***PEOPLE: International Journal of Social Sciences***
***ISSN 2454-5899***

*Akman & Bostan, 2018*

*Volume 3 Issue 3, pp. 1046-1063*

*Date of Publication: 29th January, 2018*

*DOI-https://dx.doi.org/10.20319/pijss.2018.33.10461063*

*This paper can be cited as: Akman, I & Bostan, A. (2018). ICT Usage Characteristics and Computer Security. PEOPLE: International Journal of Social Sciences, 3(3), 1046-1063.*



# ICT USAGE CHARACTERISTICS AND COMPUTER SECURITY

**İbrahim Akman**
*Department of Computer Engineering, Atılım University, Ankara, Turkey*
*ibrahim.akman@atilim.edu.tr*

**Atila Bostan**
*Department of Computer Engineering, Atılım University, Ankara, Turkey*
*atila.bostan@atilim.edu.tr*

## Abstract

*Although acquired-user security habits and user security awareness are qualified as the feeblest components in assuring the information and communication technologies security, they are deemed to be inevitable as well. While the technology in information processing domain efforts its best in establishing the highest plausible security, user awareness is still referred as the key-component. Human demographic factors, ICT usage frequency might have correlation with security related behavior routines, this dimension not to be known yet. Hence, in this study we examined the influence of ICT usage characteristics on secure computer usage behaviors. In order to investigate this relation, a survey was carried out with the participation of 466 individuals from diverse layers of the community. The results demonstrated that statistically noteworthy relations exist between several socio-demographic features, frequency and reason of ICT usage factors and secure computer usage.*

**Keywords**

Demographic Factors, Computer Security, ICT Usage Frequency

## 1. Introduction

As the information and communication technologies (ICT) pervade all business domains, the security functions needed to be performed by these technologies also get more complex and more diverse. "Security holes are shown to be on a continuous rise, as the technology efforts to develop security mechanisms in recent years," (CSI 2009; CSI 2010/2011). Users are almost always referred as the key component, when ICT security is in the focus. As they are playing administrator, technician or operator roles in ICT systems, users are inescapable and feeblest ring-chain in security-mechanisms. Vagueness in user conducts is generally considered as the estate for the faintness of users. Therefore, given any security related experimental setting, guessing the anticipated reaction of a user is usually very hard. Although they were subject to the same education, directions and training, reactions of two different users to an identical security stimulus would most likely be different than each other. Human decision-making process is ambiguous and the factors effective in that are fuzzy.

In guessing ICT user responses towards a security challenge, their behavioral practices and habits play an important role. It is pointed out in one of the research studies; "user security habits and security awareness are the key components for successful information security" (D'Arcy & Hovay, 2007). Adams and Sase (Adams, Sase, 1999) specified "human factors should be considered in design of security mechanisms, since they are developed, implemented and breached by people," (Adams & Sase, 1999). Whereas inappropriate and destructive behaviors can substantially inhibit efficiency of information security, constructive and appropriate actions by system administrators and end users can improve the effectiveness (Stanton, Stam, Mastrangelo & Jolton, 2005). Schneier asserts ''Mathematics is rational but people are unpredictable, variable, and hard to comprehend.'' in his elucidation on human behaviors in information security, Secrets and Lies, (Schneier, 2011). Security performances of end users would necessitate utilization of several tools in order to develop experimental practices. With the intention of improving user security behaviors, considerable amount of the publications in the literature denote the user training as a possible remedy. But, there are significant number of academic studies demonstrating that user beliefs are not compatible with

his practices, at all times (Palfreyman & Rodden, 1996; Gross & Rosson, 2007). Secure ICT usage habits must be developed and internalized (Gross & Rosson, 2007).

Secure ICT usage behavior development in users necessitates changes in daily practices. The prominent factors known to induce behavioral changes are training, user intentions and observed experiences. In designing ICT security mechanisms, researchers are generally attracting the attention to concentrate on user habits and motivations (Stanton, Stam, Mastrangelo & Jolton, 2005; Herzberg & Jbara, 2008; West, 2008). However, ICT system design, user awareness and security training programs would considerably benefit from the factors in developing secure-user-behavior if the affective ones and their respective influence are distinctively identified. Thus customized education and training curricula may be designed, in order to bring up a more security-aware community and cultivate secure ICT usage in social and business sectors. As it was reported by Cilliers E. J. (Cilliers, 2017), the new generation Z is more equipped with technology and presents exclusive learning and adoption strategies. Additionally, clearly recognized socio-demographic factors that are effective in secure ICT usage, would lay grounds for more efficient human resources planning, labor force recruitment and employment, particularly in security-sensitive business domains such as strategical government enterprises, banking and commercial ventures. Furthermore, given the effective factors in provoking secure usage, more user friendly and more security-inspiring ICT systems, user interfaces and user interactions would possibly be developed. Therefore, socio-demographic factors including gender age education sector of work and ICT experience constitute independent variables in this study.

