

Information Security Awareness of Academic Staff Members: An Example of Eastern Mediterranean University School of Computing and Technology

Mustafa Ilkan, Ersun Iscioglu, Fuat Egelioglu, Alper Doganalp

Abstract—This study investigated the extent of information security awareness of the Eastern Mediterranean University (EMU) School of Computing and Technology (SCT) academic staff, to what extent they fulfill information security practices, and what their attitudes towards information security awareness and practices are. The study was designed as a quantitative research. It was concluded as a result of the study that information security awareness of staff members are high, they fulfill information security practices, and their attitude towards information security awareness and practices are high. Moreover, it was also determined in the study that academic staff have trouble in the following issues; being aware of the institutions policies they most commonly work with, password management, information storage and the safe dispose of information.

Index Terms—Information security, Information security awareness, Information security practices, Attitude towards information security awareness and practices, Quantitative research.

I. INTRODUCTION

RAPID developments experienced in information and communication technologies have recently affected the whole world. Information and communication technologies undertake the key role in ensuring that individuals access information sources rapidly and dissemination of information. Processing, storing and accessing, whenever desired, has become considerably easy in the electronic environment of today's world [1]. As a return of this development, individuals, institutions and enterprises in the society have started to perform most of their works in the electronic environment [2]. Therefore, popularity of electronic environment has increased and it started to take a significant place in the daily life of individuals. Moreover, developing technology enables individuals to store and process large amounts of information in small devices [3]. As a consequence, the development of technology has accelerated the increase in "information" during the greatest part of the century in people's life and enabled the emergence of changes in the life styles of people.

M. Ilkan, *School of Computing and Technology, Eastern Mediterranean University, Famagusta, N.Cyprus. mustafa.ilkan@emu.edu.tr*.
E. Iscioglu, *School of Computing and Technology, Eastern Mediterranean University, Famagusta, N.Cyprus. ersun.iscioglu@emu.edu.tr*.
F. Egelioglu, *Department of Mechanical Engineering, Eastern Mediterranean University, Famagusta, N.Cyprus. fuat.egelioglu@emu.edu.tr*.
A. Doganalp, *School of Computing and Technology, Eastern Mediterranean University, Famagusta, N.Cyprus. alper.doganalp@emu.edu.tr*.

Developments experienced in information and communication technologies mentioned above ensured individuals to access, store, process and carry information easily. However, these developments have also caused another significant fact gained currency. This fact is "information security". With a general expression, information security is described in terms of confidence, integrity and accessibility [4]. Therefore, it is possible to mention about a number of issues threatening the security of information (e.g. human faults, theft, sabotage etc.) in an environment the concepts of confidence, integrity and accessibility are deficient or do not exist [5]. Researchers all over the world continuously carry out studies and propose innovations to the above agenda. However, one of the most important issues which should not be disregarded here is human the factor. Even though there are well developed and designed security systems, humans are located in the center of each security system [6], [7]. In other words, the human is the most significant part of security systems [6]. The human factor is as important as the technology factor in security. It is even possible to say that these two factors are equally important [3].

Most frequently experienced security incidents in 2008 were determined respectively as virus, internal abuses, computer theft and unauthorized access [3], [8]. A decline which can be considered significant was determined as experience of possible threats during the period of 1999-2008 through awareness efforts and security technologies used [3], [8]. The way of to be protected from the factors created in information security is possible by raising awareness of information security in people before making an excessive investment in technologies [3].

Therefore, awareness in individuals about risks and threats that may occur against information security has a great significance. Lack of awareness in people about such risks and threats may cause financial damage in themselves and even the institutions they are depended and harm in their information [9].

Raising awareness of individuals in risks and threats or making them conscious is only possible by educating them. At

this stage, educational institutions, especially universities and academics working in universities have great missions. Academics have responsibility about bringing the required awareness to their students and institutions in the short term and in the whole society in the long term. The extent of knowledge, competence and awareness of academicians is so significant at this point. It is an undeniable reality that anyone not being aware of information security cannot be effective in informing other persons. The current situation should be determined and activities to carry the current situation further should be carried out before holding any study in this subject. The awareness level of academicians who are considered as having an effective role in the issue of raising awareness in their students, institutions and society regarding the information security should be primarily determined.

