INFORMATION SECURITY IN THE WORLD OF DIGITAL NATIVES: HOW INTERNET ADDICTION, SENSATION SEEKING AND INFORMATION SECURITY BEHAVIORS ARE RELATED

[1]GIZEM OGUTCU, [2]OKAN CEM CIRAKOGLU, [3]SERPIL CULA

[1]Dept. of Management Information Systems, Başkent University, Ankara, Turkey
[2]Dept. of Psychology., Başkent University, Ankara, Turkey
[3]Dept. of Insurance and Risk Management, Başkent University, Ankara, Turkey
E-mail: [1]ogutcu@baskent.edu.tr, [2]okanc@baskent.edu.tr, [3]scula@baskent.edu.tr

Abstract— In the study, information security awareness of young persons, named as digital natives, is evaluated within the context of internet addictions and sensation seeking. The sample of the study consisted of 246 students. The most important finding of this study was that internet addiction had significant positive relationships with risky behaviors, exposure to crime and protective behaviors. Risky behavior scores of females and sensation seeking scores of males were significantly higher. Any significant relationship between sensation seeking and information security awareness could not be observed. Results indicated that individuals with higher internet addiction may be under greater risk in terms of information security.

Keywords— Information Security, Awareness, Addictive Internet Use, Sensation Seeking.

I. INTRODUCTION

Today, the activities, which required spatial dependency on paper media in the past, can be carried out in digital media, independent from the space. New communication technologies, social networks and electronical applications have transferred the life of people to the digital medium. Therefore, data, basically, has transformed to an e-asset which must be protected. Both e-transformation process and increased use of social media in our lives have caused such data to circulate uncontrollably in digital media.

The inappropriate utilization of technology as well as low level of awareness of information security threats have caused emergence of irreparable information security risks and cybercrimes; and the individuals had to protect themselves against digital life. Likewise, the nations had to protect their citizens from such threats and their possible consequences before the law, which even led to international cooperation.

Nowadays, with the establishment of e-government systems, such developments also cause a significant threat in terms of national information security. November-December 2004 Turkey Internet Security Research indicated that perceptions related to information security of many institutions and agencies, as well as computer users at all levels, was limited which made them prone to digital risks [1].

Therefore, many software- and hardware-based security methods have been developed in order to maintain information security. At the present time, acquiring data by the use of software and hardware gaps have become difficult to a considerable extent because of the well-developed technological means. Countless threats are intended to be eliminated by implementing technical solutions. However, recently, the abuse of such gaps is replaced with the abuse of information by exploitation of individuals. Social engineering, which is one of the most frequently observed threat, targets on individuals, the weakest link of security. Provision of information security is very difficult and the weakest link of information security in this sense is the uneducated individuals, who are exposed to direct or indirect threats, lacking awareness or having certain psychological tendencies. Basically, security is not a product but a process [2]. Moreover, security is not a problem of technology but a problem of human and management [3].

In case of a minor negligence of an individual, which is the weakest link in information security because of the lack of awareness, significant damages which cannot be assessed at institutional level may come into play. When the literature was reviewed, it was noticeable that the number of studies on factors predicting different aspects of awareness, which is one of the prominent elements of information security, was limited.

When it is taken into account that the younger generation, also known as digital natives, will be the most active users of information world in future, it can be argued that their awareness on information security becomes a crucial point. The literature shows that a considerable number of especially internet addiction studies focuses on the causes and consequences of internet addiction on young people. In the present study, sensation seeking tendency, as well as the addiction to internet and technology, was considered as an important variable which may affect information security awareness of the participants.

When studies on information security are reviewed, lack of models concerning awareness is observed. There are many studies which reveals that information security is not yet at a desired level and basic security risks arise from the individuals rather than systems and technical matters. In many studies, the relationships among several personality traits have been examined but limited number of studies deal with the context of information security. Although many strategy analyses which may increase awareness are made, directive researches to these efforts are lacking. The present study which assumes that internet addiction, as a risk factor, became widespread today, is considered to provide data to information security procedures and will contribute to the development of national and international cyber security.

II. LITERATURE REVIEW

Rapid developments in information and communication technologies have also introduced security threats. Probability of exposure of individuals to threats increase as their utilization of such technologies increase. Material and moral damages on national and international level occur as result of such threats. As the starting point of information security is the individuals, first of all, individual information security should be provided in order to provide national information security.

