ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
DOI: 10.17559/TV-20140403122930

IMPACT OF EDUCATION ON SECURITY PRACTICES IN ICT

Atila Bostan, İbrahim Akman

Original scientific paper
In assuring the security in information technology, user awareness and acquired-user habits are inevitable components, yet they may be qualified as the feeblest ones. As the information technology tries to put its best in providing maximum security, user awareness plays a key-role. Additionally, although the literature provides studies on approaches for teaching information security, there are not many evidences on the impact of education level. Therefore, this study investigates the impact of the education level on user security awareness in using the Information and Communication Technology (ICT) products. For this purpose, a survey was conducted among 433 citizens from different layers of the society. Interestingly, the results indicated that education level has significant impact on all security issues included in the analysis regarding computer usage, web usage and e-mail usage.

Keywords: *Education and ICT security awareness, Education and ICT usage, E-mail security, Computer security, Web security*

Utjecaj obrazovanja na sigurnosne mjere u ICT

Izvorni znanstveni članak
U provođenju sigurnosnih mjera u informatičkoj tehnologiji, svijest i stečene radne navike korisnika neizbježne su komponente. Ipak, može ih se označiti i kao najslabije. Premda informatička tehnologija nastoji činiti najviše što može da bi osigurala maksimum sigurnosti, svijest korisnika o tome je ključna. Uz to, iako se u literaturi mogu naći radovi koji se bave načinima podučavanja sigurnosti u informatici, nema ih mnogo koji razmatraju utjecaj stupnja obrazovanja. Stoga se u ovom radu ispituje utjecaj stupnja obrazovanja na to koliko su korisnici svjesni potrebe primjene zaštitnih mjera pri korištenju proizvoda informatičke i komunikacijske tehnologije (ICT). U tu je svrhu provedeno ispitivanje na grupi od 433 građana, pripadnika raznih društvenih slojeva. Zanimljivo je da su rezultati pokazali kako nivo obrazovanja značajno utječe na pitanja vezana uz provođenje zaštitnih mjera kad se radi o uporabi računala, internetske mreže i e-pošte.

Ključne riječi: *obrazovanje i svijest o sigurnosti ICT, obrazovanje i uporaba ICT, sigurnost računala, sigurnost E-pošte, sigurnost internetske mreže*

1 Introduction

Computer networks have turned into an inevitable technology in developing and enhancing business processes. A large number of firms (even middle, small-sized) are benefiting from computer networks in both their inner process management and customer services dissemination. In parallel with business world, a great deal of precious information for individuals are being processed, transferred and stored in computer networks as well. Computer networks, namely the Internet, provide the most general technical infrastructure for worldwide business and information sharing. Unquestionably, handling business and sharing information in a public environment, such as the Internet network, brings about security problems. Data need to be handled in a secure and trusted method to assure the business confidentiality and privacy. These features are commonly called as network and computer security. Security in digital environments covers the prevention of unauthorized excess/listening, information alteration, and service interruption.

The success of information systems security depends largely on end-user behaviour and awareness [1]. Since security mechanisms are designed, implemented, applied and, at the same time, breached by people, human factors should be considered in their design [2]. As technology endeavours to build its best protection mechanisms in computer and communication security, reported incidents of security breaches each year are still on a constant rise. In the reports of Computer Security Institute [3 ÷ 5], phishing e-mails and web spoofing were reported as the most observed violations and unfortunately, these security breaches primarily make use of user weaknesses. Lack of security awareness in user behaviours is generally attributed as the rationale for most of the security breaks. The literature provides evidences on how to teach information security in formal education [6 ÷ 9] and in specialized courses [10]. Additionally, most of the previous studies focused on the security education and stimulating the security awareness in Information and Computer Engineering education but not in generic engineering or undergraduate education. As for the demographic properties of the users, there are researches pointing out that education level has significant and direct relation with ICT usage patterns [11]. Furthermore, in their studies Andrew and Hubona [12] stated that the Technology Acceptance Model (TAM) [13] should take the education level as an important factor into consideration. A more recent study [14] presented that users with lower levels of education are more likely to be trapped by phishing e-mails. Thus, the effect of education level on secure ICT usage-behaviours still needs to be investigated thoroughly. In parallel with the assertion "to assess the effectiveness of a security mechanism, practices should be scrutinized in real-life rather than in laboratory or experimental settings" [15] since true-life experiences are more important than specialized testing. This means, in order to have a more elaborated assessment on the impact of an education level, one should study the observed behavioural changes.

In the present study, we scrutinized the impact of the education level on user security awareness in ICT usage with the help of the collected data on user real-life security practices as well as their technical awareness on digital security. We have directed a 23 question "information security and awareness" survey on 466 participants. For the purpose of the research, some of the questions were later combined to produce 13 factors to be used in the analyses. We limited the coverage of the

survey with familiarity in general information technology and usage patterns in personal-computer, secure-web and e-mail interactions, since those were generally attributed as the common business and information sharing mediums. Excluding the demographic properties of the participants, the questions in the survey were divided into three groups: real-life practices in computer usage; accustomed-behavioural patterns in secure web usage; and finally, security beliefs and practices in e-mail usage.

