Individual Differences on Conservative and Risky Behaviors about Information Security

Araştırma Makalesi/Research Article

Onur CERAN, Serçin KARATAŞ

BÖTE, Gazi Üniversitesi, Ankara, Türkiye
onur.ceran@gazi.edu.tr, sercin@gazi.edu.tr
(Geliş/Received:05.03.2020; Kabul/Accepted:17.03.2021)
DOI: 10.17671/gazibtd.697555

Abstract— In order to provide information security; hardware and software solutions are widely used; research and development endeavors increases day by day and huge amounts of investments are made. However, these attempts still cannot stop information systems' to be compromised because of the holes in the human firewall caused by vulnerable behaviors of individuals. Even though individuals have knowledge about information security, they do not always show appropriate behavior. Hence information security is not a problem that can only be solved with technological solutions. As being the weakest link, human behavior on information security needs to be evaluated and assessed. With this study it was aimed to examine the relationship between conservative and risky behaviors of individuals about information security and individual differences which are demographics, internet usage routines, personality, risk perception and exposure to offense. Behaviors and individual difference variables were examined via a survey of 619 participants who were invited through social media platforms. Multiple linear regression analysis conducted and one linear model was created in order to calculate the amount of change on conservative and risky behaviors caused by independent variables. While level of education, age, duration of being an internet user, time spent on the internet, agreeableness, neuroticism, openness, exposure to offence and risk perception variables were found as significant predictors for risky behaviors; time spent on the internet, agreeableness, conscientiousness and openness variables were found to be the significant predictors for conservative behaviors. The results of the study can be used either by organizations or educational institutes for developing personalized and adaptive training programs or for creating preventive strategies.

Keywords: individual differences, information security, risky and conservative behavior, personality, exposure to offence, risk perception

Bilgi Güvenliği Konusunda Korumacı ve Riskli Davranışlarda Bireysel Farklılıklar

Özet— Bilgi güvenliği konusunda donanımsal ve yazılımsal çözümler geniş bir şekilde kullanılmakta, araştırma ve geliştirme çabaları gün ve gün artmakta ve bu konuda büyük miktarda yatırımlar yapılmaktadır. Ancak, bireylerin zarar göremeye eğilimli davranışlarının sebep olduğu hatalardan dolayı, bu uğraşlar bilişim sistemlerinin güvenliğinin aşılmasına hala engel olamamaktadır. Bireyler bilgi güvenliği konusunda yeterli bilgileri olsa dahi bu bilgiyi her zaman davranışa dönüştürememektedirler. Bu sebeple bilgi güvenliği sadece teknolojik çözümler ile üstesinden gelinebilecek bir problem değildir. Bilgi güvenliği konusunda zincirin en zayıf halkası olarak kabul edilen insan davranışları da değerlendirilerek bu yöndeki çalışmalara dâhil edilmelidir. Bu çalışma ile bireylerin bilgi güvenliği konusunda sergilediği riskli ve korumacı davranışlar ile demografik, internet kullanım alışkanlıkları, kişilik, tehlike algısı ve suça maruz kalmadan oluşan bireysel farklılıkları arasındaki ilişki incelenmeye çalışılmıştır. Davranış ve bireysel farklılıklar sosyal medya platformları üzerinden davet edilen 619 kişinin katıldığı bir anket kullanılarak incelenmiştir. Çoklu lineer regresyon analizinin kullanılarak lineer bir modelin oluşturulması ile bireysel farklılıklar olan bağımsız değişkenlerin riski ve korumacı davranışlar üzerindeki meydana getirdiği değişimin boyutu hesaplanmıştır. Buna göre eğitim düzeyi, yaş, internet kullanım yılı, internette geçirilen zaman, uyumluluk, nevrotizm, gelişime açıklık, suça maruziyet durumu ve tehlike algısı riskli davranışları; internette geçirilen zaman, uyumluluk, özdenetim ve gelişime açıklık korumacı davranışları etkileyen önemli değişkenler olarak bulunmuştur. Çalışmanın sonuçları organizasyonların veya eğitim birimlerinin kişiselleştirilmiş ve uyarlanabilir eğitim programları geliştirmeleri için kullanılabileceği gibi bu sonuçlardan önleyici stratejiler oluşturmak için de faydalanılabilir.

Anahtar Kelimeler: bireysel farklılıklar, bilgi güvenliği, riskli ve korumacı davranışlar, kişilik, suça maruz kalma, tehlike algısı

1. INTRODUCTION

With the developments in communication and information systems, human life evolved in terms of daily processes. Especially after the invention of the World Wide Web in 1980s and smart phones in 2000s, time and location terms have disappeared for daily transactions. On one hand, easily accessible and convenient technological innovations facilitate our lives, on the other hand they also caused global issues of cyber-criminal activities [1]. Being sorted as one of the most common cyber threats [2], phishing is defined as a form of social engineering attack that tries to acquire sensitive information from people by impersonating a trustworthy third party [3], instead of technically directed attacks [4]. Any information which can be used for distinguishing one person from another by itself or by combining it with another is called as personally identifiable information (PII) [5]. Social media platforms which have billions of subscribers are valuable resources to find PIIs for intruders [6] in order to make social engineering attacks. Mitnick and Simon [7] state that state-of the-art security technologies may not protect organization's network and computer systems from attackers who performs social engineering methods and tactics to compromise.