As Canbek and Sağıroğlu [1] also stated that although many studies on the subject have been conducted, “information and information systems security” is not adequately discussed in terms of individual and psychological variables, and necessary importance is not attached to the matter. In addition, since “security” and “awareness” are of recent terminology, number of relevant academic researches is rather limited and each specific research differ greatly in itself.

According to the results of a survey study conducted by Furnell, Jusoh and Katsabas [4] to determine the end-users’ awareness of threats related to security settings on Microsoft operating system, the threat with highest awareness was viruses and with lowest awareness was phishing attacks. This results become more important when the psychological aspects of the study are also considered. In this study, 80,5% of the participants were between the ages of 17 and 29; and only 30% of them used a password when starting their computers.

In another study by Dijle [5], 72,5% of the participants stated they used unlicensed software; 81,3% of them stated they did not do e-shopping; and 86% of them stated they never encountered any phishing attack. In this study, 51,7% of the participants believed that the software they used could reveal their personal data to third parties; 15,8% of them were believing their security program could protect them; and 28,6% of them had stated they did not have any information on the matter. Finally, 61% of the participants were thinking fraud was the most dangerous cybercrime and 42,2% of them stated they wanted to be a hacker.

In Dijle’s study, acknowledgement of fraud and unlicensed software usage as the most serious cybercrime sets forth the importance of material aspects in individuals’ information security related behavior. When the results of this study are evaluated, it can be concluded that the users’ level of knowledge on the information security is inadequate. It was also interesting to observe the discrepancy between their awareness and behaviors; 75% of the participants used unlicensed software which is a very high rate, even though they thought it as a serious cybercrime. First and foremost, unlicensed software usage is a cybercrime. Unlicensed software cannot be updated and security updates cannot be received. They also create a threat to the computers they are installed in. Despite such a high rate of unlicensed software usage, 51,7% of the participants think that the software they use can reveal their personal data to third parties. Again, another contradiction between awareness and behavior shows itself at this point [6].

Another study conducted by Bensmann [7] examined password selection tendencies of Turkish users. Password is the basic step of identity check in an information system. The most commonly used access control means today is password-user name matchup. Therefore, choice of password is crucial in security. According to the findings of the study, most of the passwords of Turkish users have less than 7 characters, they are all either numerical or alphabetical, ending with numerical characters; or when the passwords have more than 7 characters, their contents have an easily predictable nature containing user information, a very well-known word such as special name etc.

As Hoonakker, Bornoe and Carayon [8] proposed, many researches concerning end-users carry commercial concerns. The number of academic studies in this field is considerably low. Today, information and computer security is at a crucial point in terms of both nations and individuals. However, unfortunately, knowledge and awareness is at a very low level especially in terms of individuals. According to authors, contrary to what is believed, 91% of identity theft, which is an important data abuse, takes place through offline channels. Moreover, only 5% of identity thefts occur by viruses, spywares or hackers and 3% thereof are made through phishing attacks.

A research conducted in 2009 by Zhaung, (cited by Hoonakker et al.) shows that 86% of institutions use user name and password system for identity check. As a reason for this, it is observed that user name and password identification is the most effortless and least costly way of security provision. However, a significant security vulnerability emerges at this point. In the study conducted by Hoonakker, Bornoe and Carayon, it was observed that the users created passwords that were easy to remember and easy to guess. According to the result of another study cited in this study, it was observed that 20% of the people working in an institution wrote down their institution password on a notepad and stick it on the screen of their computers. It was also observed that 66% of the individuals saved their passwords on papers and 58%

thereof do so on electronic papers. The problems caused by unsecured password (composed only of letters) usage has been known for the last twenty years, however, very little could have been done to overcome this. As it can be observed in the aforementioned researches, lack of personal awareness is the major source of security.

In a research in 2006 by Chai and colleagues [9] four different categorizations were made. First, experience of individuals on internet and information security; second, judgment of individuals on their own information security behavior; third, perceived importance of information security behavior; and forth, information security related behavior developed by users to protect themselves. Purpose of the research was to determine if there is significant correlation between these categories. Results revealed that there is a positive significant correlation between the individuals' internet and information security experience and their judgment of their information security behavior. However, no correlation could be found between individuals' internet and information security experience and the information security related behavior they developed to protect themselves.

Another research was carried by Yenisey, Ozok and Salvendy [10] regarding online shopping behavior of Turkish university students. Results of the study indicated that more than 50% of the participants showed the possibility of obtaining of their credit card numbers by third parties as a reason for not doing online shopping. In this study, it was also found that the individuals did not refrain from sharing their age, name, mail address information, whereas they were reluctant to share their social security numbers, telephone and credit card numbers.