Today, the data need to be handled securely to assure confidentiality and privacy in computer networks. Additionally, available studies consider the role of education on ICT security issues in general and they do not provide evidences for different usage patterns in this respect. Therefore, the main contribution of this study is to investigate the role of education in computer security, web security and e-mail security in terms of usage frequency and security awareness so that the reader may have a comparative view of different usage patterns. To the best of our knowledge, it will be the first study of this kind in the literature.

The rest of this paper is organized as follows. In the next chapter, research methodology used in the study is presented along with the hypotheses scrutinized. Following the research design and test method we stated the results found in the study. After interpreting the results in discussion section, conclusion is submitted.

2 Research methodology and hypotheses

For the citizens, ICT technologies can offer a huge range of information and services and the literature reported existence of digital divide within countries [16]. This means the key to use ICT is not technology but the citizens as there are still many people who do not or cannot access to computers and/or internet. This is due to the gap between citizens' attributes including socio-demographic factors, business and geographic areas with regard to both their opportunities to access information and communication technologies (ICTs) and their use of the internet for a wide variety of activities [17]. Some studies investigated the attitude of individuals toward using ICT and the relationships between ICT issues and socio-demographic factors (see for example [18 ÷ 23]). Of these factors education has attracted special interest.

Tarafdar and Vaidya [24] agreed about the impact of education on the ICT issues, and education level forms significant barriers to the adoption of new technologies. Bhatnagar and Ghose [25] supported this view and stated that education has a statistically significant effect on ICT usage behaviour. Additionally, most research findings indicate that the better educated use the Information Technology (IT) for diverse tasks [26]. With this backdrop, education may be taken as one of the key elements in ICT security issues which covers computer, web and communication (i.e. e-mail) securities. Therefore, the present study mainly performs a systematic analysis to investigate the impact of independent (decision) variable education level on security issues in using computers, web services and e-mail. The research model was developed to find an answer to the following main question: Does education level have an impact on the usage frequency and security awareness for computer, web and e-mail?

For this purpose the dependent variables were categorized into three empirical factors: (i) Computer usage and security, (ii) Web usage and security, and (iii) E-mail usage and security. The corresponding hypotheses are provided below.

Computer usage and security

Hyp.	Definition
$H1_1$	Higher levels of education result in higher levels of computer usage.
$H1_2$	Higher levels of education result in higher levels of awareness in computer security in general.
$H1_3$	Higher levels of education result in higher levels of awareness for security in computer usage routines.

Web usage and security

Hyp.	Definition
$H2_1$	Higher levels of education result in higher levels of web usage.
$H2_2$	Higher levels of education result in higher levels of awareness in web security in general.
$H2_3$	Higher levels of education result in higher levels of awareness for security in web usage routines.

E-mail usage and security

Hyp.	Definition
$H3_1$	Higher levels of education result in higher levels of e-mail usage.
$H3_2$	Higher levels of education result in higher levels of awareness in e-mail security in general.
$H3_3$	Higher levels of education result in higher levels of awareness for security in e-mail usage routines.

3 Research design

A survey instrument corresponding to the proposed hypotheses was developed in the native language (Turkish) of respondents. A pilot instrument was face validated and revised based on suggestions from a group of security professionals. The questionnaire contains 13 items and each item reflects a discrete variable as given in Tab. 1. The proposed independent variable of this study is: "education" whereas the dependent (empirical) variables are "c_usage", "c_awareness", "c_know", "w_usage", "w_ awareness", "w_know", "e_usage", "e_awareness" and "e_know". The respondent was allowed to opt more than one choice for questions 7, 10 and 13. The variables "gender", "age" and "sector" were used for descriptive purposes. The definitions, scales and range of values for these variables are given in Tab. 1.

The respondents were ordinary citizens belonging to different groups in the society since the survey was conducted in big shopping malls in different cities in different days of the week by the young members of Turkish Chamber of Electrical Engineers. "Judgment sampling" was used as the sampling method and participation was voluntary. A total of 466 completed survey questionnaires were received. Thirty three responses were discarded due to the existence of unqualified data, which means 433 responses included in the analysis. Thus, the approximate response rate was

approximately 93 % which can be considered acceptable for the purpose of this study [27].