II. PURPOSE OF THE STUDY

As mentioned before, determination of awareness of academic staff is considered as the first step to carry our upper level studies. Therefore, the fundamental aim of the study was determined as to determine awareness of Eastern Mediterranean University (EMU), School of Computing and Technology (SCT) academic staff. The answer for the question “what is the extent of the EMU SCT academic staffs’ information security awareness, information security practices and attitudes towards information security awareness and practice?” will be investigated.

III. METHOD

The study was dealt with within the framework of quantitative research. Information Security Awareness (ISA) Survey developed by Ryan in 2006 [10] and adapted by Nyabando in 2008 [11]¹ was used as the tool of data gathering in the study. ISA survey data gathering tool is a 4 point likert scale composed of total 31 items except the items orienting to determine demographic characteristics. The survey adapted is composed of three sub scales. These are [11]:

a. User information security awareness scale (Questions from 7 to 15)

b. Information security practice scale (Questions from 16 to 32), and

c. User attitudes towards information security scale (Questions from 33 to 37).

EMU SCT academic staff constitutes the population of the study. A sample was not taken in the study and the whole population was studied on. Therefore, the study was restricted with the academic staff (full time or part time) serving in EMU SCT in the 2008-2009 spring semester.

The data obtained from ISA survey was analyzed by SPSS 16.0 program in the computer environment in the study. The data obtained was dissolved by using percentage (%), frequency (f) and mean (M).

¹ ISA survey adapted by Nyabando (2008) was used in the study. Demographic characteristics part of the survey adapted by Nyabando (2008) was some items re-adapted according to the study universe. Moreover, the item related with FERPA (Family Educational Rights and Privacy Act) existing in the survey was removed from evaluation since it is not related with individuals in scope of the study.

IV. FINDINGS

Findings obtained as a result of the study are explained under the titles of findings relating to (concerning) participants, information security awareness of participants, information security practices of participants and attitudes of participants towards information security awareness and practices.

A. Findings related to participants

Allocation of individuals participating in the study according to their demographic characteristics is given below in Table 1, Table 2 and Table 3. Allocation of participants according to gender and age is given in Table 1, Year of computer usage and position of participants in the university are given in Table 2, and daily ratio of computer and internet usage of participants in the campus is given in Table 3.

Table 1. Allocation of participants according to gender and age

Participants:		N	%
Gender	Female	25	55.6
	Male	20	44.4
	Total	45	100
Age	20-24	3	6.7
	25-29	8	17.8
	30-34	9	20.0
	35-39	7	15.6
	40-44	3	6.7
	45-49	6	13.3
	50-54	5	11.1
	55-59	2	4.4
	60-64	1	2.2
	Over 64	1	2.2
	Total	45	100

As it is also seen in Table 1 above, total of 45 individuals composed of 25 female and 20 male participated in the study. Allocation of participants according to ages is also given in Table 1. It is seen that the great majority of individuals participating in the study are aged between 25 - 39 (53, 4 %).

Table 2. Allocation of participants related to year of computer usage and current position in the university

Participants:		N	%
Computer Usage	Less than 1 year	1	2.2
	6-10 Years	4	8.9

11-15 Years	9	20.0
16-20 Years	17	37.8
Over 20	14	31.1
<i>Total</i>	<i>45</i>	<i>100.0</i>

Positions in the University	Full Time	39	86.7
	Part Time	6	13.3
	<i>Total</i>	<i>45</i>	<i>100.0</i>

As it is seen in Table 2, great majority of individuals (38.9%) participating in the study have used computer for more than 16 years. 39 of the participants of the study work in EMU SCT as a full time instructor or full time assistant, 6 work as a part time instructor or part time assistant.