According to SANS IT security spending trends report [8] demonstrates that organizations are mainly spending their resources on 5 technologies such as access and authentication, advanced malware prevention, endpoint security, wireless security and data protection/encryption. But Levi [9], in his study, in which he tries to figure out trends on cybercrimes in police records of developed countries such as Australia, Canada, Germany, Hong Kong, Netherlands, Sweden, UK and US, emphasizes the substantial rise in online fraud. According to Federal Bureau of Investigations' (FBI) Internet Crime Report [10], while 301.580 complaints were reported resulted in loss of 1.418,7 million dollars in 2017, 351.937 complaints were reported resulted in loss of 2.706,4 million dollars in 2018. When the statistics are examined, it is obvious that investment only for IT technologies does not decreases the users' exposure to cyber security incident or amount of money which is lost. Lineberry [11] underlines the importance of security awareness training and argues that although organizations spend large percentage of their IT security budgets by buying high-tech tools, the attackers target generally untrained, uniformed and unmonitored users. AlHogail [12] argues that employees within an organization can protect themselves from insider threats through security behaviors and perceptions. As Morgan [13] states that 90 percent of successful hacking attempts start with phishing attack, however information security mostly focuses on technological solutions, it is quite important to take into consideration non-technology-related issues like human behavior [14]. As a conclusion to matters mentioned above, information security is not a problem that can only be solved with technological solutions. As being the weakest link, human behavior and awareness on information security needs to be evaluated and assessed. The main purpose of this study is to examine the relationship between conservative and risky behaviors of individuals about information security and individual differences.

2. RELATED WORK

Although information and communication technologies are evolving to increasingly complex structures, cyber criminals are also adapting their techniques to compromise these systems [15]. Hence, it is acceptable that the greater part of the studies on information security are related with protecting the information systems via technical solutions like software/hardware systems. However, as stated in the study of Zhang et al. [16] human and specifically their awareness is one of the key factor on information security and it has been studied by academia and industry progressively. Ayyagari [17] stated that breaches because of hacking attempts are decreasing while the breaches due to human factor are increasing as a result of analysis with 2633 unique data breaches.

Based on these findings, affecting factors of human behavior on information security has been studied in the academic sphere. Egelman and Peer [18] studied psychological relations to be correlated with individuals' security behaviors. The results of the study indicate that individuals who are eager to take risks on health and safety, do have a tendency not to keep an updated software and show proactive awareness. McCormac et al [19] investigate the relationship between knowledge, attitude, behaviors of individuals on information security, with individual factors such as age, gender, personality, risk-taking propensity and organizational factors. The study which is carried out with 505 Australians who work in an organization where there should be a formal information security policy, figures out that individual factors affect what people actually do about information security (IS) within what they know about policies and procedures and why they should do about IS. The results of study show that the younger adults got lower information security awareness scores than older ones. Furthermore, according to personality scores the study indicates that individuals who got higher scores on agreeableness, openness and conscientiousness also got high scores on IS and got fewer scores on taking risks in reverse. Dodel and Mesch [20] figure out which factors affect individuals' preventive cyber-safety behavior of using anti-virus software. The study conducted with 1850 Israeli internet users, emphasize that age, gender, educational level and internet usage frequency determines their preventive cyber-safety behavior. Shropshire et al. [21] examine the usage of endpoint security software towards personality, perceived organizational support, perceived usefulness and ease of use. The results of study show that conscientiousness and agreeableness in terms of personality are the major predictors of relationship between intention and actual usage of endpoint security software. It also indicates that perceived ease of use affects perceived usefulness which has a strong relationship with intention to use endpoint security software. Halevi et al. [22] investigate the relationship between personality and individuals' phishing

vulnerability and risky behavior of sharing of personally identifiable information. Nevertheless, authors indicate that that the ones who are willing to try new experiences, which is called as openness, are prone to share more information online and set less conservative privacy settings on social media platforms.

Perception of danger or risk and victimization influencing people's decision and behavior are also studied in the literature. Hajli and Lin [23] emphasize that if individuals perceive it risky they are less willing to share information about themselves on social media platforms. According to results of the study of Yucedal [24], in which factors impacting the victimization in cyberspace is examined, users who are willing to decrease the risk of being a victim and use preventive tools like firewalls or anti-virus programs are the ones who report infections more. Ybarra et al. [25] figure out the relationship between personal information sharing and talking strangers online and victimization. The study shows that risky behaviors of talking about sex and meeting with strangers online increase the odds of being a victim.

The conducted literature review indicates that human behavior on information security is affected by many different individual factors. However, related studies in the domain mainly focus on examining the relation between awareness and behaviors on information security. Although one individual has the knowledge on the risk of sharing PII through internet, the said individual may take the risk according to his/her personality. Nicholson et al. [26] that one individual who is even familiar or unfamiliar with the technology may not show conservative behavior to a risky situation regardless of his/her age. Even though having knowledge about information security is one of the key elements, it is not enough to explain behaviors on the subject. Therefore, the current study focuses on examining the individual factors and differences which may affect conservative and risky behaviors about information security.