We inspected the effect of socio-demographic factors and ICT usage characteristics on secure computer usage, in this study. In order to analyze the problem a survey was conducted in shopping centers where contacting to the respondents assumed to be easy and random enough. In total randomly selected 466 person participated in the survey study. Results of the survey analyzed to derive interpretations and study conclusions.

Following sections of this paper is structured as follows: In the next section literature review is presented. Research methodology and hypotheses are explained in the third section. Subsequent to the research design and test method sections, we report analysis results that are conducted in the study. In the final chapter, conclusions and suggested future work are submitted.

## 2. Literature Review

The literature reported that there is digital divide within countries (UNPAN 2008). The relationships between socio-demographic factors, ICT security issues and the attitude of individuals toward using ICT were investigated by several studies (see for example; Gatautis, 2008; Hui & Wan, 2007; Lightner, Yenisey & Ozok, 2006; Fang & Yen, 2006; Fisher & Jacob, 2006; Teo, & Lim 2000; Thomson & Laing, 2003; Shore, Venkatachalam, Solorzano et al., 2001).

ICT can enable a huge range of information and services for the usage of citizens which means the key to use ICT is not technology but the citizens. This is attributed to the variance among citizen-attributes including education, age, gender, income, business, households and socio-economic levels pertaining to both their chances to access ICT and to the Internet for a extensive diversity of accomplishments. Out of these characteristics, education, age, ICT experience and have attracted distinct attention. Moreover, organizational attributes such as sector of work place play an imperative part in influencing one's attitudes concerning the use of IT (Jin, Drozdenko & Bassett, 2007).

Among organizations from public and private sectors, significant variances were reported between the types of IT applications that are utilized, by several studies. Similarly, dissimilarities between the IT application types among organizations from dissimilar sectors were demonstrated by Lau and Gupta et.al. (Lau, 2003; Gupta, Gould & Pola, 2004). On the other hand, security was referred as to be an important issue influencing ICT adoption by Tan et al. (Tan, Lin & Eze, 2009). Impact of demographic factors on security awareness and secure computer-usage were examined by Maslin and Zuraini (Maslin, & Zuraini, 2008). They stated that education level and age have impact on security awareness and secure computer-usage. In his study, Choi (Choi, 2008) concluded that demographic factors influence computer security issues. ur Rehman et.al. (ur Rehman, Salam & Tareq, 2016), studied the features inspiring the use of electronic banking applications and reported the user trust as one of the prominent one. Whereas the user trust level and trust establishment are proven to have strong relation with user socio-demographics and prior experiences. In their study Kang et.al. (Kang, Dabbish, Fruchter & Kiesler, 2015) inspected the influence of familiarity with the Internet on user responses to ICT privacy and security risks. They reported that the relation between Internet familiarity and privacy-and-security risk management of the users is insignificant. As a conclusion Kang et.al.

suggested a bigger emphasis on strategies and systems which protect security and privacy without depending too much on security practices of users. By criticizing the device centric ICT security approaches and the need to acquire knowledge on how to use and manage diverse set of security policies as per each device, Montero et.al. (Montero, Yannuzzi, Shaw, Jacquin, Pastor, Serral-Gracia, & Nemirovsky, 2015) proposed an access network level security policy model in their work. Thus, they claim that users would not be forced to learn how to use and manage a various set of security applications, given the increasing number of user terminals such as tablets, notebooks, smartphones, smart TVs, desktop computers and game consoles that a regular user possess. Nurkhin, A., & Arief, S. (Nurkhin & Arief, 2015) reported that perceived mobility value, social interaction, prior experience and perceived usefulness have impact on the user acceptance of technology. On the other hand, Shropshire, et.al. (Shropshire, Warkentin, & Sharma, 2015) studied the personality constructs that are effective in security software adoption. Their conclusions point the constructs influencing security software adoption is different than that of in regular software adoption. All the above mentioned studies specify the requirement for additional researches since results may offer valuable perceptions to policy makers in common. Therefore, we use above backdrop to include security related factors including awareness, storing critical information, backup frequency, scanning frequency and usage of scanner/firewall, as mediating factors in the research. To the best of our knowledge these factors have not been used in our context in the literature yet.

## 3. Research Methodology and Hypotheses

Present study primarily accomplishes a systematic analysis to inspect the relationships between socio-demographic factors, computer security issues and frequency and reason of ICT usage. Research model can be described in schematic presentation as shown in Figure 1.

Present research model was established to analyze to the following questions:

- Is there significant influence of socio-demographic features on computer security factors?
- Is there significant impact of socio-demographic features on ICT usage frequency and reason?
- Is there any significant relationship between computer security factors and, ICT usage reason and frequency?

