The Journal of Academic Social Science Studies
Year: 14 - Number: 85 , p. 309-326, Summer 2021

Information Security Awareness Scale (ISAS) for University Students: A Validity and Reliability Study

Asst. Prof. Dr. Can Güldüren
ORCID ID: https://orcid.org/0000-0002-9048-1228
Ufuk University, Vocational School, Department of Computer Technologies, Ankara – TURKEY

Artcile History

Geliş: 10.06.2020
Kabul: 06.04.2021
On-line Yayın: 30.06.2021

Keywords

Awareness
Consciousness-Raising
Information Security
University Students
Scale Development

Research Article

DOI:
http://dx.doi.org/10.29228/JASSS.44135

Abstract

The purpose of this study is to develop a scale for university students to determine information security awareness levels. The categories and the indicators related to information security awareness were determined by the literature review. A question pool of 90-items related to the categories and the indicators was generated. Next, 23 field experts evaluated the draft scale form for the content validity. After that, the 67-point scale, which was redesigned in line with expert assessments, was practiced to the students studying at Ankara University. As a result of exploratory factor analysis, it was determined that the scale consists of 34 items and 4 subscales ('privacy and safe browsing', 'attacks and threats', ‘general security’ and ‘cyberbulling’).A confirmatory factor analysis with the data of the second group of 156 participants was performed at the following stage of the study, and the structure with four factors was confirmed. At the end of the construct validity analysis, the scale consists of four factors and 34 items, and the total variance that it can explain is 50,42%. The Cronbach Alpha internal consistency coefficient and the Spearman-Brown split-half reliability coefficient were calculated to confirm the reliability of the scale. Besides, the significance of the differences between the upper and lower 27 % group item averages was examined using the corrected item-total correlation and t-test. The Cronbach alpha internal consistency coefficient was 0.949 and the Spearman-Brown split half reliability coefficient was 0.861 for the whole scale, while it was calculated as PSB: 0.927/0.833, AT: 0.923/0.871, GS: 0.821/0.801, and CS: 0.898/0.887 for the sub-scales, respectively. All findings show that a high reliability and validity scale that can be used to determine the levels of information security awareness of university students was obtained.

Reference Information / Atıf Bilgisi

Güldüren, C. (2021). Information Security Awareness Scale (ISAS) for University Students: A Validity and Reliability Study. *Jass Studies-The Journal of Academic Social Science Studies*, 14(85): 309-326.

The Journal of Academic Social Science Studies
Yıl: 14 - Sayı: 85 , s. 309-326, Yaz 2021

Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ): Geçerlik ve Güvenirlik Çalışması

Dr. Öğr. Üyesi Can Güldüren
Ufuk Üniversitesi, Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Ankara – TÜRKİYE

Makale Geçmişi

Submitted: 10.06.2020
Accepted: 06.04.2021
Published Online: 30.06.2021

Anahtar Kelimeler

Farkındalık
Bilinçlendirme
Bilgi Güvenliği
Üniversite Öğrencileri
Ölçek Geliştirme