3. METHOD

3.1 Data Collection

Data collection was carried out with an online survey through web-based survey tool, namely Google Forms. The survey was available for participants for a 2 months period. Announcement for participation was done through social media platforms and e-mail groups. In the announcement content, it was mentioned that participants would be awarded by drawing, with some gifts provided by information security firms. Furthermore, it was also requested from participants to share the content through their social media accounts or to forward it to mail groups which they are member of.

3.2 Participants

Six hundred and nineteen (619) individuals participated in the online survey. It was aimed to reach as much participants as possible. Taking into consideration that any individual who uses a smartphone or makes any transactions on the internet may be a victim of a fraud, data collection was carried out without an age restriction.

3.3 Materials

3.3.1 Demographics

Within the survey, general demographic information including gender and age were collected. In the survey, age information was collected as birth date and converted to generation groups. Due to the fact that people's perceptions, priorities, missions, visions and behaviors are effected by the factors such as environment, important events, life and work experiences; meanwhile a distinction on age groups was made according to period of consecutive years contributing values of individuals which is called as generations [27]. Generations of the participants were defined according to the study of Adıgüzel et al. [28] which consists of five groups: Silent generation (born before 1946), baby-boomers (born between 1946 and 1965), generation-x (born between 1965 and 1979), generation-y (born between 1979 and 1995) and generation-z (born after 1995).

3.3.2 Socio-Demographics

Level of education is defined according to the Turkish education system which is mostly parallel to the majority of the world. The level of education includes primary school, high school, associate, bachelor, master and doctoral degrees. Duration of time spent on the internet (daily) and duration of being an internet user (as years) were also collected as socio-demographic information within the survey.

3.3.3 Risky and Conservative Behavior Scales (RBS and CBS)

While risky behavior scale measures the risk degrees of end users through their behaviors, conservative behavior scale measures how an end user shows protective and careful behavior while using information systems. Items are measured on a five point Likert-style scale. The items are measured by assigning points ranges from 1 (never) to 5 (always). While high scores on risky behavior scale indicates that the participant shows highly tolerant behavior, high scores on conservative behavior scale indicates that the participant shows protective and safe behaviors while using information systems [29]. These scales are not bipolar. Data collected from 62 participants suggest a good reliability with an alpha level of 0, 9345 [30]. All permissions are obtained for the scales to be used in this study from the author.

3.3.4 The Big Five Inventory (BFI)

The big five inventory measures an individual's personality through 5 dimensions which are extraversion, agreeableness, conscientiousness, neuroticism and openness. Inventory consists of 44 items (8 for

extraversion, 9 for agreeableness, 9 for conscientiousness, 8 for neuroticism and 10 for openness) measured on five point Likert-style scale ranging from 1 (strongly disagree) to 5 (strongly agree) [31]. Sümer and Sümer [32] adopted the BFI into Turkish Language within a study carried out with 56 countries in order to figure out BIF traits patterns and profiles of human self-description [33]. The cronbach alpha level of Turkish Language version of BFI moderated from 0.66 to 0.77 [34]. All permissions are obtained for the Turkish Language version of the inventory to be used in this study from the author.

3.3.5 Risk Perception and Exposure to Offence Scales (RPS and EOS)

Risk perception scale determines users' perception on information systems or technologies in terms of degree of danger which is conceptually and closely related with trust. Items are measured on a five point Likert-style scale. The items are measured by assigning points ranges from 1 (no idea) to 5 (very dangerous). Exposure to offence scale measures users' exposure any information security breach or incident because of either intentional or unintentional behavior in which the items are designed together with General Directorate of Security Cyber Crime branch and Turkish Information Security Association. The items are measured by assigning points ranges from 1 (never) to 5 (always) [29].

4. RESULTS

The main purpose of this study is to examine the relationship between conservative and risky behaviors of individuals about information security and individual differences. The relationship between demographic and socio-demographic differences were also examined. A correlation matrix is provided in Table 1. to examine the relationship between variables.

4.1 Demographics and Socio-Demographics

Six hundred and nineteen individuals (240 (%38.8) of them were male and 379 (%61.2) of them were female) participated in the online survey. Examining the age groups, %64 of the participants were in generation-Y, which was the most crowded group, %17.9 were in generation-X, %15 were in generation-Z and %3.1 were in baby boomer, which was the least crowded group. Approximately %60 of participants had a graduation degree of bachelor and above; %40 of them had a graduation degree of high school and below. Only %5.5 of the participants were internet users for 6 years and below; %94.5 of them were internet users for 7 years and above. Examining the participants' daily time spent on the internet, %81.1 of them are surfing for 3 hours and more.

4.1.1 Gender

Examining the relationship between gender and age, level of education, duration of time spent on the internet and duration of being an internet user, RPS, EOS, RPS and CBS; significant negative correlation ($p<0.01$) with duration of being an internet user ($p=0.000$, $r=-.229$) and negative correlation ($p<0.05$) with duration of time spent on the internet ($p=0.044$, $r=-.081$) were found. Specifically, it was found that %17.5 of males and %34.3 of females were internet users for 7-10 years. However, %42.5 of males and %21.9 of females were internet users for more than 15 years. Significant negative correlation was found between gender and CBS ($p=.003$, $r=-.119$) and EOS ($p=.009$, $r=-.104$). When compared to female participants ($M=42.69$, $SD=15.663$), it was found that male participants ($M=45$, $SD=15.03$) showed more protective and careful behavior while using information systems. Analyses also showed that male participants ($M=5.99$, $SD=7.482$) were exposed to crime or negative experience more than female participants ($M=4.64$, $SD=5.368$).