It was observed in the study of Şahinaslan and his colleagues [11] that 80% of the officials working in the researched institution cause information abuse without being aware. It is proposed in this study that the most recent threats are information leakage, information theft and intelligence activities.

A brief review of the literature reveals that the studies exploring internet addiction and sensation seeking, which are also considered as variables of the present study, are mostly psychological based and do not relate with information security. In a research conducted by Tsia and his colleagues [12], risk factors for internet addiction were examined. The research was conducted with university students and it was found that gender, neurotic personality traits and lack of socialization created risk factors for internet addiction.

According to the result of a study by Dalbudak and his colleagues [13] a significant positive correlation between sensation seeking and internet addiction was found among university students. In this study, females were found to be under more risk for internet addiction. The finding that sensation seeking and internet addiction are positively correlated was also replicated in a similar study by Rahmani and Lavasani in a university student sample [14]. Several researchers also found gender differences in sensation seeking being males had higher scores [15-17].

Even a brief review of literature on information security reveals that the studies mostly focus on technology and role model development and the industrial fields where researches are conducted are predominantly education, health and financial systems [18].

In many studies it was emphasized that information security awareness is important when developing country strategies; and individuals' awareness education and legislative regulations are also important along with paying attention to technical aspects of the subject [19, 20]. Moreover, the need for more research focusing on the relationship between human behavior and information security is also emphasized in many studies [21, 22].

Although aforementioned studies provide valuable findings on information safety, it can be argued that they do not scrutinize information security as a whole. However, information security should be evaluated as a whole with both awareness and behavior. Provision or evaluation of solely password security or licensed software utilization security is not sufficient. Although awareness is a core element of enabling information security, it is insufficient on its own.

Individuals may be aware of certain security problems, however, this does not necessarily mean that such individuals will engage in protective behaviors. Therefore, in the present study, the relationships among protective behavior development, exposure to crime, risky behavior tendency, sensation seeking and internet addiction were studied. In addition, gender differences among these variables were also tested.

III. MATERIALS AND PROCEDURES

In the present study, primarily individuals' level of awareness on information security is explored in terms of both in perceptual and behavioral aspects. The aim of the study is to identify the direction of the relationship between the individuals' awareness on information security and their behavior on the use of information technologies and to set forth the critical importance of the variables in this relationship. The hypotheses that are considered to serve this purpose are provided below:

-H1: Protective behavior is negatively correlated with sensation seeking

-H2: Protective behavior is positively correlated with internet addiction

-H3: Protective behavior scores of females is higher than males.

-H4: Risky behavior is positively correlated with sensation seeking

-H5: Risky behavior is positively correlated with internet addiction
-H6: Risky behavior scores of females is higher than males
-H7: Exposure to crime is positively correlated with sensation seeking
-H8: Exposure to crime is positively correlated with internet addiction
-H9: Exposure to crime scores of females is higher than males
-H10: Sensation seeking scores of males is higher than females
-H11: Internet addiction scores of males is higher than females.

Several scales were combined to be used in the study. In the Demographic Information Questionnaire (DIQ) questions such as “the purpose of internet use, the frequency of internet use” etc. are asked to the participants together with their ages and sexes.
Secondly, Arnett Inventory of Sensation Seeking (AISS), which is a four point Likert type of scale composed of 20 expressions developed to measure sensation seeking (SS) in individual level, is used [23]. The scale has two sub-scales named as Novelty and Intensity. Arnett expressed that in the development study, Cronbach Alpha for the entire scale was found to be 0,70 (0,50 for intensity and 0,64 for novelty). The scale was adapted to Turkish and used in several studies [24, 25]. In these studies, Cronbach Alphas were found between 0,70 and 0,86. In AISS, increasing scores represent higher level of sensation seeking. In the present study, total scale scores were used.
Thirdly, Internet Addiction Scale (IAS), developed by Young [26], which is a 20 item Likert type scale (between 1 and 6) was used to measure internet addiction (IA). The higher scores show higher level of internet addiction. The Turkish adaptation of the scale was done by Bayraktar and its Cronbach Alpha for the whole scale was found to be 0,91 [27].
Finally, three subscales [namely, protective behavior (PB), risky behavior (RB) and exposure to crime (EC) scales] of Information Security Awareness Scale (ISAS) developed by Öğütçü were used [6]. The scales include five point Likert type statements. Cronbach Alpha value of the questionnaire was found to be 0,93 in the original study.
All data were collected before lectures on information safety on voluntary basis.

