Teachers' Knowledge Levels About Virtual Information Security

Songül Karabatak
Department of Informatics
Fırat University
Elazig, Turkey
skarabatak@firat.edu.tr

Murat Karabatak
Department of Software Engineering
Fırat University
Elazig, Turkey
mkarabatak@firat.edu.tr

***Abstract*— In this study, it was aimed to determine the level of knowledge about the threats of teachers' virtual information security and the precautions to be taken against these elements. The sample of the study carried out in the survey model was composed of 135 teachers who were selected by the method of unstructured element sampling among the teachers working in the high school in Elazığ province center. The Information Security Achievement Scale was used as a data collection tool. Mean, percentage and frequency techniques and t test were used to analyze the data. It has emerged that most teachers in the study are not aware of the threats to the information in the virtual environment and do not know the precautions to be taken against to the attacks or threats to information security. Teachers' knowledge levels regarding threats and precautions related to information security differed significantly according to gender variables. At the end of the study, some suggestions were made about the security of virtual information.**

Key Words — virtual information; information security; information security threats, information security measures

I. INTRODUCTION

"Protecting people from the troubles that happen is only possible with knowledge. Without knowledge, they should treat themselves with knowledge. Use time well, protect it by knowing. Knowledge protects time. A person who knows, will not waste his time"[1]. This phrase in "Kutadgu Bilig" is an indication of how valuable the information is for both individuals and institutions. Because information is the most important source of intellectual capital for individuals and the competition environment for institutions, and it is the strongest having and using knowledge. Today, information and communication technologies (ICT) enable faster and easier access to information. Thanks to these technologies, people can exchange information with each other in a virtual environment synchronously or asynchronously.

ICT causes a number of problems as well as the benefits and facilities it provides. For example, the creation of unreal information and its rapid spread; illegal or harmful information can be easily accessed by individuals of all ages, and this information can adversely affect personal development and personality disorders; the difference between virtual and reality can not be distinguished so much and leads to the acquisition of bad habits. Therefore, the generation of accurate information and content and their protection is of vital importance. Protecting the accurate information will prevent both complexity of information use, corruption and abuse; as well as the protection of the rights of those who obtain it by an informed effort [2]. This may also be possible through the provision of information security.

Information security is a measure that prevents unauthorized access, use, modification, disclosure, removal, manipulation and damage of information. Information security comes in three main elements: privacy, integrity and accessibility. Privacy is the protection of information from unauthorized persons and protection against unauthorized access, integrity is that information is not changed by unauthorized persons, and accessibility also means that information can be accessed and used when authorized personnel are needed [3-4]. Information security is the period in which information is transmitted securely without modification and without being compromised by others until the sender reaches the recipient in an environment where access to information does not encounter any problems [1, 5,6].

Thanks to the changes in the risks and threats in the virtual environment, the security of information becomes more difficult and complicated. The hiding of personal and corporate information in a virtual environment arouses malicious people and threats other users and allows them to be exposed to various attacks. Increasing use of virtual social networks and e-commerce increases concern about the protection of personal data [7, 8]. Viruses, trojans, spyware, spam, exploits, keyloggers, operating system vulnerabilities, user account exploits, shares and services, and browser vulnerabilities are the most important threats to information on devices with internet access [9].

Recently, seizing bank and card information, plagiarism, obscenity, child abuse, theft of personal information and illegal publications on the Internet are among the most common information crimes in our country, and the most important source of these problems is the inability to protect the information in the virtual environment [10, 11]. Information security is in fact a security chain that is active in all processes from the time the information is acquired to the time it is destroyed, and everybody who takes part in the processing of information is responsible for certain measures [8]. The weakest ring of this security chain has always been people [12]. Information security awareness has been applied by participants from different occupational groups in one of the

978-1-5386-3449-3/18/$31.00 ©2018 IEEE

related studies, and the level of awareness of teachers has not been different from other occupational groups [5]. The Ministry of National Education (MoNE) conducted the National Education Development Project and the Opportunity Increase and Technological Improvement Movement Project (OITIM-FATIH) on the integration of education technology.

Teachers carry out all the tasks from the personalization process to the education system through ICT. It also transforms the exams and course content into electronic form when transferring to virtual venues and often uses ICT intensively for all these transactions [13]. With this study, it is aimed to determine the knowledge levels about the attacks or threats that teachers may encounter in using or storing in virtual environments and the measures to be taken against these threats, which are very important in education and training process.