4.1.2 Age Group

Examining the relationship between age and level of education, duration of time spent on the internet and duration of being an internet user; significant negative correlation with level of education ($p=0.000$, $r=-.320$) and duration of being an internet user ($p=0.000$, $r=-.342$) and positive correlation with duration of time spent on the internet ($p=.021$, $r=.093$) were found. It was found that there was a negative correlation between age group and RPS ($p=.025$, $r=-.090$) and significant negative correlation with CBS ($p=.001$, $r=-.132$) and RPS ($p=.002$, $r=.124$). While studying younger groups, one could observe more protective and careful behavior (Baby-boomers, $M=35.79$, $SD=20.305$; generation-x, $M=43.55$, $SD=15.536$; generation-y, $M=44.03$, $SD=15.248$; generation-z, $M=37.38$, $SD=14.249$) and the perception on information technologies was assessed to be more trustworthy (Baby-boomers, $M=52.00$, $SD=15.055$; generation-x, $M=54.33$, $SD=15.241$; generation-y, $M=51.69$, $SD=14.849$; generation-z, $M=48.66$, $SD=15.541$).

4.1.3 Level of Education

Examining the relationship between level of education and duration of being an internet user significant positive correlation ($p=0.000$, $r=.412$) was found. Results suggested that there was a positive correlation between level of education and CBS ($p=.043$, $r=.081$) and significant positive correlation with RBS ($p=.000$, $r=.211$) and RPS ($p=.002$, $r=.124$). Although the effect was small, as the level of education increased participants showed more protective and careful behavior while using information systems. Analysis indicated that participants showed more tolerant, risky behavior while using information systems or technologies (Primary school, $M=25.33$, $SD=9.109$; high school, $M=30.42$, $SD=14.094$; associate, $M=29.94$, $SD=12.362$; bachelor, $M=34.88$, $SD=12.245$; master, $M=36.71$, $SD=10.255$; doctoral, $M=38.44$, $SD=15.009$) although their perception on information technologies got more untrustworthy (Primary school, $M=25.33$, $SD=9.109$; high school, $M=30.42$, $SD=14.094$; associate, $M=29.94$, $SD=12.362$; bachelor, $M=34.88$, $SD=12.245$; master, $M=36.71$, $SD=10.255$; doctoral, $M=38.44$, $SD=15.009$) as their level of education increased.

Table 1. Correlations between demographics, socio-demographics, risky and conservative behaviors, risk perception and exposure to offence

Variables	*Gender*	*Age Group*	*Level of Education*	*Duration of being an Internet User*	*Time spent on the Internet*	*RPS*	*EOS*	*RBS*	*CBS*
Gender	-					-,053	-,104**	-,012	-,119**
Age Group	,058	-				-,090*	,028	,062	-,132**
Level of Education	-,066	-,320**	-			,124**	,002	,211**	,081*
Duration of being an internet user	-,229**	-,342**	,412**	-		,149**	,022	,130**	,136*
Time spent on the internet	-,081*	,093*	,021	0,24	-	,002	,038	,261**	,173**

* p < 0.05 (2-tailed) ** p < 0.01 (2-tailed)

4.1.4 Duration of Being an Internet User (DBIU)

Results suggested that duration of being an internet user showed significant positive correlation with CBS (p=0.001, r=.136), RBS (p=0.001, r=.130) and RPS (p=0.000, r=.149). Participants got higher scores on CBS (3-6 years, M=37.59, SD=20.074; 7-10 years, M=41.05, SD=15.210; 11-15 years, M=42.36, SD=16.020; 15+ years, M=45.57, SD=13.751); RBS (3-6 years, M=23.18, SD=13.726; 7-10 years, M=33.26, SD=13.170; 11-15 years, M=35.18, SD=11.586; 15+ years, M=35.32, SD=12.471) and RPS (3-6 years, M=47.53, SD=14.431; 7-10 years, M=49.45, SD=17.552; 11-15 years, M=51.60, SD=14.585; 15+ years, M=54.74, SD=12.676) as the duration of being an internet user increased.

4.1.5 Time Spent on the Internet (TSI)

Similar to duration of being an internet user, participants' time spent on the internet showed significant positive correlation with CBS (p=0.000, r=.173) and RBS (p=0.000, r=.261). Participants who spend more time daily on the internet got higher scores on CBS (0-2 hours, M=40.19, SD=16.158; 3-5 hours, M=40.92, SD=14.745; 6-10 hours, M=45.14, SD=15.733; 11+ hours, M=49.81, SD=14.431) and RBS (0-2 hours, M=28.46, SD=11.891; 3-5 hours, M=32.96, SD=11.696; 6-10 hours, M=36.72, SD=13.244; 11+ hours, M=39.85, SD=12.558).

4.2 Behaviors about Information Security

As the main purpose of this study is to examine the relationship between conservative and risky behaviors of individuals about information security and individual differences, multiple linear regression analysis was conducted in order to investigate which of the independent variables explain the changes on dependent variables of CBS and RBS. With multiple linear regression analysis, one linear model was created in order to calculate the amount of change on CBS and RBS caused by 1-unit change in independent variables.