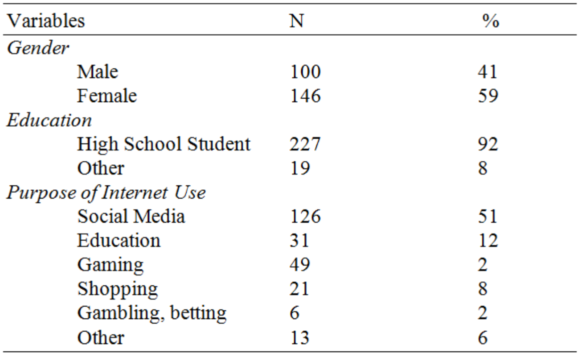
IV. RESULTS AND DISCUSSION

In this section, the study main findings of the study are provided. SPSS17.0 and STATA were used in analyses.

4.1. Demographic Characteristics

The distribution of the demographic characteristics of the participants is presented in Table 1.

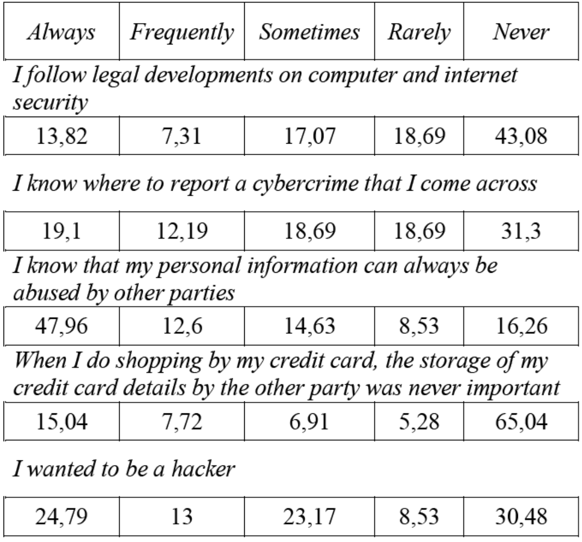
Table 1. General Profile of the Participants



Variables	N	%
Gender		
Male	100	41
Female	146	59
Education		
High School Student	227	92
Other	19	8
Purpose of Internet Use		
Social Media	126	51
Education	31	12
Gaming	49	2
Shopping	21	8
Gambling, betting	6	2
Other	13	6

As summarized in Table 1, 41% of the participants are male and 59% of them are female. The sample mainly consisted of high school students (92%). The participants stated their purpose of internet use. Half of the participants stated their primary purpose for internet use was social media (51%). Other purposes of internet use were education (12%), gaming (20%) shopping (8%) gambling and betting (2%). Six percent of the participants expressed other reasons for internet use. They expressed that they spent an average 4 hours per day and 6 days per week online.

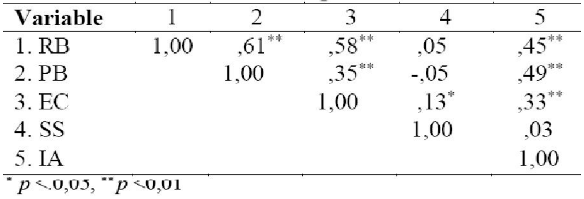
Table 2. The Percentages of Some Responses



Always	*Frequently*	*Sometimes*	*Rarely*	*Never*
I follow legal developments on computer and internet security				
13,82	7,31	17,07	18,69	43,08
I know where to report a cybercrime that I come across				
19,1	12,19	18,69	18,69	31,3
I know that my personal information can always be abused by other parties				
47,96	12,6	14,63	8,53	16,26
When I do shopping by my credit card, the storage of my credit card details by the other party was never important				
15,04	7,72	6,91	5,28	65,04
I wanted to be a hacker				
24,79	13	23,17	8,53	30,48

Some responses of participants which may be crucial for information security were summarized in Table 2. According to these responses, 43,08% of the participants stated that they never followed the legal developments on computer and internet security; they did not know where to report a cybercrime that they come across (31,3%); they always knew that their personal information can always be abused (47,96%); the storage of their credit card details by the other party was never important to them (65,04%) and they never wanted to be a hacker (30,48%).
During the testing of the given hypotheses correlation analyses and independent-group t-tests were performed. The significance level was accepted as 0,05.