II. METHOD

A. Research Model

Research is a descriptive study using the survey model. It is aimed to determine an existing situation in the survey model [14].

B. Universe and Sampling

The universe of the research consists of teachers who work in the high schools in Elazığ province center in 2017-2018 academic year. The opinions of the teachers were taken by the method of disproportionate element sampling. Disproportionate element sampling is the type of sampling in which all elements in the environment have the chance of equal selection [14]. 135 teachers, were interviewed for the research. 42,2% (n = 57) of teachers are women (n = 78) and 57,8% of them are men.

C. Data Collection Tool and Analysis

In descriptive studies, one of the methods of gathering data is usually preferred, such as observation, questionnaire, interview or test. Survey method was used in this study. For this reason, Information Security Achievements (ISA) Scale, which was compiled as a 5 point likert type scale by Erdoğmuş [1] was used. The scale was compiled using the questions on the scales used by the Öğütçü [15], Mart [5] and Tekerek and Tekerek [16]. Scale has been occurred two dimensions: Threats and Precautions. The Cronbach's Alpha score, which is the coefficient of confidence for the generalized items for the scale, was calculated as 0,91. In this study, this value was calculated as 0,95. According to this value, it can be said that the scale used is reliable.

Descriptive analysis was used in the analysis of the data and analyzes were done through the SPSS 22 program. Frequency, percentage, arithmetic mean and standard deviations were calculated, and t test was used to determine whether there was a significant difference between women's and men's knowledge levels. Interpretation of arithmetic mean 1,00 to 1,79 as "disagree strongly", 1,80 to 2,59 as "disagree"", 2,60 to 3,39 as "somewhat agree or disagree", 3,40 to 4,19 as "agree" and 4,20 to 5,00 as "agree strongly" with the criteria [17]. Interpretation of scales was not enough, mean scores of 3,39 and below were insufficient, and mean scores of 3,40 and above were found to be sufficient information level.

III. FINDINGS

This section includes findings of the analysis of collected data. Frequency and percentage distributions and arithmetic mean and standard deviation values are used when the results are tabulated.

A. Findings related to Information Security Threats

The level of knowledge about teachers' threats to information security was taken through the Threats dimension of the scale. Findings for each item of the Threats dimension are seen as in Table 1.

As seen in Table 1, most of the teachers say that they *strongly disagree* to expressions in all items of Threat dimension. For "I know how to prevent spyware from installing on my computer" expression 46,7% of teachers said they *strongly disagree* and 5,2% of them also said they *strongly agree*. For "I know how to act to avoid social engineering attacks" expression 45,2% of the teachers stated that they *strongly disagree*, and 6,7% of them said they *agree*.

TABLE I. FINDINGS OF THE TEACHERS' KNOWLEDGE LEVEL ON THE INFORMATION SECURITY THREATS

Threats		Disagree Strongly	Disagree	Somewhat Agree or Disagree	Agree	Agree Strongly	Ave	sd
1- I know what counterfeit virus protection software is.	f	47	10	46	18	14	2,57	1,36
	%	34,8	7,4	34,1	13,3	10,4		
2- I know the security precautions to be taken against identity theft	f	44	16	29	30	16	2,69	1,43
	%	32,6	11,9	21,5	22,2	11,9		
3- I know how to prevent spyware from installing on my computer.	f	63	19	29	17	7	2,16	1,28
	%	46,7	14,1	21,5	12,6	5,2		
4- I know the security measures against malware (malware)	f	54	26	25	14	16	2,35	1,4
	%	40,0	19,3	18,5	10,4	11,9		
5- I know how to act to avoid social engineering attacks	f	61	22	31	9	12	2,18	1,32
	%	45,2	16,3	23,0	6,7	8,9		
6- I can understand if my computer is spyware	f	57	21	28	12	17	2,34	1,42
	%	42,2	15,6	20,7	8,9	12,6		
7- I can understand if the computer is infected with malicious code	f	59	22	26	14	14	2,27	1,39
	%	43,7	16,3	19,3	10,4	10,4		
Threats Dimension							2,37	1,11

As seen in Table 1, the mean of the items in the Threat dimension (Ave = 2,37) is at the level of *disagree*. "I know how to prevent spyware from installing on my computer" (Ave = 2,16) and "I know how to avoid social engineering attacks" (Ave = 2,18) expressions have the lowest average level at the level of *disagree*. "I can understand if the computer is infected with malicious code" (Ave = 2,27), "I can tell if my computer is spyware" (Ave = 2,34) and "I know the security measures against malware" = 2,35) are the other expressions at the level of *disagree.* "I know the security precautions to be taken against identity theft" (Ave = 2,69) at the level of *somewhat agree or disagree* and "I know what counterfeit virus protection software is" (Ave = 2,57) at the level of *disagree* have the highest average in the Threats dimension.