Araştırma Makalesi

DOI:
http://dx.doi.org/10.29228/JASSS.44135

Öz

Bu çalışmanın amacı, bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik üniversite öğrencileri için bir ölçek geliştirmektir. Bilgi güvenliği farkındalığına ilişkin kategori ve göstergeler alanyazın taraması ile tespit edilmiştir. Kategori ve göstergelere ilişkin 90 maddelik soru-havuzu oluşturulmuştur. Daha sonra, taslak ölçek formu, kapsam geçerliği için 23 alan uzmanının görüşüne sunulmuştur. Uzman değerlendirmeleri çerçevesinde yeniden düzenlenen 67 maddelik ölçek, Ankara Üniversitesinde öğrenim gören öğrencilere uygulanmıştır. Açımlayıcı faktör analizi sonucunda, ölçeğin 34 madde ve 4 alt boyuttan ('mahremiyet ve güvenli gezinme', 'saldırı ve tehditler', 'genel güvenlik' ve 'siber güvenlik') oluştuğu belirlenmiştir. Çalışmanın bir sonraki aşamasında, 156 kişiden oluşan ikinci grup verileriyle ile gerçekleştirilen doğrulayıcı faktör analizi sonucunda geliştirilen ölçeğin 4 faktörlü yapısı doğrulanmıştır. Yapı geçerlik analizi sonunda ölçek dört faktör ve 34 maddeden oluşmakta olup açıklayabileceği toplam varyans% 50,42'dir. Ölçeğin bütününe ait Cronbach alfa iç tutarlık katsayısı ve Spearman-Brown iki yarı test güvenirlik katsayısı hesaplanmıştır. Ayrıca düzeltilmiş madde-toplam korelasyonu ve t-testi kullanılarak üst %27 ile alt %27 grupların madde ortalamaları arasındaki farkların anlamlılığı incelenmiştir. Ölçeğin tümüne ait Cronbach alfa iç tutarlılık katsayısı 0.949 ve Spearman-Brown iki yarı test güvenirlik katsayısı 0.861; her alt ölçek için sırasıyla MGG:0.927/0.833, ST:0.923/0.871, GG:0.821/0.801 ile SZ:0.898/0.887 olarak hesaplanmıştır. Tüm bulgular, üniversite öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek güvenirliği ve geçerliği yüksek bir ölçek elde edildiğini göstermektedir.

1. INTRODUCTION

The speed of developments in information and communication technologies has added new dimensions to interaction among people (Berman, 2004; Jeeger, 2018; Runtuwene, Mege, Palilingan, and Batmetan, 2018). Consequently, the acceptability, perception, and effects of new technologies entering human life have also changed depending on the social structure and time. With the widespread use of information and communication technologies and the Internet, the increase in web-based online applications cause security gaps in parallel. Therefore, the duty of ensuring information security has become everyone's responsibility in the society (Tsohou, Kokolakis, Karyda and Kiountouzis, 2008; Acılar, 2009; Vural & Sağıroğlu, 2011; Güldüren, 2015; Wilson, 2016; Güldüren, Çetinkaya & Keser, 2017).

Information Security essentially represents a practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It consists of three primary elements referred to as confidentiality, integrity, and accessibility (Puhakainen, 2006). If any of these three primary elements are damaged, a security weakness occurs. Information is an indispensable and valuable asset for people and organizations. Thus, security is vital to guard information. Moreover, the technologies that are continually developing and used for information processing pose a risk. Information systems are also becoming global today. As a result, all individuals and institutions which have a direct or indirect relationship with information systems should now contribute to information security (Vardal, 2009; Vural & Sağıroğlu, 2011; Wilson, 2016; Jeeger, 2018). It is impossible to eliminate the information security risks caused by human error. However, with a well-planned awareness training, security risks can be maintained at a satisfactory level (Kruger and Kearney, 2006; Vural, 2007; Acılar, 2009; Şahinaslan, Kandemir & Şahinaslan, 2009; Vardal, 2009; Gülmüş, 2010; Runtuwene, Mege, Palilingan, and Batmetan, 2018).

Kruger and Kearney (2006) describe information security awareness as understanding its importance through users, understanding personal responsibilities, and performing actions that are compatible with institution procedures. According to Furnell and Clarke (2012), the technology dimension does not ensure a preserved environment for information security. Therefore, end-users carry out a key role in the concept of information security.

Experts develop technology-based solutions like international standards, intrusion detection/prevention systems, antivirus software and firewalls to ensure information security. But it is still human who uses these technologies. At this point, while experts provide solutions to the problems with a technology-based perspective to ensure information security, they overlook the human factor (Chen, Shaw and Yang, 2006; Rezgui and Marks, 2008; Kjorvik, 2010; Öztemiz and Yilmaz, 2013). As a result of developing technologies, possible security weaknesses are gradually decreasing, and the whole view focuses on human errors. Therefore, the weakest link of the institution and personal information security is the human factor (Kritzinger & Smith, 2008; Veiga, 2008; Mahabi, 2010; Penmetsa, 2010). At this point, it shows the problem of information security cannot be corrected only with technology-based methods by overlooking the human factor. The most efficient solution to prevent possible threats is the awareness of people and the use of security technologies in the right place at the right time (Siponen, 2001; Mathisen, 2004; Puhakainen, 2006; Albrechtsen, 2007; Şahinaslan, Kantürk, Şahinaslan & Borandağ, 2009; Al-Shehri, 2012). It is never possible to eliminate the information security risks related to the human factor. However, with a well-planned awareness activity, security risks can be brought to a satisfactory level (Kruger and Kearney, 2006; Vural, 2007; Şahinaslan, Kandemir & Şahinaslan, 2009; Vardal, 2009; Gülmüş, 2010; Wilson, 2016; ; Jeeger, 2018).

