resources, processes, and structures used to protect against events that cause actual injustice in cyberspace and active cyberspace systems (Craigen et al., 2014). In the 2016-2019 National Cyber Security Strategy prepared by the Ministry of Transport, Maritime Affairs and Communications, the concept of cyber security includes protecting the information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information/data processed in this environment, and detecting attacks and cyber security incidents. It refers to the activation of response mechanisms against these detections and then returning the systems to their pre-cyber security incident state (USGS, 2016). The concept of cyber security, also called information security and information security, is defined by Canbek and Sağıroğlu (2006) as all efforts to create a secure information processing platform to protect the integrity of the information from unauthorized access while storing and transporting data or information in electronic environments. Cyber security education is gaining importance in order to increase awareness and precautions regarding cyber education.

Cyber Security Training in Vocational and Technical Anatolian High Schools

The field of information technologies is the field where education and training are provided to gain competencies in the branches of network operation, computer technical service, database programming and web programming, which are under the field, as well as the software and hardware installation of computer systems (MEB, 2011). Since students studying in the field of Information Technologies choose this field as a profession, they are expected to have more knowledge than others and to use cyber security methods in the information technologies they develop. In this regard, the Information Ethics and Information Security module has been added to the Programming Fundamentals course in the Framework Curriculum of the Ministry of National Education. The intended learning outcomes of the module are stated below (MEGEP, 2018).

- ✓ Explains the concepts of ethics and information ethics.
- ✓ Explains the basic concepts of information security management.
- ✓ Explains Basic Security Principles.
- ✓ Explains cyber crimes and abuses.
- ✓ Explains IT law.

The purpose of the Network Security module taught in the Network Systems and Routing course in the Network Operations branch is to ensure that when the necessary environment is provided; It is defined as being able to use security tools by taking security measures to ensure that the network operates smoothly and safely, and configuring a wireless network that works smoothly and securely (MEGEP, 2018).

When all courses in the field are examined, it is seen that there is no training on cyber security except these two courses. Since the Network Systems and Routing course is a course taken only by students who choose the Network Management branch, it does not cover all students in the field. Only the Programming Fundamentals course is among the common courses and all students in the field take this course in the 10th grade. Therefore, the Information Ethics and Information Security module included in this course is the only resource that students in the field of Information Technologies receive for cyber security education.

It has become necessary to raise awareness of the entire society as a whole in order to eliminate the threats that may come from cyberspace, which includes information technologies that all segments of society, from children to the elderly, use or have to use. In this respect, it was deemed important and researched to determine the awareness of students studying information technologies in secondary education institutions, who can be considered as qualified manpower in this field, about cyber security.

Related Research

In the study conducted by Budak (2015), the cybercrime awareness of informatics department students in Vocational and Technical High Schools was investigated, and while it was found that the students' awareness of cybercrimes was generally at a sufficient level, their cyber awareness did not show a significant difference with their class status, years of using the Internet and the status of being attacked on the Internet. However, it was observed that there was a significant difference with gender. In the research conducted by Zeybek (2011), it was revealed that female students use information technologies more ethically than male students. It has been determined that students whose families have high income levels use information technologies for more unethical purposes. A significant difference was observed between students' ethical use of information technologies and their grade levels in terms of Social Impact, Network Integrity, Intellectual Property and Security-Quality factors. Students studying in the fields of Information Technologies and Electrical and Electronic Technologies expressed more unethical opinions than those studying in the fields of Child

Development and Education and Graphics and Photography. In another study conducted by Tekerek and Tekerek (2013), it was found that students' information security awareness levels on ethical issues were at a sufficient level, while students' awareness levels on rules and issues requiring knowledge were low. This has been interpreted as revealing the idea that information and computer security awareness training and activities are insufficient. Karaci et al. In the study conducted by (2017), the cyber security behaviors of university students studying in a department related to information technologies were examined in terms of different variables. According to the results of the study, it was observed that the cyber security behaviors of the students were at a level that would ensure cyber security, while it was stated that the cyber security behaviors of the students who received Internet-computer security training or had work experience in this regard were more positive. In addition, it is seen that students who graduated from vocational high schools are more careful than students who graduated from high school in terms of leaving no trace factor. When the researches are examined, it is revealed that cyber security knowledge levels are at a sufficient level, and cyber security knowledge levels show significant differences according to gender, age and education.