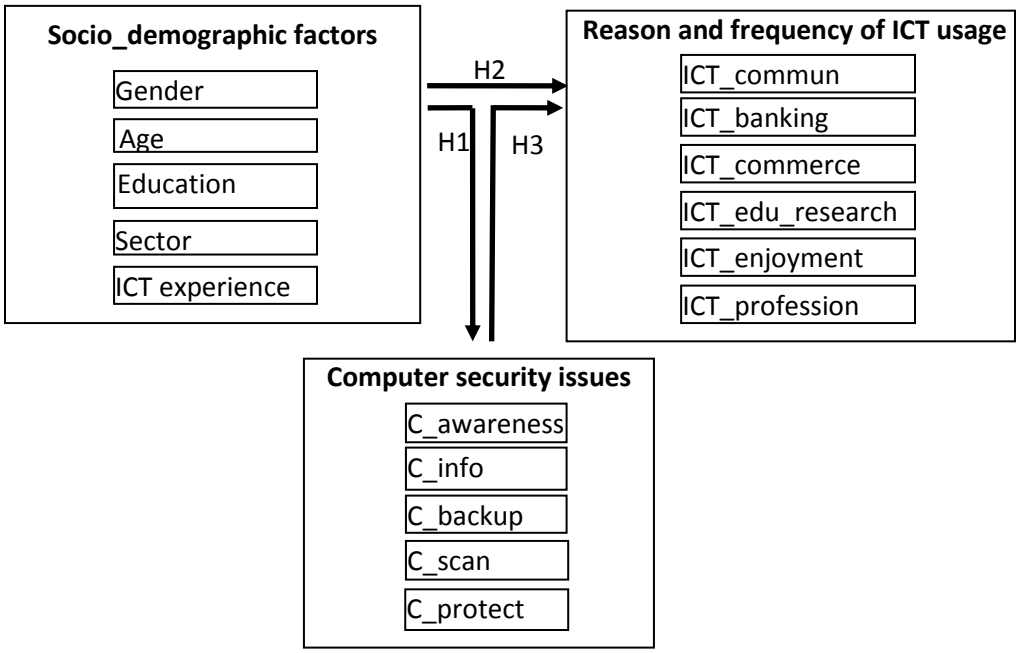


**Figure 1:** *Research Model*

For this purpose, empirical attributes (i) Socio-Demographic, (ii) Computer security and (iii) Reason and frequency of ICT usage are used as follows. The reasoning for empirical attributes and their corresponding hypotheses are listed in Table 1 below.

**Table 1:** *Summary of Research Questions and Variables*

| **Hyp.** | **Definition** |
|---|---|
| H1 | Socio-demographic $factor_i$ (i=1,2...,5) is not related to computer_security $factor_j$ (j=1,2..,5). |
| H2 | Socio-demographic $factor_i$ (i=1,2...,5) is not related to reason and frequency of ICT_usage $factor_j$ (j=1,2,..,6). |
| H3 | Computer_security $factor_i$ (i=1,2,..,5) is not related to reason and frequency of ICT_usage $factor_j$ (j=1,2,..,6). |

## 4. Research Design

Because the survey was carried out in changing days of the week and conducted in big shopping malls by Turkish Chamber of Electrical Engineers, the respondents were assumed to be usual citizens from different social classes in the society. Participation was optional in the study. The number of survey questionnaires completed was 466 in total. Owing to the unqualified data 33 responses were discarded, in conclusion 433 responses were studied in the analysis. Hence, the rate for the response was 93% in the average which can securely be interpreted as satisfactory

for the purpose of this study (Feleming & Nellis, 2000). The variables and research questions are listed in Table 2 below.

**Table 2:** *Summary of Research Questions and Variables*

| Q | 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 | education | What is your education level? | graduate/undergraduate/others, |
| 4 | sector | What is the sector of your organization? | private, public, not working (retired/student/ unemployed/ etc) |
| 5 | experience | What is the level of your ICT experience (years)? | 0, 1-5, 6-10, 11-15, 16-20, >20 |
| 6 | C_awareness | What is your level of awareness on computer security? | very high, high, average, little, very little |
| 7 | C_ info | Do you store critical / valuable info on your computer? | yes/no |
| 8 | C_backup | How frequently you back up information on your computer? | very high, high, average, little, very little |
| 9 | C_scan | How frequently you scan your computer? | very high, high, average, little, very little |
| 10 | C_protect | Do you use a licensed scanner /firewall? | yes/no |
| 11 | ICT_commun | How much do you use ICT for communication? | very high, high, average, little, very little |
| 12 | ICT_banking | How much do you use ICT for electronic banking? | very high, high, average, little, very little |
| 13 | ICT_commerce | How much do you use ICT for electronic commerce? | very high, high, average, little, very little |
| 14 | ICT_edu_research | How much do you use ICT for education and research? | very high, high, average, little, very little |
| 15 | ICT_enjoyment | How much do you use ICT for enjoyment? | very high, high, average, little, very little |
| 16 | ICT_profession | How much do you use ICT for your professional activities? | very high, high, average, little, very little |

## 5. Test Method

Hypotheses testing regarding the interactions between socio-demographic features, the reason, usage frequency and ICT security factors was examined by multivariate regression analysis. Regression Analysis is used in diverse applications and is a powerful statistical tool since no assumption is made on the type of relationship between independent and dependent

variables. Moreover, Regression Analysis can analyze categorical data more effectively and, thus, is generally favored whenever the independent variables are categorical (Milton & Arnold, 2003). Chi-square test method is also utilized in testing the significance of the observed relation between dependent and independent variables in the analysis (Milton & Arnold, 2003).