Table 1 Summary of research questions and variables

#	Variable	Definition	Range of values
1	gender	What is your gender?	male, female
2	age	What is your age?	<21, 21-30, 31-40, 41-50, 51-60, >60
3	sector	What is the sector of your organization?	private, public, not working (retired/student/ unemployed/ etc)
4	education	What is your education level?	graduate/undergraduate/ others,
5	c_usage	What is your computer usage frequency?	very high, high, average, little, very little
6	c_awareness	What is your level of awareness on computer security?	very high, high, average, little, very little
7	c_know	What do you do when you observe an attack to your computer?	I have not observed any attack, I use my own resources, I observed the attack but continued to use the computer without any precaution, I inform authorities
8	w_usage	What is your web usage frequency?	very high, high, average, little, very little
9	w_awareness	What is your level of awareness on web security?	very high, high, average, little, very little
10	w_know	Do you know how to differentiate secure web applications?	I cannot differentiate, I verify server SSL certificate details, I confirm the existence of security authority logo, I check SSL connection icon status on status or address bar
11	e_usage	What is your e-mail usage frequency?	very high, high, average, little, very little
12	e_awareness	What is your level of awareness on security attacks via e-mail?	very high, high, average, little, very little
13	e_know	What do you do when you receive an e-mail with security threat?	I clear it, I open it after scanning, I inform responsible person without opening it, first I scan and open it and then clear it and then inform responsible person

4 Test method

Hypotheses ($H1_i$, $H2_i$, $H3_i$; i=1, 2, 3) concerning the impact of education on the usage frequency and level of security awareness for computers, web and e-mail services were tested using ANOVA. Statistical inference techniques are well known and appear in many of the standard text books on probability and statistics (see for example [28 ÷ 30]). Analysis of Variance (ANOVA) is a powerful statistical tool and is used in a wide variety of applications. It has the advantage that no assumption is made about the nature of the relationship between dependent and independent variables. ANOVA can handle categorical data better and, therefore, is normally preferred when the independent variables are categorical [30]. The correlation is used to determine the direction of the relationships between the variables since it is a statistical measure that indicates the degree to which two or more variables fluctuate together. Correlation is positive when two variables develop in the same direction and negative when they move in opposite directions. Furthermore, the chi-square test method [30] is used whenever there is a need to examine the relationship between the dependent and independent variables.

5 Results

The results of the present survey are presented in the following sequence. Initially, the results of the survey are presented using descriptive analysis. This is followed by test results based on the ANOVA analysis for the dependent factor education.

5.1 Descriptive results

The background profile of respondents is provided in Tab. 2. As it can be seen in Tab. 2, respondents were observed to be almost equal in terms of gender (male: 55 %; female: 44 %) in this survey. This is expected since it was conducted in shopping malls where there is no reason for dominancy of any gender. Of the males in the sample, 21 % reported their awareness on computer security to be above average and this percentage for females is 8 %. These percentages for web security are 14 % and 5 %, and e-mail security are 26 % and 28 % respectively. Chi-square test results indicate that there is significant relationship between gender and awareness on computer (Chi-Square = 24,081; DF = 5; P-Value = 0,000) and web (Chi-Square = 14,622; DF = 5; P-Value = 0,012) securities. However, this relationship between gender and awareness on e-mail security categories was not found to be significant (Chi-Square = 9,801; DF = 5; P-Value = 0,081) at 5 % significance level.

Table 2 Profile of respondents

Variable	Number	%
Gender	433	100
Male	239	55
Female	188	44
Unknown	6	1
Age	433	100
<21	91	21
21-30	204	47
31-40	89	21
41-50	40	9
>50	9	2
Education	433	100
Graduate	21	5
Undergraduate	261	60
Others	151	35
Sector	433	100
Private	93	21
Public	76	18
Not working	238	55
Unknown	26	6

The age distribution showed a high percentage for the group of less than 30 years of age (68 %) whereas this percentage for elder people, who are greater than 40 years is only 11 % . This should be considered normal because the percentage of young people visiting shopping malls every day is observed to be high and young people show more interest in responding surveys. Of the young respondents (<30 years of age), 20 % reported their awareness on computer security to be above average and this percentage for elder people (>40 years of age) is 0 %. These percentages for web security are 14 % and 0 %, and e-mail security are 34 % and 0 %, respectively. Chi-square test results indicate significant differences in terms of age versus computer security awareness (Chi-Square = 52,197; DF = 9; P-Value = 0,000), web security awareness (Chi-Square = 97,110; DF = 12; P-Value = 0,000) and e-mail security awareness (Chi-Square = 23,668; DF = 4; P-Value = 0,000) categories.

Graduated participants constitute the biggest ratio in education category whereas most of them reported themselves as not working (66 %). This is expected, since the survey was held in week days and mostly in working hours. Interestingly, most of the graduate participants were found to be working in private sector (46 %). The difference between education level and type of workplace was observed to be significant (Chi-Square = 88,626; DF = 12; P-Value = 0,000). Additionally, education level of males was observed to be higher than females but this difference is significant only in graduate level. Respondents from private sector organizations reported their security awareness above average for computer, web and e-mail as 16 %, 10 % and 26 % , respectively. These percentages for public sector employees are observed to be 12 %, 5 % and 16 % respectively. Public sector employees seem to be less security-aware in all three dimensions and Chi-square test results show significant relationship between sector and computer (Chi-Square = 21,081; DF = 12; P-Value = 0,049) and web securities (Chi-Square = 33,557; DF = 12; P-Value = 0,001). However, this observation does not apply to e-mail security (Chi-Square = 10,890; DF = 6; P-Value = 0,092).