4.2.1 Conservative Behaviors

According to Table 2., it was concluded that regression model explained a significant amount of the variance

(p=0.000 <0.05) and Table 3. showed that the adjusted R^2 of our model was .903 with the R^2 = .905 which means that the linear regression explained 90.5% of the variance in the data.

Table 2. Significance level of model for CBS

Model	*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
Regression	1155235,589	12	96269,632	480,338	,000
Residual	121655,411	607	200,421		
Total	1276891,000	619			

Table 3. Model summary for CBS

R	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
,951	,905	,903	14,157

Table 4. showed that independent variables of time spent on the internet, agreeableness, conscientiousness and openness were significant predictors for CBS. Figure.1 illustrates how much unit effected to be changed is seen on CBS when the dedicated independent variables change for every 1-unit.

Table 4. Coefficients for CBS

Independent Variables	*Unstandardized Coefficients*		*Standardized Coefficients*		
	B	*Std. Error*	*Beta*	*t*	*Sig.*
Gender	-2,121	1,201	-,079	-1,767	,078
Level of Education	,190	,560	,016	,338	,735
Age	-1,470	,843	-,069	-1,743	,082
DBIU	1,027	,721	,069	1,425	,155
TSI	**3,818**	**,671**	**,203**	**5,686**	**,000**
Agreeableness	**,249**	**,098**	**,186**	**2,541**	**,011**
Conscientiousness	**,450**	**,094**	**,338**	**4,809**	**,000**
Neuroticism	-,089	,087	-,040	-1,023	,307
Openness	**,384**	**,083**	**,269**	**4,645**	**,000**
Extraversion	,029	,090	,017	,320	,749
EOS	-,018	,092	-,003	-,197	,844
RPS	,050	,037	,059	1,341	,181

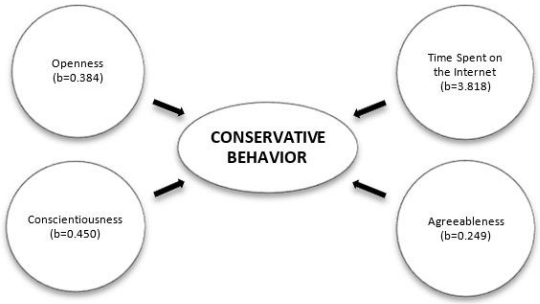

Figure 1. Variance for CBS explained by the individual differences

4.2.2 Risky Behaviors

According to Table 5. it was concluded that regression model explained a significant amount of the variance ($p=0.000 <0.05$) and Table 6. shows that the adjusted R^2 of our model was .898 with the $R^2 = .900$ which means that the linear regression explained 90% of the variance in the data.

Table 5. Significance level of RBS

Model	*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
Regression	723175,349	12	60264,612	454,549	,000
Residual	80476,651	607	132,581		
Total	803652,000	619			

Table 6. Model summary for RBS

R	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
,949	,900	,898	11,514

Table 7. Coefficients for RBS

Independent Variables	*Unstandardized Coefficients*		*Standardized Coefficients*		
	B	*Std. Error*	*Beta*	*t*	*Sig.*
Gender	,298	,976	,014	,306	,760
Level of Education	**2,673**	**,456**	**,286**	**5,865**	**,000**
Age	**2,364**	**,686**	**,140**	**3,448**	**,001**
DBIU	**1,343**	**,586**	**,113**	**2,291**	**,022**
TSI	**3,303**	**,546**	**,221**	**6,049**	**,000**
Agreeableness	**,182**	**,080**	**,172**	**2,284**	**,023**
Conscientiousness	-,139	,076	-,131	-1,822	,069
Neuroticism	**,153**	**,070**	**,087**	**2,169**	**,030**
Openness	**,170**	**,067**	**,150**	**2,532**	**,012**
Extraversion	,104	,073	,076	1,423	,155
EOS	**,175**	**,075**	**,040**	**2,336**	**,020**
RPS	**-,116**	**,030**	**-,173**	**-3,840**	**,000**

Figure 2. Variance for RBS explained by the individual differences

Table 7. showed that independent variables of level of education, age, duration of being an internet user, time spent on the internet, agreeableness, neuroticism, openness, exposure to offence and risk perception were significant predictors for RBS. Figure -2 illustrates how much unit effected to be changed is seen on RBS when the dedicated independent variables change for every 1-unit.

5. DISCUSSION

In this study, we examined mainly the relationship between conservative and risky behaviors of individuals about information security and individual differences. We also provided information about the relationship between demographic and socio-demographic variables which may affect behaviors on information security. This study may contribute to the literature both theoretically and in practicability. Even though all applicants are Turkish citizens who live in Turkey, since the information gathered is common and the scales are applicable regardless of geographical location, this study is repeatable to see the overall situation within a country, a city or even an institution. Methodology and the results of this study may be applied on individualized and adaptive training programs about information security.

In the following section, findings on relationship between variables, individual differences and behaviors about information security will be discussed.

5.1 Demographics and Socio-Demographics

Analysis showed that male participants started being a user on internet before than female participants. Furthermore, male participants spend more time on the internet than the female participants on a daily basis. It was found that

generation-z spent more time on the internet than generation-y and generation-y spent more time on the internet than generation-x. Turkish Statistical Institute's (TUIK) survey on information and communication technology usage in households and by individuals [35] reported parallel results. Report showed that females spent almost same but slightly less time on internet than males. It also emphasized that with the increase of the age people tend to spend less time on internet. Within the study, the expected results showed that the participants who are younger were in lower education level and shorter period of time being an internet user. These results and report by TUIK proved that data collected within this study is compatible with the normal flow of life.