Table 3. Correlations among Variables Variable

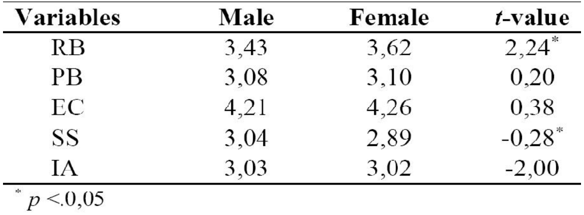


Variable	1	2	3	4	5
1. RB	1,00	,61**	,58**	,05	,45**
2. PB		1,00	,35**	-,05	,49**
3. EC			1,00	,13*	,33**
4. SS				1,00	,03
5. IA					1,00

$^{*}p<0,05$, $^{**}p<0,01$

Correlation analyses (Table 3) indicated that risky behavior was correlated with protective behavior, exposure to crime and internet addiction. Protective behavior was positively correlated with exposure to crime and internet addiction. The correlation of exposure to crime with sensation seeking and internet addiction was also positive. No other significant relationship was obtained.

Table 4. Independent-Groups t-tests



Variables	Male	Female	*t*-value
RB	3,43	3,62	2,24*
PB	3,08	3,10	0,20
EC	4,21	4,26	0,38
SS	3,04	2,89	-0,28*
IA	3,03	3,02	-2,00

$^{*}p<0,05$

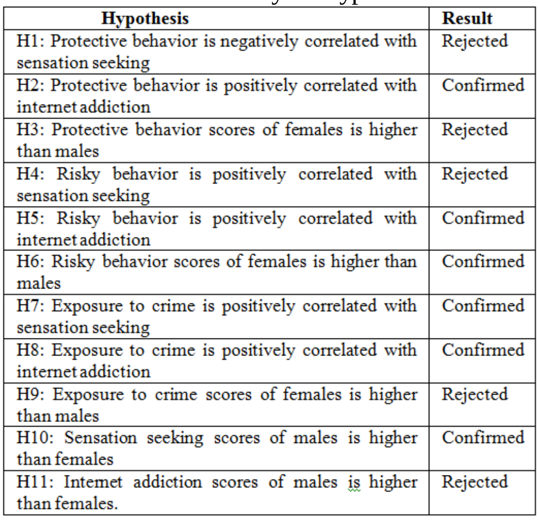
As for the t-test results (Table 4), risky behavior scores of females and sensation seeking scores of males were significantly higher. No other significant mean difference was found between males and females.

In the present study, sensation seeking, internet addiction and gender were evaluated in the context of information security. The analyses revealed that H2, H5, H6, H7, H8, and H10 were confirmed.

As expected, risky behaviors on internet was positively associated with protective behaviors, exposure to crime and internet addiction. Participants who have risky behaviors may be aware of their risks and may develop protective behaviors against them. High correlation values indicated that the relationships among internet addiction, risky behaviors and exposure to crime are very strong. Higher use of internet will place users under increased risk of being exposed to crime. The association of exposure to crime with sensation seeking and internet addiction is also understandable; higher level of sensation seeking may increase the risk of engaging risky behaviors that may be associated with crime such as illegal betting or gambling. Similarly, higher level of addiction may lead to repeated engagement of these behaviors. However, more studies are needed in order to understand the causal links among these variables in a holistic manner. Previous findings regarding males had higher sensation seeking scores [15-17] was also replicated in the present study. This difference has been explained by several researchers in the light of evolutionary changes or culturally transmitted gender norms [28].

The present study has several limitations which make the generalizability of the results difficult. First, the sample of the study is limited to generalize findings. Second, this is a correlational study which aims to explore the relationships among variables. Therefore, it does not allow causal interpretations of the findings. Finally, like all other paper-pencil studies, validity issues should be taken into account while interpreting results.

Table 5. Summary of Hypotheses



Hypothesis	Result
H1: Protective behavior is negatively correlated with sensation seeking	Rejected
H2: Protective behavior is positively correlated with internet addiction	Confirmed
H3: Protective behavior scores of females is higher than males	Rejected
H4: Risky behavior is positively correlated with sensation seeking	Rejected
H5: Risky behavior is positively correlated with internet addiction	Confirmed
H6: Risky behavior scores of females is higher than males	Confirmed
H7: Exposure to crime is positively correlated with sensation seeking	Confirmed
H8: Exposure to crime is positively correlated with internet addiction	Confirmed
H9: Exposure to crime scores of females is higher than males	Rejected
H10: Sensation seeking scores of males is higher than females	Confirmed
H11: Internet addiction scores of males is higher than females.	Rejected

CONCLUSIONS

The most important finding of the present study was that internet addiction was associated with risky behaviors and exposure to crime which may cause a great risk in the context of information security. Although, protective behaviors were also associated with internet addiction, risks should not be underestimated. Accordingly, it can be proposed that it may be difficult to maintain information security among individuals with internet addiction. It may be recommended that this factor must be kept in mind in awareness studies and training programs

REFERENCES

[1] Canbek, G., & Sağıroğlu, Ş. (2006). A review on information, information security and security processes. Journal of Polytechnic, 9, 165-174.