It is interesting to note that age and gender are positively correlated (r= 0,028), meaning that female respondents are generally older than males. Age also appears to be positively correlated with educational level (r= 0,231) and therefore older respondents tend to be better educated than younger ones. This is surprising because the educational level of the younger generation is normally expected to be higher than that of the older ones. One likely explanation is based on the fact that age was observed to be skewed in the data since 68 % of the respondents are younger than 30 years of age. One interesting note is that the correlation between age, gender and frequency of computer use was found to be negative (r= −0,290 and r= −0,075 respectively) meaning that younger males use computer more frequently. Finally, computer usage is increasing with increasing level of education (r= 0,144).

In all three dimensions (computer, web and e-mail) of secure ICT usage, web is identified as the weakest one on each category above (gender, age and job sector).

5.2 Test results

The ANOVA test results and correlations are given in Tab. 3. The reader should note here that last column of Tab. 3 shows that all the correlations are significantly positive. This means the relationships between dependent and independent variables are moving in the same direction.

In computer usage, p-values and positive correlations (Tab. 3) indicate that except for the hypotheses $H1_3$, the remaining ones are supported by the survey results at 5 % significance level. This means $H1_1$ and $H1_2$ are accepted at 5 % significance level since their p-values are 0,000 and 0,000 respectively. The p-value (0,085) for $H1_3$ shows acceptance at 10 % significance level. All these mean that higher levels of education result in higher levels of computer usage, awareness of computer security and awareness for security in computer usage routines. In other words, for variables "c_usage", "c_awareness", and "c_know" the variable education is not coming from identical populations, which may also be interpreted as the levels of education have significant impact on the usage frequency and other security issues in terms of using computer. As a consequence, increasing education level of users appears to be a significant stage for changing behaviour of individuals positively towards computer usage and computer security issues.

Table 3 ANOVA Test results against level of education

Empirical factor	Dep. Var.	Hyp.	d. f.	F value	p-value	Corr.***
Computer usage and security	c_usage	$H1_1$	19/413	2,89	0,000*	0,226
	c_awareness	$H1_2$	5/427	12,23	0,000*	0,264
	c_know	$H1_5$	5/427	1,95	0,085**	0,276
Web usage and security	w_usage	$H2_1$	30/402	1,94	0,003*	0,182
	w_awareness	$H2_2$	5/427	12,66	0,000*	0,261
	w_know	$H2_4$	5/427	2,05	0,071**	0,114
E-mail usage and security	e_usage	$H3_1$	5/427	3,87	0,002*	0,137
	e_awareness	$H3_2$	5/427	8,83	0,000*	0,226
	e_know	$H3_3$	5/427	3,91	0,002*	0,193

* indicates statistically significant at 5 % significance level.
** indicates statistically significant at 10 % significance level.
*** indicates that all the correlations were found to be statistically significant at 1 % significance level.

Interestingly, for the hypotheses $H2_1$, $H2_2$, $H2_3$, p-values were found to be 0,000; 0,000; 0,071; and the correlations between dependent and independent variables are all positive. Therefore we again accept $H2_1$ and $H2_2$ at 5 % significance level and accept $H2_3$ at 10 % significance level in the empirical category web usage. This also means higher levels of education result in higher levels of web usage, awareness of web security and awareness for security in web usage routines. In other words, for the variables "w_usage", "w_awareness" and "w_know" the variable "level of education" does not come from identical populations. This means, level of education categories does not show identical behavior in their populations for usage frequency of web and security awareness issues for web. Therefore, we conclude that education level has significant positive impact on the use of web sites, awareness of web security, and level of awareness for differentiating secured web sites. This also indicates that most of the variance for individuals' attitude towards web usage and web security issues may be

explained by their education level, which leads to the fact that higher educated individuals believe that they have control over their web usage attitude. Therefore, the individual's intention to engage in web usage is strongly positively related to their educational qualifications.

Regarding e-mail usage category, all the hypotheses were found to be significant at 5 % significance level since the *p*-values were found to be 0,002; 0,000 and 0,002. This and positive correlations, conclude the acceptance of all the hypotheses (i.e. $H3_1$, $H3_2$ and $H3_3$). It means higher levels of education result in higher levels of e-mail usage, awareness of e-mail security and security awareness in e-mail usage routines. This also shows that the level of education does not come from identical populations and therefore is not independent of using e-mail services and awareness of e-mail security issues. In other words, e-mail has provided a global and faster way of mass communication since 1990s and higher education is influencing compliance behavior towards related issues.

6 Discussion

This paper examines impact of education level with regards to IT security, which is one of the most critical areas considering proliferation among organizations and individuals in terms of IT security. The discussions on the results of this paper mainly focused on the three empirical categories of "computer usage and security", "web usage and security" and "e-mail usage and security".