In general, it is seen that both the Threats dimension mean and the mean of any item are not higher than 3,39. This situation can be interpreted as the knowledge level of teachers on the threats toward virtual information is at inadequate level.

B. Findings related to Precautions to be Taken against Threats

Teachers' level of knowledge on the precautions they have taken against the threats was taken through the Precaution dimension of the ISA Scale. Findings related to the analyzes are as in Table 2.

As seen in Table 2, 35,6% of the teachers stated "I know how to use the virus protection software used in information systems", 33,3% of them stated "I know things that need to be paid attention to providing physical security for mobile devices" and 34,1% of them stated "I use the real-time protection feature of my computer's virus protection software" at the level of *strongly disagree.* 25,9% of them stated stated "I know the things to be aware of when using USB drivers" and 25,9% of them stated "I know things to pay attention to about data security for portable devices" at the level of *somewhat agree or disagree*. 26,7% of them stated "I can provide automatic update of my computer's virus protection software" at the level of *agree.*

When examined individually items, while "I can provide automatic update of my computer's virus protection software" (Ave = 3,18), "I know the things to be aware of when using USB drivers" (Ave=3,11), "I know things to pay attention to regarding data security for portable devices" (Ave=2,92), "I use the real-time protection feature of my computer's virus protection software" (Ave=2,70), "I know things that need to be paid attention to providing physical security for mobile devices" (Ave=2,62) expressions are at the level of *somewhat agree or disagree,* "I know how to use the virus protection software used in information systems" (Ave=2,54) expressions are at the level of *disagree.*

In general, the mean of items of Precaution dimension (Ave = 2,85) is at the level of *somewhat agree or disagree*. It is seen that both the dimension mean and the mean of none of the item of the dimension are not higher than 3,39. This can be interpreted as the inadequate level of knowledge regarding the precautions that could be taken against the threats to which the teachers' virtual information would be confronted. This suggests that teachers' knowledge level of precautions against threats is inadequate.

Indepent group t-test was conducted to determine whether the dimensions of the ISA Scale differ significantly according to the gender variable. The findings are shown in Table 3.

TABLE II. FINDINGS OF THE TEACHERS' KNOWLEDGE LEVEL ON PRECAUTIONS TO BE TAKEN AGAINST THE INFORMATION SECURITY THREATS

Precautions		Disagree Strongly	Disagree	Somewhat Agree or Disagree	Agree	Agree Strongly	Ave	sd
8. I know how to use the virus protection software used in information systems	**f**	48	23	27	17	20	2,54	1,45
	%	35,6	17,0	20,0	12,6	14,8		
9. I know things that need to be paid attention to providing physical security for mobile devices	**f**	45	20	32	17	21	2,62	1,45
	%	33,3	14,8	23,7	12,6	15,6		
10. I use the real-time protection feature of my computer's virus protection software	**f**	46	17	26	23	23	2,70	1,51
	%	34,1	12,6	19,3	17,0	17,0		
11. I know the things to be aware of when using USB drivers	**f**	26	18	35	27	29	3,11	1,4
	%	19,3	13,3	25,9	20,0	21,5		
12. I know things to pay attention to regarding data security for portable devices	**f**	31	18	35	33	18	2,92	1,36
	%	23,0	13,3	25,9	24,4	13,3		
13. I can provide automatic update of my computer's virus protection software	**f**	26	20	23	36	30	3,18	1,43
	%	19,3	14,8	17,0	26,7	22,2		
						Precautions Dimension	2,85	1,18

TABLE III. T-TEST RESULTS ACCORDING TO GENDER VARIABLE

Dimensions	Gender	n	Ave	sd	t	df	p
Threats	Woman	78	2,17	1,05	-2,41	133	.02
	Man	57	2,63	1,17			
Precautions	Woman	78	2,62	1,19	-2,62	133	.01
	Man	57	3,15	1,10			

In Threats dimension [$t_{(133)} = 2,41$, $p < .05$] the knowledge level of the teachers showed a significant difference according to the gender variable. Regarding this dimension, men (Ave = 2,63) expressed their opinions at the level of *somewhat agree or disagree* with and women (Ave = 2,17) expressed their opinions at the level of *disagree*. In Precautions dimension [$t_{(133)} = 2,61$, $p < .05$] the knowledge level of the teachers showed a significant difference according to the gender

variable. Regarding this dimension, men (Ave = 2,62) expressed their opinions at the level of *somewhat agree or disagree* and women (Ave = 3,15) expressed their opinions at the level of *agree*. It has been seen that women are less informed about both the threats to information security and the precautions to be taken than men.