## 6. Results

Presentation order of the results is as follows. Firstly, descriptive results for the survey data are reported. In this section, chi-square test method was also used when it is assessed to provide more explanation to the profile of respondents. Afterwards, regression analysis results of demographic factors are presented.

### 6.1 Descriptive Results

Gender, age and work-sector distribution of respondents are listed in Table 3.

The gender distribution of the respondents was found to be almost equal (male: 55%; female: 44%). This is not surprising since the survey was carried out in shopping centers where dominancy of any gender is not expected. For male samples, 21% reported their awareness on computer security to be higher than average and for females this figure is 8%. Chi-square test results demonstrate a significant relation between computer security awareness and gender (Chi-Square = 24.081; DF = 5; P-Value = 0.000).

With respect to the age distribution, the group whose ages are less than 30 years, a high fraction (68%) is identified while this number for the other groups (whose ages are greater than 40 years) is 11%. It should be interpreted as normal since the number of young people going to shopping centers is normally expected to be high and youngsters are generally more keen to respond surveys. Out of the respondents whose ages are less than or equal to 30 years, 20% reported their computer security awareness level is higher than average and this figure for elder people (>40 years of age) is 0%. The relation between computer security and age is shown to be significant by the Chi-square test results (Chi-Square = 52.197; DF = 9; P-Value = 0.000).

**Table 3:** *Profile of Respondents*

| **Variable** | **Turkish graduate students** | |
|---|---|---|
| | **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 |
| Sector | 433 | 100 |
| Private | 93 | 21 |
| Public | 76 | 18 |
| Not working | 238 | 55 |
| Unknown | 26 | 6 |

From the working sector point of view, 16% of the private sector respondents declared their computer security awareness is higher than average. This number for respondents from public sector is 12%. Public sector workers are found to be less security-aware and Chi-square test results point to important relationship between computer security and work-sector (Chi-Square = 21.081; DF = 12; P-Value = 0.049).

**6.2 Test Results**

In right most column of Table 4, P-values show that except for the hypotheses H114, all the hypothesis are found to be insignificant by the results for C_awareness at 5% significance level. In other words, $H1_{11}$, $H1_{12}$, $H1_{13}$ and $H1_{15}$ are rejected since their p-values are all 0.000 where the threshold is 5 percent. This means socio-demographic factors gender, education, experience and age have significant influence on the computer security awareness. Hypothesis test results indicate gender, age, education and experience are predictors of awareness regarding computer security. Interestingly the work place does not demonstrate any influence on security awareness. Similar results are also observed for the dependent variables C_backup and C_scan. That is to say, H121, $H1_{22}$, $H1_{23}$ and $H1_{25}$ for C_backup and $H1_{31}$, $H1_{32}$, $H1_{33}$ and $H1_{35}$ for C_scan are rejected with 5% significance threshold. Which implies the independent variables education, age, experience and gender do not influence the user conduct in frequency of having back up for the data stored on personal computer and frequency of scanning the computer.

**Table 4:** *Regression Test Results of Socio-Demographics against Computer Security*

| **Dependent var.** | **Indep. var.** | **Hyp.** | **alpha-value** | **p-value*** |
|---|---|---|---|---|
| C_awareness | gender | $H1_{11}$ | -0.372 | 0.000* |
| | age | $H1_{12}$ | -0.328 | 0.000* |
| | education | $H1_{13}$ | 0.123 | 0.000* |
| | sector | $H1_{14}$ | -0.035 | 0.489 |
| | experience | $H1_{15}$ | 0.504 | 0.000* |

| | | | | |
|---|---|---|---|---|
| C_info | gender | $H1_{21}$ | -0.236 | 0.000* |
| | age | $H1_{22}$ | -0.109 | 0.066 |
| | education | $H1_{23}$ | 0.199 | 0.418 |
| | sector | $H1_{24}$ | 0.140 | 0.000* |
| | experience | $H1_{25}$ | 0.121 | 0.000* |
| C_backup | gender | $H1_{31}$ | -0.325 | 0.000* |
| | age | $H1_{32}$ | -0.247 | 0.021* |
| | education | $H1_{33}$ | 0.157 | 0.000* |
| | sector | $H1_{34}$ | 0.093 | 0.185 |
| | experience | $H1_{35}$ | 0.371 | 0.000* |
| C_scan | gender | $H1_{41}$ | -0.439 | 0.000* |
| | age | $H1_{42}$ | -0.207 | 0.042* |
| | education | $H1_{43}$ | 0.145 | 0.001* |
| | sector | $H1_{44}$ | -0.002 | 0.973 |
| | experience | $H1_{45}$ | 0.391 | 0.000* |
| C_protect | gender | $H1_{51}$ | -0.271 | 0.000* |
| | age | $H1_{52}$ | -0.105 | 0.054* |
| | education | $H1_{53}$ | 0.0485 | 0.032* |
| | sector | $H1_{54}$ | 0.0839 | 0.020* |
| | experience | $H1_{55}$ | 0.134 | 0.000* |