Purpose of The Research

The aim of this research is to determine the knowledge levels of students in the field of information technologies in vocational high schools regarding personal cyber security. For this purpose, answers were sought for the following sub-objectives.

1. What is the knowledge level of Vocational and Technical Anatolian High Schools Information Technologies students regarding personal cyber security?

2. Knowledge levels of Vocational and Technical Anatolian High Schools Information Technologies students regarding personal cyber security

- ✓ Receiving training on cyber security,
- ✓ Grade levels (10th and 12th grade),
- ✓ Does it differ depending about victimization regarding cyber security?

METHOD

In this section, the research model, sample, data collection tool and data analysis are included.

Research Model

Quantitative method will be used in the research, and the model of the research with its quantitative dimension is designed in the survey model. The survey model is a research model that enables collecting or describing data to test hypotheses or answer questions about the past or current situation of the subject of the research (Karasar, 2010). In accordance with the purposes of the research, singular and relational scanning models were used.

Population and Sample

The population of the research consists of Vocational and Technical Anatolian High Schools with students in the 10th and 12th grades in the field of Information Technologies, located in the central districts of Konya, Karatay, Selçuklu and Meram, in the 2017-2018 academic year. Within the scope of the research, two schools from each region were randomly included in the sample and data was collected from the students in these schools. The determination of 10th graders as participants is due to the fact that the students chose the field of Information Technologies when they passed the 10th grade and have not yet taken vocational courses. The reason for determining the 12th grade is that they have taken all vocational courses. Data was collected from 310 participants by the researcher, 3 scales were left unfinished, 2 scales were deemed invalid because they were marked as a single option, and as a result, the data of 305 participants were evaluated.

Data Collection Tool

The Personal Cyber Security Ensuring Scale developed by (Erol, Şahin, Yılmaz, & Haseski, 2015) was used to collect data in the study. The scale, developed with 810 users, consists of 5 factors and 25 items. The relevant items consist of expressions in the form of 5-point Likert. While the Cronbach Alpha value for the reliability of the scale is expressed as .735, this value for the research was calculated as .828.

Analysis of Data

In addition to descriptive statistics (arithmetic mean, standard deviation, percentage, frequency) in the analysis of the data, the independent sample t test was used to determine the difference between groups. To interpret

students' views on their level of ensuring personal cyber security, 5-point Likert items were scored in three equal ranges as low, medium and high, 1.00 - 2.33 for low, 2.34 - 3.66 for medium, and 3.67 - 5.00 for a high level of cyber security knowledge. It was commented that the level of SPSS 22.0 (Statistical Package for the Social Sciences) package program was used in the statistical analysis of all data, and the significance level was taken as .05.

RESULTS

The findings from the research are given below.

Students' Knowledge Levels Regarding Personal Cyber Security

To find out the students' knowledge levels regarding personal cyber security, data was collected from the participants with a scale form. The analysis results of the data obtained from 305 students are given below (Table 1).

Table 1: Students' Knowledge Levels Regarding Personal Cyber Security

Factors	$\bar{X}$	sd	Level
Protecting Personal Privacy	3,77	0,574	High
Avoiding the Untrustworthy	3,61	0,997	Medium
Taking Precautions	3,46	0,852	Medium
Protecting Payment Information	3,46	1,344	Medium
Leave No Trace	3,79	0,733	High
Overall Average	**3,66**	**0,458**	**Medium**

When Table 1 is examined, it was found that the students' general cyber security knowledge level was at a medium level ($\bar{X}$=3.66). In terms of sub-factors, it is high for the dimension of protecting personal privacy ($\bar{X}$=3.77), medium for the dimension of avoiding the untrustworthy ($\bar{X}$=3.61), medium for the dimension of taking precautions ($\bar{X}$=3.46), medium for the dimension of protecting payment information ($\bar{X}$=3.46) and they have a high level of knowledge ($\bar{X}$=3.79) for the leaving no trace dimension.

Personal Cyber Security Knowledge Levels of Students According to Their Educational Status

The effect of participants' cyber security training on their personal cyber security knowledge is given statistically in the table below (Table 2).