Regression analyses showed that while spending more time on internet caused participants to use risk involving information technologies more, it also provided participants to behave more protective and carefully while using them. This was also reported by Öğütçü et al. [29] mentioning that respondents, who spend more time on internet, use risk included information technologies more and also have a tendency to protect themselves more. Analyses showed that there was no correlation between times spent on internet and duration of being an internet user. Although being an internet user for longer time caused participants to behave comparatively riskier, however it did not show any effect on conservative behaviors while using information technologies. That is supported by Halevi et al. [22] who found that participants who uses internet more are more aware of its risks but they are not able to defend themselves better and that the real-time response is less dependent on their awareness.

While observing a younger age group, participants' risky behavior score increased. This was also reported by Sheng et al. [36] who found that people between 18 and 35 are more susceptible to phishing emails than older groups of age due to the fact that younger individuals seems to behave in a riskier manner. The results of the study of Whitty et al. [37] showed that younger age groups were likely to show the risky behavior of sharing passwords, compared with older age groups.

Having higher educational degree affected the rate of showing riskier behavior about information security. Zukowski and Brown [38] suggested that internet users who have lower level of education are more concerned about information privacy than users with higher level of education. This finding align with the research of Fatokun et al. [39] who found that postgraduates, who made more progress in life, acted riskier on information security cautions than undergraduates, who were more controllable and guarded by parents. Although there are researches in the literature [36], [40], [41] mentioning the effect of gender on behaviors about information security, gender was not found to be as a significant predictor within the current study.

5.2 Personality, Risk Perception and Exposure to Offense

Identifying the personality characteristics which may cause risky behaviors or provide conservative behaviors is an important step to create strategies for preventing information security threats. Regression analyses were also conducted in order to investigate the impact of personality on conservative and risky behaviors about information security. It was found that while openness and agreeableness had an effect on both conservative and risky behaviors, their impact on conservative behaviors were relatively significant. Govani and Pashley [42] and Debatin et al. [43] indicated that although users claimed that they understood the issues about privacy, benefits of sharing personal information was perceived remarkably higher than the risk linked to it. This shows that risky behavior may also be seen with conservative behavior together due to the fact that many users underestimate or ignore the risks while focusing on the advantages of the information technology. While conscientiousness was found to be positive effect on conservative behavior, neuroticism had a positive influence on risky behavior about information security.

Parallel to current study, McCormac et al. [41] found that individuals, who were more conscientious, agreeable and open, got higher information security awareness scores which were linked to more conservative and less risky knowledge, attitude and behavior [44]. According to Warkentin et al.'s [45] study, more agreeable participants demonstrated greater care on protecting their data than less agreeable ones. Shropshire et al. [21] indicated that conscientiousness and agreeableness were linked to secure behaviors. Furthermore, it was found that the relationship between intention and conservative behavior of using security software got stronger when the level of agreeableness and conscientiousness got higher. These findings were also supported by Alohali et al. [46] who found that conscientiousness, agreeableness and openness were negatively correlated with the risk level of security behavior showing that participants with higher scores among these personality threats tend to behave more conservative while using information systems or technologies. On the other hand, Halevi et al.'s [22] study showed that woman participants who had higher scores on neuroticism in which high level tend to become more vulnerable to different addictions behaved riskier causing them to be more susceptible to phishing attacks. According to results of Sumner et al.'s [47] study, which was carried out with 537 participants from 15 different countries, risky behaviors of sharing personally identifiable information on social media was mediated by neuroticism, openness and agreeableness. Based on the results of Kelley's [48] study it was found that those who score high on neuroticism tend to be less cyber secure because of risky behaviors within the security behaviors survey.

According to Nicholson et al. [26], individual's risk taking level is relative and may change due to the situation. Loss or gain with the outcome defines the behavioral change of individuals. Their study, which was handled with 2151 research participants, suggested that risk taking would be

predicted through high scores on openness and low scores on neuroticism, agreeableness and conscientiousness. Johnston et al. [49] emphasized that insiders who shows more openness tend to behave risky if they may get a benefit from added risk within the context of information security policy violations. Gratian et al. [50] found that willingness of users on taking risks significantly correlated with security behaviors of said users. Study of Korzaan and Boswell [51], which was carried out with 230 participants in order to find out the influence of personality traits and information privacy concerns on behavioral intentions, indicated that agreeableness and neuroticism had a positive influence on concerns for information privacy and computer anxiety. Within that framework, the result supports the current study in the fact that risk perception has a negative influence on risky behavior about information technologies.

One of the key findings of the current study was that exposure to offence within the context of information security affected risky behavior positively. Bulgurcu et al. [52] emphasized that direct negative life experiences may affect building awareness on information security. On the contrary, according to our study, participants who were exposed to offence tended to have unchanged behavior or with riskier behavior. In addition to that, the difference may be related with the risk-perception or the benefit that would be gained after said risky behavior although it may cause an offense. This result shows a parallelism to Wittebrood and Nieuwbeerta [53], who emphasize that individuals follow patterns of their routine activities, once one falls victim, that individual would have a greater risk of becoming a victim subsequently.