Today, every individual (information owner, information user, or information system administrator) who carries out an active role in information systems is responsible for ensuring information security (Straub and Welke, 1998; Thomson and von Solms, 1998; Siponen, 2000;). In this case, its level depends on the sensitivity that all users show. In other words, user awareness is of critical importance in establishing it (Rotvold, 2008; Furnell and Clarke, 2012).

On the hand, electronic applications produced as a result of developments in information and communication technologies, facilitate the functioning of life, but on the other, they bring new security threats and new crime types (Gülmüş, 2010). The interest in information security in the last 15-20 years has increased tremendously in our country as it has in the world. As a result, research on this subject has increased in our country. The researches on information security deal with the problems frequently from a technological perspective and overlook the human factor (Chen, Shaw and Yang, 2006; Rezgui and Marks, 2008; Kjorvik, 2010). It is impossible to assure the security of the institutional and personal information only with technical security measures (Rezgui and Marks, 2008). Furthermore, institutions and individuals must have information security awareness.

The findings of the literature review also approve higher education institutions are not in a remarkably excellent condition in terms of awareness of information security (Cox, Connolly and Currall, 2001; Rezgui and Marks, 2008; Vardar, 2009; Güldüren, 2015). The researches explain that higher education institutions are one of the risky places in the world in terms of it (Foster, 2004; Rezgui and Marks, 2008; Mahabi, 2010; Tekerek & Tekerek, 2013; Yıldırım & Varol, 2013). The investigations show that there are many insufficiencies and vulnerabilities in the information systems of higher education institutions (Rezgui and Marks, 2008; Mahabi, 2010). Information and informatics systems security studies obtain a necessity for higher education institutions as it does in other organizations. 435 higher education institutions participated in the research conducted by the University of Wisconsin in the USA (Caruso, 2003; Haeussinger and Kranz, 2013). The findings were determined that only one-third of the institutes participating in the survey provided information security awareness training for students and staff.

According to the Higher Education Institution Statistics (YÖK,2020), as of January 2020, about 8 million 76 thousand 615 students are attending school this fall. The YÖK also reports that there are 170 thousand 561 faculty members currently in Turkey. That is over 8.25 million students and faculty members spending their time inside schools, on their Wi-Fi, online programs, and much more. Cyber-criminals have higher education institutions in their crosshairs. According to some reports, higher education accounted for 13 percent of all data breaches in 2019, with only the health and financial sectors targeting higher rates. Higher education institutions confront unique threats in their data security. Hackers directly target universities for the sensitive information stored in their systems. Because the personal data of alumni, staff and faculty, academic studies, and cross-institutional information become the targets of hackers. According to the research findings in our country, it is possible to say that the conditions in our country are not better than the situation presented in this study (Vardar, 2009; Karaoğlan Yılmaz, Yılmaz & Sezer, 2014; Akgün & Topal, 2015; Gökmen & Akgün, 2015). Students studying at universities have to prioritize the issue of information security and educate themselves on this issue. In this context, it is necessary to identify the level of information security awareness of higher education students and the level of their deficiencies. In the literature review on information security awareness, a study detailed by Kruger and Kearney (2006), which developed a methodological approach to estimate information security awareness both abroad and for an international mining company. There were no studies present on information security awareness for higher education students at home. The studies are predominantly focused on those topics of information security management systems, risk evaluation, information security awareness training, and due diligence process regarding information security issues abroad and domestically. The studies are predominantly conducted to determine the general situations. There was no study to determine the level of awareness of information security of the human element, expressed as the 'weakest link' in information security. This research aims to develop a scale that determines the information security awareness level of university students and determining the pre-psychometric properties.