6.1 Computer usage and security

Our test results provide strong indications for the presence of influence of education on computer usage frequency. Rezgui & Marks [31] and Sheng, Holbrook, Kumaraguru, Cranor & Downs [32] are only two of the studies that support this view. Rezgui & Marks [31] emphasized the role of training and education for keeping everyone up-to-date for IT threats. Bulgurcu, Cavusoglu & Benbasat [33] used another perspective and stated their belief that the level of education may influence compliance behavior for information security. All these may be an indication of the fact that information systems security constitutes a technologically complex field and needs comprehensive set of relevant competencies and skills, which can be better fulfilled with formal education. It means that information systems security should not be considered as a field that can be subjected to some form of informal training [34]. This is because such trainings are directed to broad audiences and the learners are mostly passive recipients [34]. Our finding is conflicting with Bulgurcu, Cavusoglu & Benbasat [33], who supported that there is no significant relationship between education level categories and computer technology usage. Similar findings were also reported by Mesko & Bernik [35]. They examined a sample from a population of mostly middle school or higher graduates. The results revealed that there is no increasing familiarity in computer applications with increasing level of education. They actually reported that youngsters are more familiar in this respect. An explanation of these may be based on the findings of Doyle & O'Flaherty [36], who supported that higher level of education does not add to lower education level student achievements in terms of computer usage due to the nature of contents of curriculum at these levels.

Interestingly, we have observed that education level has significant impact on computer security awareness in general. Naturally, test results also indicated significant effect of education level on knowledge of what to do against an attack. It was observed that there is significant difference between education level and security awareness (Chi-Square = 45,072; DF = 12; P-Value = 0,000). This finding is consistent with that reported by Rezgui & Marks [31]. Rezgui & Marks explored factors that affect security awareness related to computer usage within the context of a developing country. They concluded that education is an essential part of defending IS security and recommended that educational institutions should build security awareness training and education components for their students and staff. Similar findings were reported by Takemura & Umino [37]. Takemura & Umino examined existence of differences among Japanese ICT users, in terms of security awareness. They used analysis of variance technique and reported existence of significant differences in individuals' attributes. According to their study, the users who received the information security education have rather higher security recognition. They also suggested that the information security education should be enhanced in different levels of education so that users may appropriately take information security countermeasures. All these show that the role of the human factor in computer security is recognized to be important by the research community [31]. One plausible explanation for the similarities of findings from different countries may be based on the fact that in parallel to ICT proliferation in every field of daily life, everyone needs to be aware of up-to-date IT threats so that they can apply the security procedures in the most effective way [38]. It may also be taken as an indication of the fact that, on the contrary of many other ICT issues such as gender differences, digital divide, internet usage etc, the effect of culture is significantly dominated by education level of individuals when computer security is of interest.

6.2 Web usage and security

In parallel with the results in computer usage category, education level was found to have impact on web-usage in our study. Based on the positive intercorrelation, increasing level of education is supposed to increase web usage frequency (r=0,177). This finding was supported by the previous studies [39, 40, 4]. Hoffman and Novak [41] pointed the level of education as one of the effective factors in owning a computer and using web services in daily life processes along with some other factors. They refer education as "what counts", in order to emphasize the importance of it. Jalal, Marzooq & Nabi [39] and Bart, Shankar, Sultan & Urban [40] studied the motivating factors effecting online banking services. They attributed education as a significant factor among others. In another study (Muzividzi, Mbizi & Mukwazhe, 2013) authors concluded that in order to adopt internet banking services, significant level of education deemed to be necessary. One possible reason for underpinning

results is that education enhances the understanding of new technology, which means high educated are more aware of new technologies and therefore they are early adopters. On the other hand, educated users are already motivated to keep up and train themselves [42]. Thus, it is important to spend every effort to provide institutional or scholar training programs on IT for those without relevant education. Such programs may help individuals to bridge the digital divide and to share the advantages of online services more equally.

Our results also indicate a relationship for education level versus web security awareness (w_awareness) and knowledge of differentiating secure web applications (w_know). The literature also provides evidences calling more educational efforts towards security awareness regarding web and internet issues. Tekerek & Tekerek [43] and Srikwan & Jakobsson [44] are only two examples of such studies. According to Tekerek & Tekerek, students who have higher level of education have higher level of information security awareness. Srikwan & Jakobsson [44] used a different perspective and stated that poor user education can result in serious harm due to lack of ICT security awareness.

Interpretation of this finding with the guidelines in ITL security Bulletin [45] and the results of [46] which states "…training is not sufficient to ensure compliant behavior by end users, but needed." may help explaining the findings in our study. Also test results indicated significant differences between education categories in terms of web security awareness (Chi-Square = 38,022; DF = 12; P-Value = 0,000). In other words, users with higher education are concerned with secured web sites more since the correlation was observed to be positive (r = 0,094). This may be an indication of insufficient coverage regarding ICT security issues in the curriculums of lower levels of education. Another plausible explanation for our finding may be based on Siponen [47] that public may consider awareness in different depths depending on the level of education because web security falls outside the scope of the traditional computer issues. On the other hand, Doyle & O'Flaherty [36] pointed out that education level impacts moral reasoning. Accordingly, the findings in our study possibly illustrate the due effects of the improved reasoning and interpretation skills with the education level. Alternatively, the probability for people to take information security courses or get advice on web security topics increases with the extended education period.