Table 3. Allocation of participants related to daily ratio of computer and internet usage in the campus

Participants:	N	%	
Average Daily Computer Usage (on-campus)	Less than 1 hour	3	6.7
	1-2 Hours	8	17.8
	3-4 Hours	18	40.0
	5-6 Hours	14	31.1
	7-8 Hours	1	2.2
	More than 8 hours	1	2.2
	<i>Total</i>	<i>45</i>	<i>100</i>
Average Daily Internet Usage (on-campus)	Less than 1 hour	4	8.9
	1-2 Hours	18	40.0
	3-4 Hours	14	31.1
	5-6 Hours	4	8.9
	7-8 Hours	4	8.9
	More than 8 hours	1	2.2
	<i>Total</i>	<i>45</i>	<i>100</i>

Table 3 indicates daily ratio of computer and internet use of participants in the campus. It is seen that the great majority of the participants (61.1%) use a computer about 3-6 hours daily in average. Moreover, as it is also seen in Table 3, the great majority of participants (61.1%) use the internet for about 1-4 hours daily in average.

B. Information security awareness of participants

9 items between the items 7 and 15 of ISA survey used in the study measures the awareness of information security and safe computing behaviors of the users [11]. Table 4 gives the allocation of participants concerning their information security awareness.

Table 4. Information security awareness of participants

Questions	Not Aware		Somewhat Unaware		Somewhat Aware		Aware	
	N	%	N	%	N	%	N	%
7. I am aware of the requirements and expectations of the computer use policies at my institution	2	4.4	3	6.7	13	28.9	27	60.0
8. I am aware of the impact that a virus can have on my computer system.	-	-	-	-	5	11.1	40	89.9
9. I am aware that virus protection software can identify and remove viruses.	-	-	-	-	6	13	39	86.7
10. I am aware that virus protection software requires frequent updates.	-	-	-	-	5	11.1	40	89.9
11. I am aware that I should keep my passwords secure.	-	-	1	2.2	1	2.2	43	95.6
12. I am aware of the impact of responding to phishing emails.	2	4.4	2	4.4	4	8.9	37	82.2
13. I am aware that it is important to back-up my files.	1	2.2	1	2.2	3	6.7	40	89.9

14. I am aware that encryption can prevent unauthorized access to confidential information. 2 4.4 2 4.4 8 17.8 33 73.3

15. I am aware of the vulnerabilities associated with sharing devices such as files and drives. - - 3 6.7 12 26.7 30 66.7

When the answers given by EMU SCT academic staff for the items related with information security given in Table 4 are examined, it is understood their awareness regarding information security is high. It is possible to say that the participants substantially agree with the items related with awareness included in the survey and they are aware of the issues mentioned in the items. It is observed in Table 4 that awareness of participants related with security policy of the institution they work in has the lowest percentage (60% of the participants are aware of the security policy of the institution they work in). Moreover, the issue with the highest awareness for the participants is that they must keep their password secret (95.6% of the participants are aware that they must keep their password secret).

The mean of answers given by the participants according to awareness sub-scale of the survey are given in table 5.

Table 5. Mean of answers given by the participants of awareness items of ISA survey

Question #	Mean
Q7	3.44
Q8	3.89
Q9	3.87
Q10	3.89
Q11	3.93
Q12	3.69
Q13	3.82
Q14	3.60
Q15	3.60
Total	3.35

The answers given for the information security sub-scale of ISA survey are evaluated as follows; “unaware” 1, “somewhat unaware” 2, “somewhat aware” 3 and “aware” points. It was recognized that average values between 1.00-1.74 shall be evaluated as “unaware”, those between 1.75-2.49 as “somewhat aware”, those between 2.50-3.24 “somewhat aware” and those between 3.25-4.00 as “aware” while mean are interpreted. These intervals including the levels were

obtained by dividing the serial width between the lowest value and highest value given to the options into the number of options (levels).

The mean of the answers given by the participants were calculated as 3.35 in the study. This result indicates that the participants have awareness about information security in general.

C. Information Technology Practices of Participants

14 items between items 16 and 29 of the ISA survey used in the study measure the safe computing behaviors practices of users [11]. Table 6 gives allocation of participants related with their information security practice.