2. METHOD

This section includes explanations for the model, working group, development of scale form, data collection and analysis processes used in the research.

2.1. Research Model

Balcı (2009) describes the research model as the regulation of conditions that ensure economic collection and analysis of data by the research objective, which guarantees to test research hypotheses or answer research questions. For this purpose, a theoretical scale development model proposed by Yurdagül (2005) was used to develop an information security awareness scale for university students. Workgroup features and scale development work phases presented in subheadings.

2.2. Participants

Guilford (1954) and Kline (1994) emphasize that a sample of at least 200 participants is satisfactory to extract reliable factors in scale development studies. Similarly, the sample size can be determined based on the number of items or factors. While Nunnally (1978) and Kline (1994) suggest the sample size as ten times the number of items, Tavşancıl & Keser (2002) suggest it is within five and ten times. As a general rule, at least 300 sample sizes are appropriate for a factor analysis (Tabachnick & Fidell, 2007; Çokluk, Şekercioğlu & Büyüköztürk, 2010). In this study, a particular attention was paid to the number of observations so that they it does not fall below the minimum number of observations to determine the psychometric feature of the scale with the least error.

The literature recommends conducting Exploratory factor analysis (EFA) and Confirmatory factor analysis (CFA) using different samples (Çakmak, Kılıç, Çebi & Kan, 2014; Ilhan & Cetin, 2014). Accordingly, the factor analyses (EFA and CFA) were performed on data from different participant groups. The measuring tool was developed through the data collected from the students studying in separate departments of Ankara University. The fundamental assumptions of multivariate statistics were examined before EFA. As a result of the examination, it determined that a total of 442 forms filled by the students were suitable for statistical analysis. 291 (65.84%) of the students were female, and 151 (34.16%) were male. 162 of the students (36.65%) were 1st grade, 34 (7.69%) were 2nd grade, 43 (9.73%) were 3rd grade and 203 (45.93%) were 4th grade. 93 (21.04%) of the students were from The Computer Education and Instructional Education Program, and 61 (13.80%) of them were from The Guidance and Psychological Counseling Program, 54 (12.22%) of them were from The Early Childhood Education Program, and 52 (11.76%) of them were from The Social Sciences Teacher Education Program, and 51 (11.54%) of them were from The Primary School Teacher Education Program, 131 (29.64%) of them were from other programs (Turkish Teaching, Mathematics Education, Nursing, Applied English and Translation Programme, Public Administration, Business Administration). CFA was carried out in printed form through the data from the other public and foundation university (Gazi, Hacettepe, ODTÜ, Yıldırım Beyazıt, Başkent and TOBB) students in Ankara. The fundamental assumptions of multivariate statistics were examined before CFA. As a result of the examination, it determined that a total of 156 forms filled by the students were proper for statistical analysis.

2.3. Scale

The items in the scale were discovered on a theoretical basis to refer to all possible sub-dimensions of the measured structure (Tezbaşaran, 2008). The literature review was conducted before determining the scale items and developing the trial form. The categories and indicators related to information security awareness were determined by the literature review. A question pool of 90-items related to the categories and indicators was generated. As the response format, the 5-point Likert scale ranging from 'strongly disagree' to 'strongly agree' was used.

The scale validity (construct, and content) was investigated. Lawshe (1975) technique was applied in order to analyze the content validity. A total of 23 field experts (on educational technologies, measurement, and assessment) assessed the 90-items draft scale. The draft scale was evaluated to measure the level of information security awareness, the relationship with the sub-dimension and the clarity of expression. The content validity indexes (CVI) were calculated by summing up the scores provided by the experts for each item. CVI was compared with the content validity criterion (CVC). Veneziano and Hooper (1997) converted CVC into a table. The statistical significance of the CVI was analyzed with the CVC (CVC20=0.42, α<0.05). In line with expert advice, some items were reviewed, and 23 items beneath CVC were removed from the draft scale form. The content validity index of the 67-item scale developed was 0.89. Later a Turkish language expert analyzed the scale for a linguistic evaluation. After the arrangements, a pilot study was conducted with a group of university students to get feedback on the scale items and the time it took to complete the scale. The primary dataset not included data from this group of students (n=25). Next, the 67-item scale was finalized to apply it to the principal participants.