This can also be interpreted as that, except sector of work place, all the remaining factors appear to be significant determinants for backup and scanning frequencies. The work place does not have this effect. The test results show that gender (p-value=0.000), sector (p-value=0.000) and experience (p_value=0.000) significantly predict the users behavior for storing critical information on their personal computers. In other words, educated females with more ICT experience show more cautiousness in storing critical (may be personal) information in computers. Interestingly education (p_value=0.418) and age (p_value=0.066) are found to have no relationship at alpha=0.05 significance level. The p-values in the right most column of Table 4 shows rejection of $H1_{51}$, $H1_{52}$, $H1_{53}$, $H1_{54}$ and $H1_{55}$ in this grouping. Which means that the socio-demographic factors age, education, gender, work-sector and experience have significant influence on the behavior for using a licensed scanner on personal computer. Considering the coding scheme, it is possible to conclude that elder educated females with more ICT experience and not working (student, retired) show more intention to use a licensed scanner. Finally, it is interesting to note that gender and experience are significant indicators for all factors in the empirical category of computer security.

Interestingly, with regard to the experience, p-values in the right most column of Table 5 point rejection of $H2_{15}$, $_{25}$, $_{35}$, $_{45}$, $_{55}$ and $H2_{65}$. This implies, dependent variables, ICT_commerce,

ICT_banking, ICT_commun, ICT_edu_research, ICT_profession and ICT_enjoyment are completely influenced by the socio-demographic factor experience since p-values are all 0.000. In other words, with the increasing level of experience, ICT usage in commerce, banking, communication, education and research, professional and enjoyment values is also increasing. Alternatively, p-values indicate rejection of $H2_{11}$, $_{31}$, $_{41}$ and $H2_{51}$ for the dependent variable gender. That is to say, gender has influence on ICT usage for communication, commerce, education-and-research, and enjoyment. This results also point that the relation between gender and ICT usage for commerce, communication, enjoyment and education-and-research is significant. For variable age which is one of the socio-demographic factors in the study, $H2_{22}$, $_{32}$, $_{52}$ and $H2_{62}$ are rejected. This can be interpreted as, age has significant influence on ICT usage for commerce, banking, enjoyment and professional purposes. Regarding the level of education, p-values for the hypotheses $H2_{13}$, $_{23}$, $_{33}$, $_{43}$, $_{53}$ and $H2_{63}$, were identified as 0.024, 0.0, 0.008, 0.0, 0.125 and 0.0 respectively. These results leads to acceptance of $H2_{53}$ and rejection of $H2_{23}$, $_{33}$, $_{43}$ and $H2_{63}$ at 5 percent significance threshold in the education grouping. In other words, level of education has important influence on the ICT usage for commerce, banking, communication, professional and education-and-research purposes.

**Table 5:** *Regression Test Results of Socio_Demographics against Reason and Frequency of ICT Usage*

| Dependent var. | Independent var. | Hyp. | alpha-value | p-value* |
|---|---|---|---|---|
| ICT_commun | gender | $H2_{11}$ | - 0.548 | 0.000* |
| | age | $H2_{12}$ | - 0.003 | 0.975 |
| | education | $H2_{13}$ | 0.085 | 0.024* |
| | sector | $H2_{14}$ | 0.037 | 0.536 |
| | experience | $H2_{15}$ | 0.696 | 0.000* |
| ICT_banking | gender | $H2_{21}$ | - 0.045 | 0.425 |
| | age | $H2_{22}$ | - 0.247 | 0.026* |
| | education | $H2_{23}$ | 0.193 | 0.000* |
| | sector | $H2_{24}$ | 0.067 | 0.361 |
| | experience | $H2_{25}$ | 0.593 | 0.000* |
| ICT_commerce | gender | $H2_{31}$ | - 0.130 | 0023* |
| | age | $H2_{32}$ | - 0.218 | 0.052* |
| | education | $H2_{33}$ | 0.125 | 0.008* |
| | sector | $H2_{34}$ | - 0.194 | 0.009* |
| | experience | $H2_{35}$ | 0.436 | 0.000* |
| ICT_edu_research | gender | $H2_{41}$ | - 0.447 | 0.000* |
| | age | $H2_{42}$ | - 0.011 | 0.924 |
| | education | $H2_{43}$ | 0.196 | 0.000* |

| | | | | |
|---|---|---|---|---|
| | sector | $H2_{44}$ | - 0.364 | 0.000* |
| | experience | $H2_{45}$ | 0.683 | 0.000* |
| ICT_enjoyment | gender | $H2_{51}$ | - 0.602 | 0.000* |
| | age | $H2_{52}$ | - 0.213 | 0.040* |
| | education | $H2_{53}$ | 0.066 | 0.125 |
| | sector | $H2_{54}$ | - 0.238 | 0.001* |
| | experience | $H2_{55}$ | 0.649 | 0.000* |
| ICT_profession | gender | $H2_{61}$ | - 0.048 | 0.449 |
| | age | $H2_{62}$ | - 0.259 | 0.039* |
| | education | $H2_{63}$ | 0.242 | 0.000* |
| | sector | $H2_{64}$ | 0.236 | 0.005* |
| | experience | $H2_{65}$ | 0.627 | 0.000* |