Table 2: Personal Cyber Security Knowledge Levels of Students According to Their Educational Status

	Education Status	f	$\bar{X}$	Sd	df	t	p
Cyber Security Knowledge Level	I received training	61	3,77	0,524	303	2,067	0,040*
	I did not receive training	244	3,64	0,438			

* p<.05

When Table 2 is examined, there is a significant difference in the students' general cyber security knowledge levels ($t_{(303)}$=2.067; p<.05) according to their cybersecurity training status. Based on this analysis, it can be said that the general cyber security knowledge level of students who received cyber security training ($\bar{X}$=3.77) is higher than the students who did not receive it ($\bar{X}$=3.64).

Personal Cyber Security Knowledge Levels of Students by Grade Levels

The effect of the participants' grade levels on their personal cyber security knowledge levels was examined and the findings are shown in Table 3.

Table 3. Personal Cyber Security Knowledge Levels of Students by Grade Levels

	Grade Levels	f	$\bar{X}$	Sd	df	t	p
Cyber Security Knowledge Level	10^{th}	181	3,64	0,456	303	-,998	,324
	12^{th}	124	3,69	0,462			

* p<.05

When Table 3 is examined, there is no significant difference in the general cyber security knowledge levels of the students according to their grade levels ($t_{(303)}$=-0.998; p>.05). There is no statistically significant difference between the average scores of 10^{th} grade students ($\bar{X}$=3.64) and the average scores of 12^{th} grade students ($\bar{X}$=3.69) in the personal privacy protection dimension.

Personal Cyber Security Knowledge Levels of Students According to Cyber Victimization Situations

The impact of students' cyber victimization on their personal cyber security levels was examined and the findings are given in Table 4.

Table 4. Examining the Difference According to Cyber Victimization Situations

	Cyber Victimization	f	$\bar{X}$	Sd	df	t	p
Cyber Security Knowledge Level	I experienced	43	3,64	0,492	303	-0,912	,319
	I didn't experience	262	3,67	0,453			

* p<.05

According to the developments in Table 4, there is no significant difference in general cyber security knowledge levels (t(303)= -0.912; p>.05) according to the situations of experiencing cyber-attack situations. There is no significant difference between the duration of personal privacy protection and the average scores experienced by cyber victimization ($\bar{X}$=3.64) and the average scores experienced ($\bar{X}$=3.87).

RESULTS AND DISCUSSION

As a result of the research, it was revealed that the students' general cyber security knowledge levels were at a medium level. In the study conducted by Tekerek and Tekerek (2013) on the information and computer security awareness levels of primary and high school students, it was found that the students' information security awareness levels were at a sufficient level. It seems that this inference is in line with the inference we made. When examined in terms of sub-dimensions, it is seen that they have a medium level of knowledge in the dimensions of avoiding the untrustworthy, taking precautions and protecting payment information. It has been determined that they have a high level of knowledge in terms of protecting personal privacy and leaving no trace. Liu et al. (2022) state that cyber security threats are an important problem of our age. The fact that the knowledge awareness of students, especially those studying in the field of informatics, is relatively low can be expressed as an important deficiency in terms of their professional lives.

When the findings were analyzed in terms of their cyber security training, it was seen that 20% of the students had received cyber security training. It was concluded that the general cyber security knowledge levels of students who received cyber security training were higher than those who did not receive cyber security training. Şahinaslan et al. (2009) in the study on information security awareness training, the conclusion that information security awareness activities to be carried out to individuals will make great contributions to ensuring information security also supports this inference. In the study conducted by Öğütçü (2010), it was concluded that the protective behavior score of the group that received security training was higher than the group that did not receive security training, thus clearly showing that the training increased awareness in individuals. This result seems to be in line with our result. In light of the findings, it can be stated that cyber security education provides meaningful changes in students' cyber security awareness.

In terms of the grade level variable, there is no significant difference between the cyber security knowledge levels of 10th and 12th grade students. This result can be interpreted as the Information Technologies courses taken by students in the 10th and 11th grades do not contribute to their cyber security knowledge levels. In the study conducted by Bostan and Akman (2011), it was stated that as age increases, sensitivity about computer security decreases and awareness about web security increases. It can be said that these two opposite results balance each other in the context of general cyber security knowledge level, and therefore no difference occurs. In the study conducted by Budak (2015) on the cyber crime awareness of informatics students in vocational high schools in Erzurum, it was concluded that there was no significant difference between the type of class and the students' perception of cyber crimes, their comfort level on the internet and the level of precautions they took on the internet. It seems that this result is in line with the research conclusion.