2.4. Data Analysis

The construct validity (factor structure) of the scale was examined by way of exploratory factor analysis (EFA). It was aimed to discover the latent structures measured by the scale items with this analysis (Büyüköztürk, 2011). Confirmatory factor analysis (CFA) was then performed to determine the compliance level of the determined factor structure. The factor analyses (EFA and CFA) were performed after ISAS was applied to the first group of participants.

The reliability of the data obtained using scale was analyzed using Cronbach's alpha and Spearman-Brown Split-half parallel reliability correlations. The top 27 percent and the bottom 27 percent of participants which compared and adjusted item-total correlations were calculated to examine the discriminatory power of the items. SPSS 17.0 and Lisrel 8.57 package programs were used for statistical analysis.

3. FINDINGS

In this part of the study, the findings and comments obtained from the research are discussed under the subheadings. EFA and CFA were applied respectively to test the construct validity. These analysis steps are presented under separate headings.

3.1. Exploratory Factor Analysis

At this stage of the research, EFA was performed with the data obtained from the first group of participants. In the literature, it is recommended to check the data before analysis. The sample size is the most crucial requirement for EFA. In the factor analysis, it is declared as a general rule that at least 300 sample numbers are relevant (Tabachnick & Fidell, 2007; Çokluk vd., 2010). The sample size of the first group of 442 participants for EFA was satisfactory. Kaiser-Mayer-Olkin (KMO) test is performed to test the compatibility of the data structure for factor analysis in terms of sample size. Bartlett's test of sphericity is performed to determine whether the data come from the multivariate normal distribution. If the value for the sample size is less than 0.50, it is interpreted that the test cannot be continued and if it is above 0.90, it is interpreted as 'perfect' Tavşancıl, 2005; Çokluk et al. 2010). EFA was executed with the first group data. Before the analysis, the data compatibility was analyzed with Barlett's test of Sphericity and KMO test (Tabachnick and Fidell, 2007; Çokluk et al. 2010). The KMO test value of the scale was 0.947. This finding can be evaluated as the data structure is perfectly sufficient for a factor analysis. Similarly, as a result of the analysis Bartlett's test of sphericity was significant at the 0.01 level (χ2= 19739.220 df=2211 p=0.000). This finding means that the data came from the multivariate normal distribution and therefore another criterion of factor analysis was met (Tabachnick and Fidell, 2007). Analysis results show that the data is appropriate for EFA. While determining the number of factors according to the Kaiser-Guttman principle, the line graph of the eigenvalues that were greater than one, the factor eigenvalues and the variance rates they explained were examined (Zwick & Velicer, 1986). In EFA, factors with eigenvalues of one and above are considered stable (Büyüköztürk, 2002; Çokluk vd., 2010). To decide on the structure of the factors, the solution proposed should be theoretically-based (Zwick & Velicer, 1986). It is sufficient that the variance explained in single factor patterns is 30 percent or more. In multi-factor scale structures, the variance explained in the social sciences is considered to be sufficient between 40 percent and 60 percent (Tavşancıl, 2005). There are two types of ways to increase the variance described. The first is to increase the number of important factors, and the second is to look for a higher factor load in item selection (Büyüköztürk, 2011). EFA can be conducted using multiple factorization techniques (MFA). The principal component analysis (PCA) is more robust in psychometric terms among MFA. Therefore, the PCA was used for factorization in this study.

With these principles, while starting the EFA analysis, the eigenvalue was accepted as 2 and the factor load value as 0.55. As a result of EFA, the scale was collected under 4 factors (eigenvalue> 2). The variance explained by these factors was 50.42%. During AFA, the items that made up the factors were evaluated in terms of the degree of cross-loading and factor load values. In multi-factor patterns, items with cross-loading and low factor load-values can be combined. Although it is not a definite rule, the item removal process is expected to start with cross-loading items(Çokluk et al. 2010). The cross-loading and low factor load-value items were removed from the scale and EFA was repeated 15 times. The factor load values and common factor variance related to the items which were the result of EFA are presented in Table 1.