Table 6. Participants’ practice of safe computing behaviors

Questions	Never		Almost Never		Almost Always		Always	
	N	%	N	%	N	%	N	%
16. I log off or lock my computer before I step away from my desk.	6	13.3	7	15.6	12	26.7	20	44.4
17. I log off when I finish using a computer system.	4	8.9	1	2.2	7	15.6	33	73.3
18. When choosing a password, I use a combination of letters, numbers and special characters.	4	8.9	4	8.9	7	15.6	30	66.7
19. I write down my password(s).	19	42.2	12	26.7	5	11.1	9	20.0
20. I share my password(s) with my co-workers.	33	73.3	9	20.0	1	2.2	2	4.4
21. I back-up my files on reliable media.	3	6.7	4	8.9	17	37.8	21	44.7
22. I have antivirus software on my home computer(s).	2	4.4	-	-	8	17.8	35	77.8
23. I keep the antivirus software on my home computer updated.	2	4.4	1	2.2	13	28.9	29	64.4
24. I allow programs to save my usernames and passwords for faster access	19	42.2	12	26.7	10	22.2	4	8.9

in the future.									
25. I download and install programs from the internet as I deem necessary on my work computer.	7	15.6	8	17.8	13	28.9	17	37.8	
26. I protect confidential files with passwords.	8	17.8	10	22.2	9	20.0	18	40.0	
27. I check whether a website is secure or not before making a financial transaction over the internet.	3	6.7	1	2.2	12	26.7	29	64.4	
28. I seek out information about information security.	3	6.7	12	26.7	15	33.3	15	33.3	
29. I open emails regardless of not knowing the sender's identity.	30	66.7	7	15.6	3	6.7	5	11.1	

Table 6 gives practices of safe computing behaviors in individuals participating in the study. According to the answers given, most individuals participating in the study have an antivirus program in their personal computer (77.8%). This is the situation participants agree on at the highest level. Moreover, it was determined that the great majority of the participants do not share their passwords with co-workers (73.3%). According to the evidences obtained, great majority of the individuals participating in the study log off their computer while leave their desk (44.4 % always, 26.7 % almost always), turn off computers after completing their task (73.3 % always), use combinations of letters, numbers and special characters while determining a password (66.7 % always), continuously backup important documents (44.7 % always, 37.8 % almost always), continuously update antivirus program in their home computers (64.4 % always, 28.9 % almost always), protect confidential files with passwords (40.0 % always, 20.0 % almost always), check security of web site before carrying out a financial transaction (64.4 % always, 26.7 % almost always). However, there are also some other results which should not be disregarded. Some of the participants (40%) protect confidential files without passwords (17.8 % never, 22.2 % almost never), download any program they consider required (need) for their computer from the internet (37.8 % always, 28.9 % almost always). Moreover, some number of participants which cannot be underestimated (almost 30%) saves their passwords by writing on a paper.

Three additional questions were directed to learn the practice of participants in the survey used in the study in addition to the above given items. These items are number 30, 31 and 32 items of the ISA survey. Answers of the participants to these items are as follows.

Participants were asked about wireless internet connection at their home in item 30. 31.1% (14 people) of the participants answered this question as safe, 4.4% (2 people) as not safe, 13.3% (6 people) I don't know and 51.1% (23 people) as I don't have wireless internet connection in my home.

The participants asked about the frequency they change their password in item 31. 8.9% (4 persons) of the participants answered this question as when the system asks 4.4% (2 people) as every month, 15.6% (7 people) in every three months or earlier, 13.3% (6 people) as in every six months, and 13.3% (6 people) in every 12 months. However, the most surprising result given to the same item is that remaining 44.4% (20 people) of the participants stated that they have never changed their password for years. This result is actually an indicator showing that academic staff having security awareness in general experiences information deficiency in this issue.

Participants were asked about the way of disposing confidential documents in the item 32. 20.0% (9 people) of the participants answered that they place them in the trashcan, 66.7% (30 people) tear up the documents and place them in the trashcan and 13.3% (6 people) use a shredder.