6.3 E-mail usage and security

The results in this category indicate that education level has impact on e-mail usage frequency and security awareness in e-mail usage. In the literature there are several studies inspecting the security awareness in e-mail services (see for example, [36, 43, 48, 49]). Common to the majority of the studies in literature, education level enhances the security awareness, as our results specify as well. They also recommend special awareness education as mitigation for e-mail security risks. Interestingly, Ferguson [49] and Eyong [48] signified that the theoretical education without useful practices does little contribution to develop and internalize secure usage patterns. With the fact that the e-mail is the oldest service in the internet, it is in pervasive use and it is intensively utilized by the users. Furthermore e-mail services are reported as the most frequently used means by the attackers [5]. Therefore, probability for e-mail users to encounter the situations which they can gain experience is high. This characteristic of e-mail service may help explaining the observed significance level for dependent variable e_know which is less than 5 % while for c_know and w_know are both less than 10 %. On the other hand, the stronger relation between education and e_know than that of between education and both c_know and w_know suggests that the impact of education on security-action taken after being subject to a security attack in computer and web usage is less than that of e-mail usage. These findings may be interpreted as due effect of people's strong belief on counter-actions against a security attack requires more technical background or as the direct result of inadequate information. Because users are most probably well informed on the types of e-mail attacks and on the counter-measures of e-mail security treats in educational settings and practices, the relation between education and e_know is observed to be stronger.

ICT security-awareness level for elder people (>40 years of age) was observed as 0 %. The reason for this extreme result may be their unfamiliarity with the ICT products. Unquestionably, using ICT in education helps students in gaining familiarity with these products and applications. Thus, the youngsters might have developed secure usage behaviours in their school time, either by direct technology usage courses or by indirect usage of ICT products in other courses. The effect of ICT usage in curriculum on developing secure ICT usage practices needs to be investigated.

Finally and interestingly, the research [35] reveals that if people think that the organization in which they are working is responsible for the security then they are not spending enough effort in understanding and practicing the security precautions. In parallel with their statement, our results also indicate that the people who are working in private sector are more aware of security issues in computer, web and e-mail usage than that of in public sector. This is probably because the public sector employees do not feel the need to keep up with the latest developments in ICT assuming that their jobs are always secured. Additionally, according to [50], public sector employees are likely to worry more that Internet usage may increase security risks by creating more opportunities for computer hackers. The difference between sectors was also indicated to be significant by Frank & Lewis [51] and Bonson & Escobar [52]. Frank & Lewis reported the existence of differences between public and private sectors in terms of organizational characteristics, whereas Bonson & Escobar pointed significant differences between IT applications in public and private sectors. This means organizational characteristics and values play an important role in shaping individuals' attitudes towards the use of IT [53].

7 Conclusions

The paper presents the findings of a survey conducted among the citizens in Ankara. The results show in general

that education level is an important factor in frequency of ICT usage and awareness on security in using ICT. Our results may provide significant insight for universities regarding inclusion of IT security courses in their curriculum. On the other hand, since the level of education had significant impact on awareness of ICT security, efforts should also be directed towards increasing the awareness level of IT professionals in parallel to rapidly changing technology. This means, more efforts should be directed by organizations to train their employees in this regard via seminars and conferences.

Specifically in engineering education, there are courses to teach how to use ICT products to solve engineering problems. But those courses do not always cover the security and privacy aspects that need to be gained and internalized by users. Enhancing the course contents with regards to the security feature would provide a strong support in developing secure ICT usage behaviours.

There are some limitations to the present study. The sample is composed basically of ordinary citizens, which may not be representative of different layers in the society. Therefore, an extension to consider different groups in the society such as professionals or females-only may provide interesting results. Other socio-economic factors such as experience, gender and income should also be investigated. Another important limitation may be the effect of organization and culture, since the studies of Calhoun, Teng & Cheon [54], Chirkov, Ryan & Kim [55] and other researchers demonstrated that culture and organizational structure affects use of ICT in significant ways. Alternatively, Viberg & Grönlund [56] indicated that technology itself is more important than culture and other demographic factors. The effect of culture on ICT usage among organizations may be studied in detail from organizational perspective in the future.

8 References

[1] D'Arcy, J.; Hovav, A. Deterring Internal Information Misuse. // Communications of the ACM, 50, 10(2007), pp. 113-117.

[2] Adams, A.; Sase, M. A. Users Are Not The Enemy. // Communications of the ACM. 42, 12(1999).

[3] CSI 2008, CSI Computer Crime & Security Survey (2008), Computer Security Institute, http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf (13.12.2013).

[4] CSI 2009, 14th Annual CSI Computer Crime & Security Survey, Comprehensive Addition, Computer Security Institute, http://gocsi.com/purchase_survey (11.06.211).

[5] CSI 2010-2011, 15th Annual CSI Computer Crime & Security Survey, Computer Security Institute, http: //reports.informationweek.com/cart/index/downloadlink/id/7377 (12.12.2013).

[6] Irvine, C. E.; Chin, S-K.; Frincke, D. Integrating Security into the Curriculum. // Cybersquare-IEEE / December 1998, pp. 25-30.