When Table 1 is examined, it can be seen that the first sub-factor consists of 15 items. The factor load values of this sub-factor ranges from 0.56 to 0.67. In the same way, common factor variances for these items are between 0.47 and 0.57. The second sub-factor consists of 10 items. The factor load values of this sub-factor ranges from 0.57 to 0.75. In the same way, common factor variances for these items are between 0.43 and 0.67. The third sub-factor consists of 6 items. The factor load values of this sub-factor ranges from 0.55 to 0.76. In the same way, common factor variances for these items are between 0.38 and 0.67. The fourth sub-factor consists of 3 items. The factor load values of this sub-factor ranges from 0.75 to 0.77. In the same way, common factor variances for these items are between 0.68 and 0.80. It can be said that the highest contribution to the total variance was made by the 35th item (factor load = 0.77 and common factor variance = 0.80). It can be stated that the lowest contribution to the total variance was made by the 3rd item (factor load = 0.55 and common factor variance = 0.38).

Table 1. Factor Loadings and Common Factor Variance

F1	Item	FL	CFV	F2	Item	FL	CFV	F3	Item	FL	CFV	F4	Item	FL	CFV
Privacy and Safe Browsing	B52	0,67	0,57	Attacks and Threats	B31	0,75	0,67	General Security	B17	0,76	0,67	Cyber Bullying	B35	0,77	0,80
	B54	0,66	0,57		B26	0,74	0,64		B16	0,70	0,53		B36	0,75	0,74
	B55	0,66	0,50		B32	0,74	0,64		B18	0,68	0,57		B34	0,75	0,68
	B53	0,65	0,51		B30	0,72	0,59		B15	0,67	0,48				
	B50	0,65	0,56		B33	0,70	0,60		B44	0,56	0,48				
	B67	0,64	0,52		B25	0,67	0,61		B03	0,55	0,38				
	B56	0,62	0,50		B29	0,67	0,54								
	B58	0,62	0,57		B28	0,65	0,63								
	B57	0,62	0,50		B22	0,62	0,43								
	B59	0,61	0,54		B27	0,57	0,56								
	B66	0,60	0,49												
	B60	0,59	0,51												
	B49	0,58	0,48												
	B65	0,58	0,51												
	B51	0,56	0,47												
	Eigenvalue:		9,11		Eigenvalue:		8,50		Eigenvalue:		6,46		Eigenvalue:		2,66
		ETV	17,18			ETV	16,03			ETV	12,20			ETV	5,01
* Factor load values less than 0.55 are not shown in the table.													Explained Total Variance:		50,42
FL: Factor Loadings, CFV: Common Factor Variance, ETV: Explained Total Variance															

The total variance that the first sub-factor can explain is at the level of 17.18%. It has been identified as 'privacy and safe navigation' considering the item contents and literature. The total variance that the second sub-factor can explain is at the level of 16.03%. It has been identified as 'attacks and threats' considering the item contents and literature. The total variance that the third sub-factor can explain is at the level of 12.20%. It has been identified as 'general security' considering the item contents and literature. The total variance that the third sub-factor can explain is at the level of 5.01%. It has been identified as 'cyberbullying' considering the item contents and literature.

The total variance explained by the four-factor structure is 50.42%. The variances explained in the social sciences in multi-factor systems are considered to be satisfactory between 40% and 60% (Tavşancıl, 2005). Based on this criterion, the four-factor scale structure achieved was found satisfactory for surveying university students ' information security awareness. The factor loadings remained above 0.55 for all thirty-four items on the scale. In the literature, items with a factor loading of 0.45 and above are considered as items that should be strictly kept on the scale (Kline, 2000: 167-168; Büyüköztürk, 2011: 124). Based on this criterion, it was decided that the scale should include all thirty-four items under four factors.