Furthermore, education level categories do not demonstrate matching behavior in their populations for using ICT usage for the purpose of enjoyment. Finally, the work-sector variable is found to be not in favor of $H2_{34}$, $_{44}$, $_{54}$ and $H2_{64}$, which concludes to the rejection of the hypothesis since inspection of p-values indicate figures greater than 5%. Additionally, work place has noteworthy influence on the frequency and reason of ICT usage for professional, commerce, enjoyment and education and research purposes.

**Table 6:** *Regression Test Results of Computer Security against Reason and Frequency of ICT Usage*

| **Dependent var.** | **Independent var.** | **Hyp.** | **alpha-value** | **p-value*** |
|---|---|---|---|---|
| ICT_commun | C_awareness | $H3_{11}$ | 0.701 | 0.000* |
| | C_info | $H3_{12}$ | 0.159 | 0.080 |
| | C_backup | $H3_{13}$ | 0.038 | 0.533 |
| | C_scan | $H3_{14}$ | - 0.045 | 0.489 |
| | C_protect | $H3_{15}$ | 0.281 | 0.004* |
| ICT_banking | C_awareness | $H3_{21}$ | 0.514 | 0.000* |
| | C_info | $H3_{22}$ | - 0.419 | 0.000* |
| | C_backup | $H3_{23}$ | 0.242 | 0.000* |
| | C_scan | $H3_{24}$ | 0.098 | 0.179 |
| | C_protect | $H3_{25}$ | 0.093 | 0.394 |
| ICT_commerce | C_awareness | $H3_{31}$ | 0.491 | 0.000* |
| | C_info | $H3_{32}$ | - 0.397 | 0.000* |
| | C_backup | $H3_{33}$ | 0.232 | 0.001* |
| | C_scan | $H3_{34}$ | 0.007 | 0.925 |
| | C_protect | $H3_{35}$ | - 0.077 | 0.466 |
| ICT_edu_research | C_awareness | $H3_{41}$ | 0.727 | 0.000* |
| | C_info | $H3_{42}$ | - 0.380 | 0.001* |
| | C_backup | $H3_{43}$ | 0.0171 | 0.817 |
| | C_scan | $H3_{44}$ | 0.178 | 0.025* |

| | | | | |
|---|---|---|---|---|
| | C_protect | $H3_{45}$ | 0.222 | 0.051* |
| ICT_enjoyment | C_awareness | $H3_{51}$ | 0.675 | 0.000* |
| | C_info | $H3_{52}$ | - 0,050 | 0.617 |
| | C_backup | $H3_{53}$ | - 0.025 | 0.711 |
| | C_scan | $H3_{54}$ | 0.060 | 0.398 |
| | C_protect | $H3_{55}$ | 0.464 | 0.000* |
| ICT_profession | C_awareness | $H3_{61}$ | 0.597 | 0.000* |
| | C_info | $H3_{62}$ | - 0.219 | 0.065 |
| | C_backup | $H3_{63}$ | 0.307 | 0.000* |
| | C_scan | $H3_{64}$ | 0.0619 | 0.463 |
| | C_protect | $H3_{65}$ | - 0.091 | 0.473 |

With regards to the relation between computer security and frequency, reason of ICT treatment, the regression test results are given in Table 6. Interestingly, p-values in the right most column of Table 6 show parallel inclination for ICT usage for banking and commerce purposes. This means, $H3_{31, 32}$ and $H1_{33}$ for C_commerce and $H3_{21, 22}$ and $H3_{23}$ for C_banking are rejected at 5% significance threshold. In other words, C_info, C_awareness and C_backup have influence on the dependent variables C_commerce and C_banking. That is to say, the behavior of storing critical/valuable information on personal computer, computer security awareness, and the user behavior concerning frequency of having back up are related to the ICT usage and frequency for commerce and banking purposes. User behaviors for the frequency of scanning computer and using licensed scanner/firewall on personal computers do not have influence on the ICT usage for commerce and banking. Interestingly, for the dependent variables ICT_enjoyment and ICT_commun, test results demonstrate similar results. This means, the relationship between the dependent variables ICT_commun, ICT_enjoyment and the independent variables C_awareness and C_protect are significant. Hence, $H3_{11}$ and $H3_{15}$ are rejected for ICT_commun and $H3_{51}$ and $H3_{55}$ are rejected for ICT_enjoyment. The other hypothesis are accepted in these categories. In other words, security awareness and the behavior using licensed scanner/firewall on personal computers for protection against attacks are significantly related to frequency and reason for using ICT for communication and enjoyment purposes. Additionally, using ICT for education and research purposes is significantly influenced by all the security variables, except behavior for backup frequency (p_value=0.817). In other words, security awareness (p_value=0.000), the behavior of storing critical/valuable info on personal computer (p_value=0.001), scanning frequency (p_value=0.025) and using licensed scanner on personal computers have significant impact on using ICT for research and educational purposes (p_value=0.051).