[7] Yang, T. A.; Computer Security and Impact on Computer Science Education. // Journal of Computing in Small Colleges (JCSC). 16, 4(2001), pp. 233-246.

[8] LeBlanc, C.; Stiller, E. Teaching Computer Security at a Small College. // Proceedings of ACM Special Interest Group on Computer Science Education 2004 (SIGCSE)'04 / March 3-7 Norfolk-Virginia/USA , pp. 407-411.

[9] Marsa-Maestre, I.; De la Hoz, E.; Gimenez-Guzman, J. M.; Lopez-Carmona, M. A. Design and evaluation of a learning environment to effectively provide network security skills // Computers & Education, 69, (2013), 225-236.

[10] Barnett, S. F.; Computer Security Training and Education: A Needs Analysis, Security and Privacy, Proceedings of 1996. // IEEE Symposium on Computer Security and Privacy / Oakland CA, 1996, pp. 26-27.

[11] Hall, M. A. M. L.; Swanberg, D. L. Factors Affecting Information Technology Usage: A Meta-Analysis of the Empirical Literature. // Journal of Organizational Computing and Electronic Commerce. 11, 2 (2001), pp. 107-130.

[12] Andrew, B. J.; Hubona, G. S. The mediation of external variables in the technology acceptance model. // Information & Management. 43, 6(2006), pp. 706-717.

[13] Davis, F.; Perceived Usefulness, Perceived Ease of Use and End User Acceptance of Information Technology. // MIS Quarterly. 13, 3(1989), pp. 318-339.

[14] Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L.; Downs, J. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. // Proceedings of ACM Conference on Human Factors in Computing Systems (CHI) 2010 / April 10-15, Atlanta, Georgia, USA, pp. 373-382.

[15] Herzberg, A.; Jbara, A. Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks. // ACM Transactions on Internet Technology. 8, 4 (2006), Article 16.

[16] UNPAN 2008, From e-Government to Connected Governance. United Nations e-Government Survey 2008, United Nations New York. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf (27.08.2012).

[17] Akman, I.; Yazici, A.; Mishra, A.; Arifoglu, A. E-Government: A global view and an empirical evaluation of some attributes of citizens. // Government Information Quaterly. 22, 2(2005), pp. 239-257.

[18] Fisher, Y.; Jacob, O. B. Measuring Internet usage: the Israeli case. // International Journal of Human-Computer Studies. 64, (2006), pp. 984-997.

[19] Fang, X.; Yen, D. C. Demographics and behavior of Internet users in China. // Technology in Society. 28, (2006), pp. 363-387.

[20] Lightner N. J.; Yenisey, M. M.; Ozok, A. A. Shopping behavior and preferences in e-commerce of Turkish and American university students: implications from cross-cultural design. // Behaviour & Information Technology. 21, (2006), pp. 373-385.

[21] Hui, T-K.; Wan, D. Factors affecting Internet shopping behaviour in Singapore: gender and educational issues. // International Journal of Consumer Studies. 31, (2007), pp. 310-316.

[22] Gatautis, R. The Impact of ICT on Public and Private Sectors in Lithuania. // Inzinerine Ekonomika- Engineering Economics. 4, 59(2008), pp. 18-28.

[23] Lai, C.; Gwung, H. The effect of gender and Internet usage on physical and cyber interpersonal relationships. // Computers & Education. 69, (2013), pp. 303-309.

[24] Tarafdar, M.; Vaidya, S. D. Challenges in the adoption of E-Commerce technologies in India: The role of organizational factors. // International Journal of Information Management. 26, (2006), pp. 428-441.

[25] Bhatnagar, A.; Ghose, S. Online Information Search Termination Patterns Across Product Categories and Consumer Demographics. // Journal of Retailing. 80, (2004), pp. 221-228.

[26] Losh, S. C. Gender and educational Digital Chasms in Computer and Internet Access and Use Over Time: 1982-2000. // IT and Society. 1, 4(2003), pp. 73-86.

[27] Fleming, N. C.; Nellis, J. G. Principles of Applied Statistics 2nd Edition, 1994.