3.2. Confirmative Factor Analysis

CFA was performed to evaluate the covariance structure analysis of the model discovered by exploratory factor analysis (Kline, 2005). CFA was performed to evaluate the covariance structure analysis of the model discovered by EFA (Kline, 2005). The analysis was conducted through the data from the second group to validate the results of the EFA and to test the theoretical constructed scale model. Chi-square goodness fit and other fit indices were examined to evaluate the model fit. In this study, root mean square error of approximation (RMSEA), goodness of fit index (GFI), adjustment goodness of fit index (AGFI), root mean square residuals (RMR), standardized root mean square residual (SRMR), comparative fit index (CFI), normed fit index (NFI), non-normed fit index (NNFI), incremental fit index (IFI), relative fit index (RFI), parsimony normed fit index (PNFI), parsimony goodness of fit index (PGFI), Akaike information criterian (AIC-Model), consistent Akaike information criterion (CAIC-Model), expected cross-validation index (ECVI-Model), and chi-square goodness of fit test were examined for CFA.

The goodness of fit indices reached without any tests on the model and before the proposed modification suggestions are as follows: [χ2/df=3.190 (p=.00); RMSEA= 0.119; GFI= 0.610; AGFI= 0.560; RMR= 0.150; SRMR= 0.097; CFI= 0.920; NFI= 0.880; NNFI= 0.910; IFI= 0.920; RFI= 0.880; PNFI= 0.082; PGFI= 0.540; AIC Model= 1809.890; CAIC Model= 2109.580; ECVI Model= 11.680]. As a result of the analysis, six modification suggestions among B67-B66, B56-B55, B26-B25, B50-B49, B28-B27, B33-B32 items were taken into consideration. Theoretically, these items measure similar situations. Therefore, modification suggestions were applied sequentially.

After the modification suggestions, the goodness of fit indices for the model was formed as follows: [χ2/df=2.381 (p=.000); RMSEA= 0.094; GFI= 0.680; AGFI= 0.630; RMR= 0.140; SRMR= 0.093; CFI= 0.950; NFI= 0.910; NNFI= 0.940; IFI= 0.950; RFI= 0.900; PNFI= 0.083; PGFI= 0.590; AIC Model= 1386.130; CAIC Model= 1710.12; ECVI Model= 8.94]. Figure 1 presents the structural equation model for the four-factor structure. Table 2 presents the t and R2 (multiple correlation coefficient) values for the scale items. Table 3 presents the measurement model and standardized values obtained as a result of CFA.

Table 2. t and R^2 Values of the Items

F1	Item	t	R^2	F2	Item	t	R^2	F3	Item	t	R^2	F4	Item	t	R^2
Privacy and Safe Browsing	B49	7.98	0.36	Attacks and Threats	B22	6.46	0.25	General Security	B03	7.49	0.33	Cyber Bullying	B34	11.78	0.64
	B50	8.08	0.37		B25	7.68	0.34		B15	8.03	0.37		B35	14.41	0.83
	B51	6.81	0.28		B26	9.75	0.49		B16	11.16	0.60		B36	14.01	0.81
	B52	8.20	0.38		B27	8.18	0.38		B17	13.86	0.80				
	B53	9.97	0.51		B28	8.99	0.44		B18	13.22	0.75				
	B54	10.18	0.52		B29	10.30	0.53		B44	8.55	0.41				
	B55	9.09	0.44		B30	12.68	0.71								
	B56	9.68	0.49		B31	12.32	0.68								
	B57	10.20	0.53		B32	11.50	0.62								
	B58	9.05	0.44		B33	10.87	0.58								
	B59	9.75	0.49												
	B60	9.22	0.45												
	B65	9.52	0.47												
	B66	9.38	0.46												
	B67	8.51	0.40												

$p<0.01$ (all t values are above 2.56)