Finally, test results point that C_awareness (p_value=0.000) and C_backup (p_value=0.000) have significant impact on the dependent variable ICT_profession, thus $H3_{61}$ and $H3_{63}$ are rejected. The other hypotheses are accepted in this category. This can be explained as the relationship between the dependent variable using ICT for professional purposes and the independent variables security awareness and backup frequency is statistically significant. This means, individuals who are using ICT for professional purposes are more computer security aware and intend to have data backup on their personal computers more frequently.

## 7. Conclusions

In this study we have used multivariate regression analysis method. The results demonstrate significant correlations between socio-demographic variables, ICT usage frequency/reason and ICT security indicators with various relation strengths.

Although there are considerable number of socio-demographic and ICT security relations revealed in this study, the most prominent findings listed as;

- socio-demographic factors gender, age, education and ICT experience have significant influence on the awareness of computer security
- ICT experience has meaningful influence on the purpose of ICT usage (commerce, communication, banking, enjoyment and education-and-research)
- using ICT for enjoyment purpose is not correlated with the level of education
- individuals using ICT for professional purposes have more awareness on computer security and intend to get backup for the data stored in their computer more frequently

Our findings are mostly in parallel with results reported by Maslin and Zuraini (Maslin, & Zuraini, 2008) in that they concluded education level and age have impact on computer use and security awareness as well. One of the distinguishing results in our study is that education level does not influence the ICT usage for the purpose of enjoyment. Alternatively, in line with the previous studies (Jin, Drozdenko & Bassett, 2007; Lau, 2003; Gupta, Gould & Pola, 2004; Tan, K. S., Lin & Eze, 2009) findings in this study demonstrate a significant relation between the ICT usage sector and security awareness.

Limitations of present study can be listed as follows. The survey sample was composed of regular people who were randomly subjected to the survey, which may not represent all the

distinct socio-economic layers in the community. Hence, further studies to examine different socio-economic layers in the society, for example professions, may yield interesting results. Additional socio-economic dynamics, i.e. annual income categories, should better be inspected. Another imperative limitation may be the culture of the respondents. Since the studies conducted by Calhoun et al. (Calhoun, Teng & Cheon, 2002), Chirkov et al. (Chirkov, Ryan & Kim, 2003) and several other scientific researchers show that user culture significantly affects the ICT usage behaviors. Hence, a study on the effect of culture difference on the dependent variables inspected in this study would adhere to the generalization of the findings. From an organizational perspective, the discrepancy in ICT usage behaviors among different organizations may also be studied in the future.

## Acknowledgment

We would like to extend our sincere appreciation to The Chamber of Electrical Engineers-Ankara office for their support in conducting the survey.

## References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46. https://doi.org/10.1145/322796.322806

Calhoun, K. J., Teng, J. T., & Cheon, M. J. (2002). Impact of national culture on information technology usage behaviour: an exploratory study of decision making in Korea and the USA. *Behaviour & Information Technology*, *21*(4), 293-302. https://doi.org/10.1080/0144929021000013491

Chirkov, V., Ryan, R. M., Kim, Y., & Kaplan, U. (2003). 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*(1), 97. https://doi.org/10.1037/0022-3514.84.1.97

Choi, K. (2008, November 12). An Empirical Assessment of the Relationships between Demographic Variables and Risk Factors for Computer Crime, Paper presented at the annual meeting of the ASC Annual Meeting, St. Louis Adam's Mark, St. Louis,

Missouri, Retrieved from http://citation.allacademic.com/meta/p_mla_apa_research_citation/2/6/1/6/3/p261632_index.html.

Cilliers, E. J. (2017). The Challenge of Teaching Generation Z. People: International Journal of Social Sciences, 3(1). https://dx.doi.org/10.20319/pijss.2017.31.188198

CSI 2009, Computer Security Institute (2009). CSI 2009 14th Annual CSI Computer Crime & Security Survey, Comprehensive Addition, Computer Security Institute. Retrieved from http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive %20Edition.pdf

CSI 2010/2011, Computer Security Institute (2011). CSI Computer Crime and Security Survey 2010/2011.Retrieved from http://gocsi.com/survey

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, *50*(10), 113-117. https://doi.org/10.1145/1290958.1290971

Fang, X., & Yen, D. C. (2006). Demographics and behavior of Internet users in China. *Technology in Society*, *28*(3), 363-387. https://doi.org/10.1016/j.techsoc.2006.06.005

Feleming N.C., & Nellis J.G. (2000). *Principles of Applied Statistics 2nd Edition*, Thomson Business Press, 2000, ISBN: 1-86152-586-9.