It can be said about this sub-scale that academic staff takes care about and uses information security practices. However, it is also seen that some number of academic staff even though so little have trouble about the issues of information storage or disposing the information.

D. Attitudes of participants towards information security awareness and practices

The study tried to also determine attitudes of participants towards information security awareness and practices. Attitudes of individuals participating in the study towards safe computing behaviors is determined according to the answers they give for items 32, 33, 34, 35 (total 4 items) of ISA survey [11]. This sub scale of the survey is answered as "strongly disagree", "disagree", "agree" and "strongly agree" [11]. Table 7 gives the information related with attitudes of individuals participating in the study.

Table 7. Attitudes of participants towards information security awareness and practices

Questions	Strongly disagree		Disagree		Agree		Strongly agree	
	N	%	N	%	N	%	N	%
32. I think it is fairly easy to follow secure information security practices.	2	4.4	5	11.1	27	60	11	24.4
33. I believe my actions as a user play a part in	1	2.2	5	11.1	23	52.2	16	35.6

securing computer systems.									
34. I find it easy to keep up with new developments related to information security.	1	2.2	11	24.4	19	42.2	14	31.2	
35. I am reluctant to adapt new technologies until I see the majority of the people around me accept them.	5	11.1	11	24.4	18	40.0	11	24.4	

When the answers of the participants given in Table 7 are examined, it can be said that their attitude related with the item is positive. The participants marked agree and strongly agree options most for the item 33 (52.2 % agree, 35.6 % strongly agree). Therefore, it can be said that the participants consider individuals as a part of security systems.

Mean of the items according to answers of the participants are given in Table 8.

Table 8. Mean of individuals' answers related with attitudes

	Question 32	Question 33	Question 34	Question 35	Total
Mean	3.04	3.20	3.02	2.78	3.01

The answers given for sub-scale of the ISA Survey related with attitudes are evaluated as follows; "strongly disagree" 1, "disagree" 2, "agree" 3 and "strongly agree" 4 points. It was recognized that average values between 1.00-1.74 shall be evaluated as "strongly disagree", those between 1.75-2.49 as "disagree", those between 2.50-3.24 "agree" and those between 3.25-4.00 as "strongly agree" while means are interpreted. It was determined as a result of the study that participants agree the items included in the sub-scale related with attitudes (mean = 3, 01). According to this result, it can be said that attitudes of individuals are positive.

V. CONCLUSION

This study investigated information security awareness, information security practices of EMU SCT academic staff and their attitudes towards information security awareness and practices. As a result of the study, it was determined that information security awareness of EMU SCT academic staff, their status in practicing information security and their attitude towards information security awareness and practices are high. It was determined that the participants have trouble especially in the issues of being aware of policies of the institutions they work with, password management, information storage and dispose of information in a right way (or safely).

It is possible to remove (or change) these troubles in obtained results very rapidly. For example, it is possible to

remove troubles of SCT staff with short term education practices.

Another reason why these results obtained related with the participants are such positive may result from their situation of being SCT staff. SCT staff always performs computer teaching and make researches by nature of their duty. Therefore, this situation may affect their awareness positively. Additionally, such researches should be applied throughout the whole university and efforts should be taken to remove (or change) failures.

ACKNOWLEDGMENT

We would like to thank to all of the School of Computing and Technology staff.