6. LIMITATIONS

Although current study makes both theoretical and applied contributions, further research is still required because of a number of limitations. It is important to note that the data collection relied on a subjective method which is self-reported survey. Thus, the study is not able to assert to provide insight into actual user behaviors. In order to assure confidentiality and anonymity and to prevent socially desirable responses, participants were not forced to provide personally identifiable information such as name, surname, ID number or nickname. However, the gifts for participants might have caused multiple participation because of inexistency of a mechanism checking it through personal information. Random clicking should also be taken into consideration.

There are huge number of factors that may affect individual behaviors to either comply or violate information security policies or rules [54]. For instance, Vroom and Von Solms [55] examined culture, Warkentin et al. [45] studied self-efficacy and threat severity, Flores and Ekstedt [56] figured out organizational factors affecting information security. However, they have not been examined in the current study. The scope of factors examined in this study is limited with aforementioned.

7. CONCLUSION

This study examined the relationship between conservative and risky behaviors of individuals about information security and individual differences. It was found that conscientiousness has a significant effect on conservative behaviors; level of education, age, duration of being an internet user, neuroticism, exposure to offence and risk perception have significant effect on risk behaviors about information security. The time spent on the internet, agreeableness and openness were found to be affecting both behaviors. Tan et al. [57] created an adaptive web based learning system in which the systems automatically decides the amount of the content to be shown to user according to learners' prior knowledge on information security and learning speed. Pattinson et al [58] put forth a concept framework of information security training considering individual differences of learning preferences. Hatzivasilis et al. [59] developed an adoptable training program and a pilot system about cyber-security considering trainee type, trainee's needs and his/her performance. Our findings have implications for institutes and organizations as they can help to develop personalized training programs.

REFERENCES

[1] R. Sarre, L. Y.-C. Lau, and L. Y. Chang, "Responding to cybercrime: current trends", *Taylor & Francis*, 19(6), 515-518, 2018.

[2] H. Berger and A. Jones, "Cyber Security & Ethical Hacking For SMEs", **11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society,** 2016.

[3] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing", *Communications of the ACM*, 50(10), 94–100, 2007.

[4] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", *Journal of Information Security and applications*, 22, 113–122, 2015.

[5] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks", **2nd ACM workshop on Online social networks**, Barcelona, Spain, 2009.

[6] Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T.J., Kruegel, C., McCoy, D., Savage, S. and Vigna, G., "Framing dependencies introduced by underground commoditization", 2015.

[7] K. D. Mitnick, W. L. Simon, **The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers,** John Wiley & Sons, 2009.

[8] B. Filkins, "**IT Security Spending Trends**", SANS, 2016.

[9] M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and issues", *Crime, Law and Social Change*, 67(1), 3–20, 2017.

[10] M. Gorham, **Internet Crime Report,** Internet Crime Complaint Center, FBI National Press Office, Annual (202) 324- 3691, 2018.

[11] S. Lineberry, "The human element: The weakest link in information security", *Journal of Accountancy*, 204(5), 44, 2007.

[12] A. AlHogail, "Design and validation of information security culture framework", *Computers in Human Behavior*, 49, 567–575, 2015.

[13] S. Morgan, **2019 Official Annual Cybercrime Report,** Herjavec, 2019.

[14] D. Trček, R. Trobec, N. Pavešić, and J. F. Tasič, "Information systems security and human behaviour", *Behaviour & Information Technology*, 26(2), 113–118, 2007.

[15] D.-E. Neghina and E. Scarlat, "Managing information technology security in the context of cybercrime trends", *International journal of computers communications & control*, 8(1), 97–104, 2013.

[16] J. Zhang, B. J. Reithel, H. Li, "Impact of perceived technical protection on security behaviors", *Information Management & Computer Security*, 2009.

[17] R. Ayyagari, "An exploratory analysis of data breaches from 2005-2011: Trends and insights", *Journal of Information Privacy and Security*, 8(2), 33–56, 2012.

[18] S. Egelman, E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (sebis)", *33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882, 2015.

[19] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *computers & security*, 42, 165–176, 2014.

[20] M. Dodel, G. Mesch, "Cyber-victimization preventive behavior: A health belief model approach", *Computers in Human behavior*, 68, 359–367, 2017.

[21] J. Shropshire, M. Warkentin, S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *computers & security*, 49, 177–191, 2015.

[22] T. Halevi, J. Lewis, N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits", *22nd International Conference on World Wide Web*, 737–744, 2013.

[23] N. Hajli, X. Lin, "Exploring the security of information sharing on social networking sites: The role of perceived control of information", *Journal of Business Ethics*, 133(1), 111–123, 2016.

[24] B. Yucedal, "**Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories**", Doctoral Dissertation, Kent State University, 2010.

[25] M. L. Ybarra, K. J. Mitchell, D. Finkelhor, J. Wolak, "Internet prevention messages: Targeting the right online behaviors", *Archives of Pediatrics & Adolescent Medicine*, 161(2), 138–145, 2007.

[26] N. Nicholson, E. Soane, M. Fenton-O'Creevy, P. Willman, "Personality and domain-specific risk taking", *Journal of Risk Research*, 8(2), 157–176, 2005.