[2] Sağsan, M. (2002). Bilgi teknolojileri güvenliği: Ulusal bilginin korunmasına pragmatik bir yaklaşım ve Türkiye perspektifi. Stratejik Analiz, 2, 74-81

[3] Mitnick K. D. (2009). Aldatma Sanatı. Ankara: ODTÜ Yayıncılık

[4] Furnell, S. M., Jusoh, A., & Katsabas, D. (2005). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25, 27-35.

[5] Dijle, H. (2006). Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımı. Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü.

[6] Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers & Security, 56, 83-93.

[7] Bensmann, L. (2009). Intelligent search strategies on human chosen passwords. Technische Universtat, Fakultat für Informatik, Dortmond.

[8] Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password authentication from a human factors perspective: Results of a survey among end-users. Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting.

[9] Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. (2006). Role of perceived importance of information security: an exploratory study of middle school children's information security behavior. Issues in Informing Science and Information Technology, 3, 127-135..

[10] Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2008). Perceived security determinants in e-commerce among Turkish university students. Proceedings of World Academy of Science, Engineering and Technology, 24, 259-274.

[11] Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. Akademik Bilişim '09 - XI. Akademik Bilişim Konferansı Bildirileri, (597-602). Şanlıurfa.

[12] Tsai, H. F., Cheng, S. H., Yeh, T. L., Shih, C. C., Chen, K. C., Yang, Y. C., & Yang, Y. K. (2009). The risk factors of Internet addiction-A survey of university freshmen. Psychiatry Research, 167, 294-299.

[13] Dalbudak, E., Evren, C., Aldemir, S., Taymur, I., Evren, B., & Topcu, M. (2015). The impact of sensation seeking on the relationship between attention deficit/hyperactivity symptoms and severity of Internet addiction risk. Psychiatry Research, 228, 156–161.

[14] Rahmani, S., & Lavasani, M. G. (2011). The comparison of sensation seeking and five big factors of personality between internet dependents and non-dependents. Procedia - Social and Behavioral Sciences, 15, 1029-1033.

[15] Bitton, M. S., & Medina, H. C. (2015). Problematic internet use and sensation seeking: Differences between teens who live at home and in residential care. Children and Youth Services Review, 58, 35-40.

[16] Bradley, G., & Wildman, K. (2002). Psychosocial predictors of emerging adults' risk and reckless behavior. Journal of Youth and Adolescence, 31, 253-265.

[17] Lynne-Landsman, S. D., Graber, J. A., Nichols, T. R., & Botvin, G. J. (2011). Trajectories of aggression, delinquency, and substance use across middle school among urban, minority adolescents. Aggressive Behavior, 37, 161-176.

[18] Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security-A survey and classification of the research area. Computers & Security, 30, 748-769.

[19] Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30, 803-814.

[20] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

[21] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90-101.

[22] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36, 215-225.

[23] Arnett, J. (1994). Sensation seeking: A new conceptualization and a new scale. Personality and Individual Differences, 16, 289–296.

[24] Sümer, N., & Özkan, T. (2002). The role of driver behavior, skills, and personality traits in traffic accidents. Turkish Journal of Psychology, 17, 1-26.

[25] Sümer, N. (2003). Personality and behavioral predictors of traffic accidents: Testing a contextual mediated model. Accident Analysis and Prevention, 35, 949-964.

[26] Young, K. S. (1996). Internet addiction: The emergence of a new clinical disorder. CyberPsychology and Behavior, 1, 237-244.

[27] Bayraktar, F. (2001). İnternet kullanımının ergen gelişimindeki rolü. Yayımlanmamış Yüksek Lisans Tezi, Ege Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

[28] Cross, C. P., Cyrenne, D. M., & Brown, G. R. (2013). Sex differences in sensation-seeking: A meta-analysis. Scientific Reports, 3, doi:101038/srep02486.

★★★