IV. Conclusion and Discussion

Most of the teachers expressed their opinion that they do not know the expressions of all items in the Threat dimension of the scale. This can be interpreted as the fact that most teachers are not aware of the attacks or threats to their knowledge in the virtual environment. In the study done by Akgün and Topal [10], the awareness of the teacher candidates about the information security issues is not sufficient; in the study done by Kapanoğlu [18], the level of awareness of the teachers' information security is "moderate" and in the study done by Mart [5] it is seen that they are not enough about the information security issues. The study of personal data security by Çetin [7] has shown that participants use virus protection programs for information security, especially in their personal computers. The researcher 's study also revealed that a large majority of participants were aware that information security was important, but that half were not aware of the latest information security risks. Gökmen and Akgün [19] found that most of the Computer and Teaching Technology Education (CTTE) teacher candidates did not take a course to provide information security, which proved that they were not sufficient in terms of teaching information security issues. The results of the studies carried out in the field and the results of this study coincided with each other.

Findings from the study have shown that teachers partly know the automatic updating and use of real-time protection features of antivirus software, attention to be taken when using USB drivers, and attention to data security and physical security for portable devices. However it has emerged that teachers did not know how to use the virus protection software used in information systems. These findings showed the fact that the teachers do not know the precautions that should be taken against the attacks or threats towards information security.

It was revealed that women have less information about elements that threaten information security than men. This can be interpreted as the fact that women consider threats more than men. Gökmen and Akgün [20] and Yilmaz, Şahin and Akbulut [13] also found that men were more aware of information security than women. However, in the study done by Mart [5], it was concluded that women working in different professions are more aware of the threats they may encounter than men, but that this is the opposite of gender for teachers. This can be explained by the fact that men take more risks in safety issues than women, as stated in the findings of Kınay [20] and Topçu [21].

The most important limitation of this study is that the teachers are not willing to participate in such studies and therefore the view of more teachers is not available. This can be stated in the context of various researches that the teachers are often concerned about their opinions, the intensity of their work or their dissatisfaction with the questionnaires.

V. Recommendations

The most important source of problems in the virtual environment can be stated as the failure to fully secure the personal or institutional information. However, it is necessary to take various precautions in order to reduce these problems. In particular, if these issues concern an institution, it is necessary to develop various policies against potential risks at the institutional level. If it concerns the individual, first of all consciousness-raising activities should be carried out in the society and in the schools regarding the security of virtual information.

Educational institutions are also at the forefront of these institutions. However, when teacher trainings and in-service training activities conducted in large-scale projects implemented by both universities and MoNE in recent years are examined, it is seen that there is no study to talk about the security of information in virtual environments. The various projects, events and competitions to which the public institutions and organizations, the private sector, non-governmental organizations, written and visual media are involved and in which the teachers and administrators will actively take part should be organized under the leadership of MoNE and universities.

Within the scope of the project, OITIM project, which was launched in 2011, has been made very important tenders and distributed to 432 thousand 288 intelligent boarding schools and 1 million 438 thousand tablet students. 432 thousand 288 smart boards were distributed to schools and 1 million 438 thousand tablets were distributed to students. It is also planned to distribute 2 million 700 thousand computers to the 5th and 9th classes and about 200 thousand computers to the teachers in 2018 - 2019 academic year. In this context, it is necessary to keep information to be processed or stored for education should be stored in a safer manner in ICTs which are widely used for education. At this point, MoNE needs to make needs analysis so that they can produce effective solutions to the problems related to information security and to carry out detailed research on the trainings to be prepared.

In the case of in-service trainings to be organized by MoNE, technological leadership competencies should be developed so that school administrators can sensitively approach information security. The digital citizenship of both school administrators and teachers should be improved. This must be ensured to be informed on digital access, digital commerce, digital ethics, digital communication, digital literacy, digital law, digital rights and responsibilities, digital health and digital security issues. They should be ensured to be informed on digital access, digital commerce, digital ethics, digital communication, digital literacy, digital law, digital rights and responsibilities, digital health and digital security issues.

Not only CTTE candidates, but all teacher candidates should be sufficient in terms of teaching information security issues. For this reason, the use of information technologies and

information security training should be given to the prospective teachers especially before their professional career.