REFERENCES

- [1]. Y.Vural and S.Sagioglu, "Kurumsal Bilgi Guvenligi: Guncel Gelismeler". 2007. 3rd Information Security and Cryptology Conference. Available: <http://www.iscturkey.org/2007/pdf/sozlu/27.pdf>.
- [2]. S.Sagioglu, E.Ersay, and M.Alkan, "Bilgi Guvenliginin Kurumsal Bazda Uygulanmasi". 2007. 3rd Information Security and Cryptology Conference. Available: <http://www.iscturkey.org/2007/pdf/sozlu/28.pdf>
- [3]. E.Sahinaslan, A.Kantirk, O.Sahinaslan, E.Borandağ, "Kurumlarda Bilgi Guvenligi Farkindaligi, Onemi ve Olusturma Yontemleri". 2009. Akademik Bilisim Konferansi. Available: <http://ab.org.tr/ab09/bildiri/95.pdf>.
- [4]. D.B.Parker, "Fighting Computer Crime: A new Framework for Protecting Information". John Wiley & Sons, USA. 1998.
- [5]. L.Drevin, H.A., Kruger, T.Steyn. "Value-focused assessment of ICT security awareness in academic environment". 2007. *Computer & Security*. 26, 36-43.
- [6]. J.J.,Gonzalez and A.Sawicka, "A Framework for Human Factors in Information Security". 2002. WSEAS Int. Conf. on Information Security, Rio de Janeiro. Available: <http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf>
- [7]. M.Bishop, *Introduction to Computer Security*. 2005. Boston: Pearson.
- [8]. R. Richardson, "2008 CSI Computer Crime and Security Survey". Available: <http://i.zdnet.com/blogs/csisurvey2008.pdf>.
- [9]. K.Özenc, "Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Guvenliginin Saglanması". 2007. 3rd Information Security and Cryptology Conference. Available: <http://www.iscturkey.org/2007/pdf/sozlu/26.pdf>
- [10]. J.E.Ryan, "A comparison of information security trends between formal and informal environments". 2006. Doctoral Thesis. ProQuest Digital Dissertations database. Publication No: AAT 3225287. Auburn University.
- [11]. C.J.Nyabando, "An Analysis of Perceived Faculty and Staff Computing Behaviors that Protect or Expose Them or Others to Information Security Attacks". 2008. Doctoral Thesis. East Tennessee State University.

Mustafa İLKAN received his B.Sc. degree in Electrical and Electronic Engineering from Higher Technological Institute in North Cyprus (1984), M.Sc. degree from Middle East Technical University (Ankara, Turkey,1987) and Ph.D. degree from Eastern Mediterranean University (2004). He is currently the director of School of Computing and Technology and teaching in the Electrical and Electronics Technology and Information Technology departments. His research interests include renewable energy resources, environmental problems, electrical circuit analysis, software project management and vocational education.

Ersun ISCIOGLU received the B.Sc. degree in Electrical and Electronic Engineering from the Eastern Mediterranean University, Famagusta, North Cyprus and M.A. degree in Educational Sciences from Eastern Mediterranean University in 2002 and 2005, respectively. He received his Ph.D. degree on Educational Technology at University of Ankara (Ankara, Turkey). He is a Senior Instructor at the School of Computing and Technology of Eastern

Mediterranean University. His research interests include Engineering Education, Vocational Education, Distance Learning, ICT Learning, Learning Technologies, and Computer Education.

Fuat EGELIOĞLU received the BSc degree in Mechanical Engineering from Boğaziçi University, Turkey (1978), MSc degree from Eastern Mediterranean University, North Cyprus (1993) and PhD degree Eastern Mediterranean University, North Cyprus (2002). Assoc. Prof. Dr. Fuat Egelioğlu, started to work as an assistant lecturer at the Higher Technological Institute in 1983. In 1986 he became a lecturer at the Eastern Mediterranean University (EMU). He was employed as a research associate at the Energy Analysis and Diagnostic Center-San Diego State University between 1993-94. In 1995 and 1996 he was a member of the TRNC electricity commission committee. His research interests include Thermal power plant simulation and optimization Thermal system design, Renewable energy, Electrical Energy and Power Load Forecasting, Gas turbines, Desalination.

Alper DOĞANALP received his B.Sc. degree in Electrical and Electronic Engineering from Higher Technological Institute in North Cyprus (1984), M.Sc. degree from Istanbul Technical University (Electronics) (Istanbul, Turkey, 1987) and Ph.D. degree from Eastern Mediterranean University (Control Theory, 2005). He is an Asst. Professor in Eastern Mediterranean University-School of Computing and Technology.