When the findings are examined in terms of cyber victimization, it is seen that 262 students who participated in the study did not experience cyber victimization, while 43 students did. In addition, it was observed that cyber security knowledge levels did not differ according to the situations of experiencing cyber victimization. This result shows that students who experience cyber victimization do not make an effort to improve their personal cyber security or take precautions on the internet. In the study conducted by Budak (2015), it is stated that students' exposure to any cyber attack does not change their awareness of cyber crimes. On the other hand, Slonje et al. (2013) stated that individuals who were exposed to cyberbullying were more careful regarding their subsequent information technology experiences. Based on this, the conclusion that people who are victims of cyber victimization will take more precautions than others differs from our first conclusion. This difference may be due to the fact that people who have been cyber victimized do not know how to change their information technology usage behavior after being victimized because they do not have sufficient cyber security knowledge. Additionally, Ghelani (2022) states that target audience characteristics are also important in cyber security. With this conclusion, the importance of cyber security training emerges once again.

RECOMMENDATIONS

As a result of the research, the following recommendations can be made. Students studying in the field of Information Technologies must have the highest level of cyber security knowledge in order to be individuals who use technology the most and to be individuals who will produce and develop these technologies. It may be recommended to provide training to students to both raise awareness and take precautions about cyber security. As a matter of fact, it was concluded that the awareness of the individuals receiving training was high. On the other hand, needs analysis can be conducted through qualitative research that will determine students' cyber security levels. Additionally, research can be conducted to determine how students' awareness of cyber security education is reflected in their projects.

REFERENCES

Alqahtani, M. A. (2022). Cybersecurity awareness based on software and e-mail security with statistical analysis. Computational Intelligence and Neuroscience, 2022.

Bostan, A., & Akman, İ. (2011). Bilişim güvenliği: kullanıcı açısından bir durum tespiti (IT security: a due diligence from the user's perspective). IV. Ağ ve Bilgi Güvenliği Sempozyumu, 51-56.

Budak, Ö. S. (2015). Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği. Yüksek Lisans Tezi, Atatürk Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD, Erzurum.

Budak, Ö. S. (2015). Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği (Cyber Crime Awareness of Informatics Students: Example of Vocational and Technical High Schools in Erzurum Province.). Yüksek Lisans Tezi, Atatürk Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD, Erzurum.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme (A review of information, information security and processes). Politeknik Journal, 9(3), 165-174.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4 (10), 13–21.

Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Personal cyber security provision scale development study kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. Journal of Human Sciences, 12(2), 75-91.

Ghelani, D. (2022). Cyber Security in Smart Grids, Threats, and Possible Solutions. Authorea Preprints.

ISCTurkey. (2018). Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (International Conference on Information Security and Cryptology.). https://www.iscturkey.org/index.html adresinden 16.03.2020 tarihinde erişilmiştir.

Karacı, A., Akyüz, H. İ., ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. Kastamonu Eğitim Dergisi, 25(6), 2079-2094.

Karasar, N. (2010). Bilimsel Araştırma Yöntemi: Kavramlar, İlkeler, Teknikler. Ankara: Nobel Yayın Dağıtım.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology, 13, 927398.

MEB. (2011). Bilişim Teknolojileri Alanı Çerçeve Öğretim Programı. Ankara: Milli Eğitim Bakanlığı.

MEB. (2018). 2023 Eğitim Vizyonu Belgesi. Milli Eğitim Bakanlığı.

MEGEP. (2018). Bilişim Teknolojileri Alanı 10.Sınıflar İçin Çerçeve Öğretim Programı. http://meslek.eba.gov.tr/?p=Ogretim-Programi&tur=mem&sinif=10 , adresinden 15.03.2020 tarihinde erişilmiştir.15.03.2019

Öğütçü, G. (2010). E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi. Unpublished Master's Thesis, Başkent Üniversitesi, İstatistik ve Bilgisayar Bilimleri ABD, Ankara.

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in human behavior, 29(1), 26-32.

Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. Akademik Bilişim, 9, 189-194.

Tekerek, M., & Tekerek, A. (2013). A Research on Students' Information Security Awareness. Turkish Journal of Education,, 2(3), 61-70.

USGS. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Zeybek, G. (2011). Bilgisayar Meslek Dersi Alan Ortaöğretim Öğrencilerinin Bilişim Teknolojilerini Kullanımlarının Etik Açıdan Değerlendirilmesi. Yüksek Lisans Tezi, Selçuk Üniversitesi, Eğitim Programı ve Öğretimi Bilim Dalı, Konya.