Moreover, in this quantitative study, it was tried to determine the knowledge level about threats and precautions related to information security. At the end of the study it was seen that the teachers did not have sufficient knowledge level on both threats and precautions. It will be useful for literature that the qualitative researches should be done on why teachers' gains on information security are low.

REFERENCES

[1] Y. H. Hacip, Kutadgu Biligten Seçmeler (Türk ve Dünya Edebiyatından Seçmeler-1). Işık Publication, 2015.

[2] A. Erdoğmuş, Üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği, Master Thesis, Afyon Kocatepe University, Institute of Natural Science, 2017.

[3] Canbek, G. ve Sağıroğlu, Ş. Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Journal of Dergisi, Vol: 9(3), pp. 165-174, 2006.

[4] NormaTÜRK (2016). Bilgi güvenliği nedir? Ne işe yarar? Bilgi Güvenliği Gelişmeleri. http://blog.normaturk.com/bilgi-guvenligi-nedir/

[5] İ. Mart, Bilişim kültüründe bilgi güvenliği farkındalığı. Master Thesis, Kahramanmaraş Sütçü İmam University, Institute of Natural Science, 2012.

[6] Y. Vural, Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri. Master Thesis, Gazi University, Institute of Natural Science, Ankara, 2007.

[7] H. Çetin, Kişisel veri güvenliği ve kullanicilarin farkindalik düzeylerinin incelenmesi, Akdeniz University, Journal of Faculty of Economics and Administrative Sciences, Vol: 14(29), pp. 86-105, 2014.

[8] T. Henkoğlu, Kişisel verileriniz ne kadar güvende? Bilgi güvenliği kapsamında bir değerlendirme. World of archive, Vol: 18-19, pp. 36-47, 2017. http://dergipark.gov.tr/ad/issue/33457/372372

[9] Ö. Zeydan, Kişisel Bilgisayarlar ve İnternet Güvenliği, XI. Internet in Turkey Conferences, 2006.

[10] Ö. E. Akgün, ve M. Topal, Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya üniversitesi eğitim fakültesi örneği. Journal of Sakarya University Educational Science, Vol:5(2), pp. 98-121, 2015.

[11] Ç. İlbaş ve M. A. Köksal, Türkiye Bilişim Suçları Raporu: 1990-2011 July. Proceeding book of 2nd. International Information Law Congress, İzmir, 2011.

[12] N. Barrett, Penetration testing and social engineering: Hacking the weakest link. Information Security Technical Report, Vol: 8(4), pp. 56-58, 2003.

[13] E. Yılmaz, Y. L. Şahin, ve Y. Akbulut, Öğretmenlerin dijital veri güvenliği farkındalığı. Sakarya University Journal of Education, Vol: 6(2), pp. 26-45, 2016.

[14] N. Karasar, Bilimsel araştırma yöntemi. Ankara: Nobel Publishing and Distribution, 2008.

[15] G. Öğütçü, E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı Ve Farkındalığının Analizi, Master Thesis. Başkent University, 2010

[16] M. Tekerek, ve A. Tekerek, Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. Turkish Journal of Education, Vol: 2(3), 2013.

[17] B. Şahin, Seyahat acentalarının pazarlama faaliyetlerinde etik karar verme süreci: İstanbul Örneği, Balıkesir University, Institute of Social Sciences, Phd Thesis, Balıkesir, 2011.

[18] G. Kapanoğlu, Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi. Master Thesis, Gazi University, Institute of Educational Science, Ankara, 2016.

[19] Ö. F. Gökmen ve Ö. E. Akgün, Bilgisayar ve ögretim teknolojileri egitimi ögretmen adaylarinin bilisim güvenligi bilgilerinin çesitli degiskenlere göre ıncelenmesi. Çukurova University. Journal of Educational Faculty, Vol: 44(1), pp. 61-84, 2015.

[20] H. Kınay, Lise öğrencilerinin siber zorbalık duyarlılığının riskli davranış, korumacı davranış, suça maruziyet ve tehlike algısı ile ilişkisi ve çeşitli değişkenler açısından incelenmesi. Master Thesis, SakaryaUniversity, Institute of Educational Sciences, Sakarya, 2012.

[21] Ç. Topcu, The Relationship Of Cyberbullying to Empathy, Gender, Traditional Bullying, Internet Use and Adult Monitoring. Master Thesis. Middle East Technical University, Institute of Social Science. Ankara., 2008.