[28] Mendelhal, W.; Sincich, T. Statistics for the engineering and computer sciences. Maxwell McMillan International Editions 1989.
[29] Miller, I.; Freund, J. E. Probability and Statistics for Engineers, Prentice-Hall 1985.
[30] Milton, J. S.; Arnold, L.C. Introduction to probability and statistics: principles and applications for engineering and the computing Sciences.Ed-4, McGraw Hill, Boston, MA. 2002.
[31] Rezgui, R.; Marks, A. Information security awareness in higher education: An exploratory study. // Computers & Security. 27, 7-8(2008), pp. 241-253.
[32] Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L.; Downs, J. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. // ACM Conference on Human Factors in Computing Systems (CHI) 2010/ April 10-15, Atlanta, Georgia, USA, pp. 373-382.
[33] Bulgurcu, B.; Cavusoglu, H.; Benbasat I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. // MIS Quarterly. 34, 3(2010), pp. 523-548.
[34] Katsikas, S. K. Health care management and information systems security: Awareness, training or education? // International Journal of Medical Informatics. 60, 2(2000), pp. 129-135.
[35] Mesko, G.; Bernik, I. Cybercrime: Awareness and Fear. Slovenian Perspectives. // Proceedings of 2011 European Intelligence and Security Informatics Conference, IEEE Computer Society / Athens, 2011, pp. 28-32.
[36] Doyle, E.; O'Flaherty, J. The impact of education level and type on moral reasoning. // Irish Educational Studies. 32, 3(2013), pp. 377-393.
[37] Takemura, T.; Umino, A. A Quantitative Study on Japanese Internet User's Awareness to Information Security: Necessity and Importance of Education and Policy, World Academy of Science. // Engineering and Technology. 3, 12(2009), pp. 888-895.
[38] Piazza, P. Security goes to school. // Security Management. 50 ,12(2006), pp. 46-51.
[39] Jalal, A.; Marzooq, J.; Nabi, H. A. Evaluating the Impacts of Online Banking Factors on Motivating the Process of E-banking. // Journal of Management and Sustainability. 1, 1(2011), pp. 32-42.
[40] Bart, Y.; Shankar, V.; Sultan, F.; Urban, G. L. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. // Journal of Marketing. 69, (2005), pp. 133-152.
[41] Hoffman, D. L.; Novak, T. P. Bridging the Racial Divide on the Internet. // SCIENCE, 280, (1998), pp. 390-391.
[42] Muzividzi, D. K.; Mbizi, R.; Mukwazhe, T. An Analysis of Factors That Influence Internet Banking Adoption Among Intellectuals: Case of Chinhoyi University Of Technology. // Interdisciplinary Journal of Contemporary Research in Business. 4, 11(2013), pp. 350-369.
[43] Tekerek, M.; Tekerek, A. A Research on Students' Information Security Awareness. // Turkish Journal of Education. 2, 3 (2013), pp. 61-70.
[44] Srikwan, S.; Jakobsson, M. Using cartoons to teach Internet Security. // Cryptologia. 32, 2(2008), pp. 137-154.
[45] Wilson, M.; Hash, J. Information Technology Security Awareness, Training, Education, and Certification, National Institute of Standards and Technology (NIST). // Information Technology Laboratory Security Bulletins, ITL October 2003, http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm. (01.12.2013)
[46] Stephanou, A. T.; Dagada, R. The Impact of Information security Awareness Training on Information Security Behaviour: The Case for Further Research. // Proceedings of the ISSA 2008 Innovative Minds Conference / 7-9 July 2008, pp. 309-326
[47] Siponen, M. T. Five Dimensions of Information Security Awareness. // Computers and Society. 31, 2(2001), pp. 24-29.
[48] Eyong, B. K. Information Security Awareness Status of Business College: Undergraduate Students. // Information Security Journal: A Global Perspective. 22, 4(2013), pp. 171-179.
[49] Ferguson, A. J. Fostering E-mail Security Awareness: The West Point Carronade. // Educase Quarterly. 1, (2005), pp. 45-57.
[50] Iscan, O. F.; Naktiyok, A. Attitudes towards telecommuting: The Turkish case. // Journal of Information Technology. 20, (2005), pp. 52-63.
[51] Frank, A. S.; Lewis, G. B. Government employees, working hard or hardly working. // The American Review of Public Administration. 34, 1(2004), pp. 36-51.
[52] Bonson, E.; Escobar, T. Digital reporting in Eastern Europe: An empirical study. // International Journal of Accounting Information Systems. 7, (2006), pp. 299-318.
[53] Jin, K. G.; Drozdenko, R.; Bassett, R. Information technology professionals' perceived organizational values and managerial ethics: an empirical study. // Journal of Business Ethics. 71, 2(2007), pp. 149-159.
[54] Calhoun, K. J.; Teng, J. T. C.; Cheon, M. J. Impact of national culture on information technology usage behaviour: an exploratory study of decision making in Korea and the US. // Behaviour and Information Technology. 21, (2002), pp. 293-302.
[55] Chirkov, V.; Ryan, R. M.; Kim, Y. Differentiating autonomy from individualism and independence: a self-determination theory perspective on internalization of cultural orientations and well-being. // Journal of Personality and Social Psychology. 84, (2003), pp. 97-110.
[56] Viberg, O.; Grönlund, Ä. Cross-cultural analysis of users' attitudes toward the use of mobile devices in second and foreign language learning in higher education: A case from Sweden and China. // Computers & Education. 69, (2013), pp. 169-180.

Authors' addresses

Atila Bostan, Asst. Prof. Dr.
Atılım University
Computer Engineering Department
Kızılcaşar Mah, İncek-Gölbaşı/Ankara/Turkey
E-mail: abostan@atilim.edu.tr

İbrahim Akman, Prof. Dr.
Atılım University
Computer Engineering Department
Kızılcaşar Mah, İncek-Gölbaşı/Ankara/Turkey
E-mail: akman@atilim.edu.tr