[27] J. Bejtkovský, "The current generations: the baby boomers, x, y and z in the context of human capital management of the 21st century in selected corporations in the Czech Republic", *Littera scripta*, 9(2), 25–45, 2016.

[28] O. Adıgüzel, H. Z. Batur, N. Ekşili, "Kuşakların değişen yüzü ve Y kuşağı ile ortaya çıkan yeni çalışma tarzı: Mobil yakalılar", *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1(19), 165–182, 2014.

[29] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness", *Computers & Security*, 56, 83–93, 2016.

[30] Öğütçü, "**E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığı Analizi**", Master Thesis, Başkent University, 2010.

[31] O. P. John and S. Srivastava, "The Big Five trait taxonomy: History, measurement, and theoretical perspectives", **Handbook of personality: Theory and research**, 2(1999), 102– 138, 1999.

[32] Internet: Sümer, H. C. Sümer, Beş faktör kişilik özellikleri ölçeği https://scholar. google.com.tr, 10.05.2020.

[33] D. P. Schmitt, J. Allik, R. R. McCrae, V. Benet-Martínez, "The geographic distribution of Big Five personality traits: Patterns and profiles of human self-description across 56 nations", *Journal of cross-cultural psychology*, 38(2), 173–212, 2007.

[34] N. Sümer, T. Lajunen, T. Özkan, "Big five personality traits as the distal predictors of road accident", *Traffic and transport psychology: Theory and application*, 215, 215–227, 2005.

[35] TUİK, "**Hanehalkı Bilişim Teknolojileri Kullanım Araştırması**", 2016.

[36] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", *SIGCHI Conference on Human Factors in Computing Systems*, 373–382, 2010

[37] M. Whitty, J. Doodson, S. Creese, D. Hodges, "Individual differences in cyber security behaviors: an examination of who is sharing passwords", *Cyberpsychology, Behavior, and Social Networking*, 18(1), 3–7, 2015.

[38] T. Zukowski, I. Brown, "Examining the influence of demographic factors on internet users' information privacy concerns", **2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries**, 197–204, 2007.

[39] F. B. Fatokun, S. Hamid, A. Norman, J. O. Fatokun, "The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities", *Journal of Physics: Conference Series*, 1339, 2019.

[40] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, L. Xu, "Gender difference and employees' cybersecurity behaviors", *Computers in Human Behavior*, 69, 437–443, 2017.

[41] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness", *Computers in Human Behavior*, 69, 151–156, 2017.

[42] T. Govani and H. Pashley, "Student awareness of the privacy implications when using Facebook," *Unpublished paper presented at the "Privacy poster fair" at the Carnegie Mellon university school of library and information science*, 9, 1–17, 2005.

[43] B. Debatin, J. P. Lovejoy, A.-K. Horn, B. N. Hughes, "Facebook and online privacy: Attitudes, behaviors, and unintended consequences", *Journal of computer-mediated communication*, 15(1), 83–108, 2009.

[44] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers & Security*, 66, 40–51, 2017.

[45] M. Warkentin, M. McBride, L. Carter, A. Johnston, "The role of individual characteristics on insider abuse intentions", *AMCIS*, 2012.

[46] M. Alohali, N. Clarke, F. Li, S. Furnell, "Identifying and predicting the factors affecting end-users' risk-taking behavior", *Information & Computer Security*, 2018.

[47] C. Sumner, A. Byers, and M. Shearing, "Determining personality traits & privacy concerns from facebook activity", *Black Hat Briefings*, 11(7), 197–221, 2011.

[48] D. Kelley, "Investigation of attitudes towards security behaviors", *McNair Research Journal SJSU*, 14(1), 10, 2018.

[49] A. C. Johnston, M. Warkentin, M. McBride, L. Carter, "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems*, 25(3), 231–251, 2016.

[50] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, A. Ginther, "Correlating human traits and cyber security behavior intentions", *computers & security*, 73, 345–358, 2018.

[51] M. L. Korzaan, K. T. Boswell, "The influence of personality traits and information privacy concerns on behavioral intentions", *Journal of Computer Information Systems*, 48(4), 15– 24, 2008.

[52] B. Bulgurcu, H. Cavusoglu, I. Benbasat, "Information security policy compliance: an empirical study of rationality- based beliefs and information security awareness", *MIS quarterly*, 34(3), 523–548, 2010.

[53] K. Wittebrood, P. Nieuwbeerta, "Criminal victimization during one's life course: The effects of previous victimization and patterns of routine activities", *Journal of research in crime and delinquency*, 37(1), 91–122, 2000.

[54] G. Dhillon, J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Communications of the ACM*, 43(7), 125–128, 2000.

[55] C. Vroom, R. Von Solms, "Towards information security behavioural compliance", *Computers & Security*, 23(3), 191–198, 2004.

[56] W. R. Flores, M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness", *computers & Security*, 59, 26–44, 2016.

[57] Z. Tan, R. Beuran, S. Hasegawa, W. Jiang, M. Zhao, and Y. Tan, "Adaptive security awareness training using linked open data datasets", *Education and Information Technologies*, 25, 5235–5259, 2020.

[58] M. Pattinson *et al*., "Matching training to individual learning styles improves information security awareness", *Information & Computer Security*, 2019.

[59] G. Hatzivasilis *et al.*, "Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees", *Applied Sciences*, 10(16), 5702, 2020.