Fisher, Y., & Bendas-Jacob, O. (2006). Measuring internet usage: The Israeli case. *International Journal of Human-Computer Studies*, *64*(10), 984-997. https://doi.org/10.1016/j.ijhcs.2006.05.003

Gatautis, R. (2008). The impact of ICT on public and private sectors in Lithuania. *Engineering economics*, *59*(4).

Gross, J. B., & Rosson, M. B. (2007, March). Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (p. 10). ACM. https://doi.org/10.1145/1234772.1234786

Gupta, P. B., Gould, S. J., & Pola, B. (2004). "To pirate or not to pirate": A comparative study of the ethical versus other influences on the consumer's software acquisition-mode decision. *Journal of Business Ethics*, *55*(3), 255-274. https://doi.org/10.1007/s10551-004-0991-1

Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology (TOIT)*, *8*(4), 16. https://doi.org/10.1145/1391949.1391950

Hui, T. K., & Wan, D. (2007). Factors affecting Internet shopping behaviour in Singapore: gender and educational issues. *International Journal of Consumer Studies*, *31*(3), 310-316. https://doi.org/10.1111/j.1470-6431.2006.00554.x

Jin, K. G., Drozdenko, R., & Bassett, R. (2007). Information technology professionals' perceived organizational values and managerial ethics: An empirical study. *Journal of Business Ethics*, *71*(2), 149-159. https://doi.org/10.1007/s10551-006-9131-4

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015, July). My data just goes everywhere: user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)* (pp. 39-52). Berkeley, CA: USENIX Association.

Lau, E. K. W. (2003). An empirical study of software piracy. *Business Ethics: A European Review*, *12*(3), 233-245. https://doi.org/10.1111/1467-8608.00323

Lightner, N. J., Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2002). Shopping behaviour and preferences in e-commerce of Turkish and American university students: implications from cross-cultural design. *Behaviour & Information Technology*, *21*(6), 373-385. https://doi.org/10.1080/0144929021000071316

Masrom, M., & Ismail, Z. (2008). Examining the influence of demographic factors on ethical awareness: computer use and security. *Living, Working and Learning Beyond*, 558.

Milton, J. S., & Arnold, J. C. (2002). *Introduction to probability and statistics: principles and applications for engineering and the computing sciences*. McGraw-Hill, Inc..

Montero, D., Yannuzzi, M., Shaw, A., Jacquin, L., Pastor, A., Serral-Gracia, R., ... & Nemirovsky, M. (2015). Virtualized security at the network edge: a user-centric approach. *IEEE Communications Magazine*, *53*(4), 176-186. https://doi.org/10.1109/MCOM.2015.7081092

Nurkhin, A., & Arief, S. (2015). The Determinant Of Student's Intention To Use Mobile Learning. *PEOPLE: International Journal of Social Sciences*, *1*(1). https://dx.doi.org/10.20319/pijss.2015.s11.102117

Palfreyman, K., & Rodden, T. (1996, November). A protocol for user awareness on the World Wide Web. In *Proceedings of the 1996 ACM conference on Computer supported cooperative work* (pp. 130-139). ACM. https://doi.org/10.1145/240080.240236

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Shore, B., Venkatachalam, A. R., Solorzano, E., Burn, J. M., Hassan, S. Z., & Janczewski, L. J. (2001). Softlifting and piracy: Behavior across cultures. *Technology in Society*, *23*(4), 563-581. https://doi.org/10.1016/S0160-791X(01)00037-9

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191. https://doi.org/10.1016/j.cose.2015.01.002

Sin Tan, K., Choy Chong, S., Lin, B., & Cyril Eze, U. (2009). Internet-based ICT adoption: evidence from Malaysian SMEs. *Industrial Management & Data Systems*, *109*(2), 224-244. https://doi.org/10.1108/02635570910930118

Teo, T. S., & Lim, V. K. (2000). Gender differences in internet usage and task preferences. *Behaviour & Information Technology*, *19*(4), 283-295. https://doi.org/10.1080/01449290050086390

Thomson, E. S., & Laing, A. W. (2003). "The Net Generation": Children and Young People, the Internet and Online Shopping. *Journal of Marketing Management*, *19*(3-4), 491-512. https://doi.org/10.1080/0267257X.2003.9728221 https://doi.org/10.1362/026725703321663764

UNPAN 2008, From e-Government to Connected Governance. United Nations e-Government Survey 2008, United Nations New York. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf

Ur Rehman, M. S., Salam, Z. A., & Tareq, M. A. (2016). Tele-Pay a Substitute of Conventional Banking: A Conceptual Study. *PEOPLE: International Journal of Social Sciences*, *2*(2). http://dx.doi.org/10.20319/pijss.2016.22.3040

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34-40. https://doi.org/10.1145/1330311.1330320