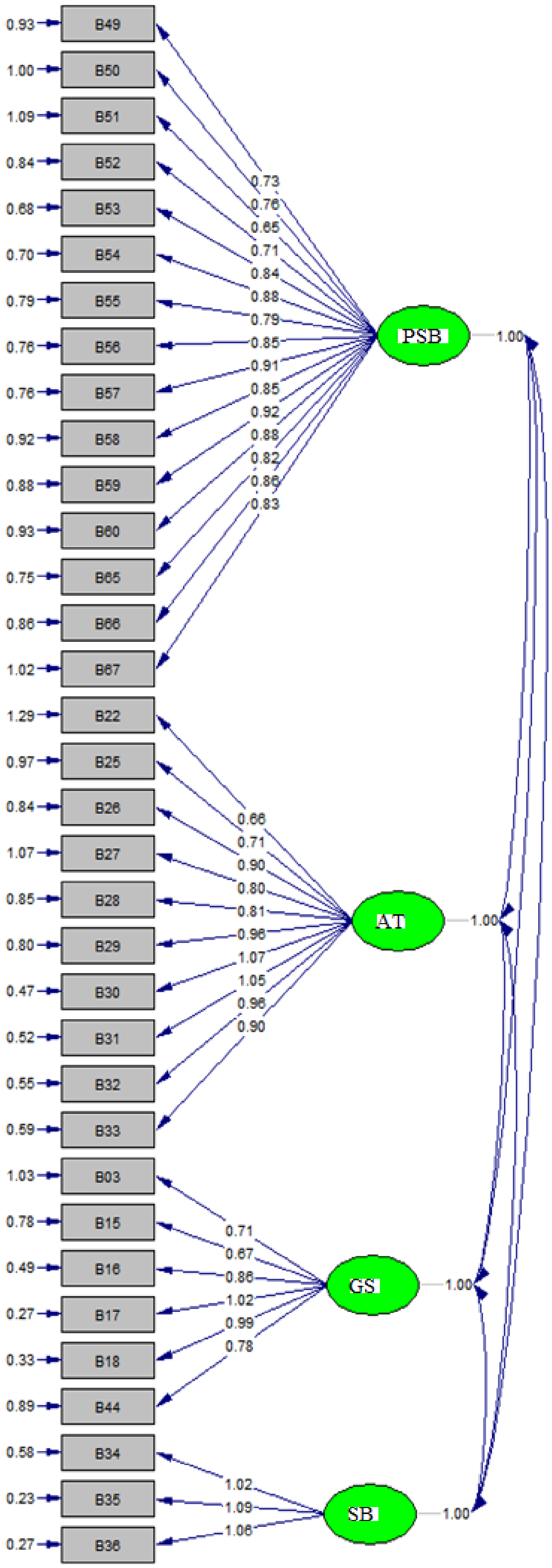

Figure 1. Model and Standardized Values Obtained as a Result of CFA.

The fit indexes presented in Table 3 were analyzed by considering the cut-offs that indicated a good fit and acceptable fit of the model. The findings show that Chi-Square goodness of fit has a value of 2.381 (below 2.5 for small samples, perfect fit, Kline, 2005; Çokluk vd., 2010). It is observed that the calculated RMSEA value is 0.094 (acceptable fit, Jöreskog & Sörbom, 1993; Brown, 2006). It can be declared that the model provides a weak fit for GFI value 0.680 and AGFI value 0.630 (GFI, AGFI > .90 perfect fit, GFI> .85 and AGFI>.80 acceptable fit; Jöreskog & Sörbom, 1993). Likewise, the model's RMR value indicates a weak fit for 0.140, while the SRMR value is 0.093. A value less than 0.010 indicates an acceptable fit (Byrne, 1994; Brown, 2006). When the literature is examined, it is emphasized that these index values are affected by the sample size (Şimşek, 2007:48). In this context, the goodness of fit indices adjusted for sample size effects were examined (CF, NFI, NNFI, IFI, RFI and PNFI). CFI and IFI values are greater than 0.95 (CFI, IFI>= 0.95 perfect fit; Sümer, 2000; Thompson, 2004). NFI and RFI values are greater than 0.90 (NFI, RFI>= 0.90 perfect fit; Sümer, 2000; Thompson, 2004). NNFI and PNFI values indicate acceptable fit (NFI< 0.95 and PNFI >= 0.80 acceptable fit; Sümer, 2000; Thomson, 2004). Similarly, Akaike information criterion (AIC), consistent Akaike information criterion (CAIC), and expected cross-validation indices (ECVI) confirm the model fit. As a result of confirmatory factor analysis, AIC value (1386.13 <13006.77), CAIC value (1710.12 <13144.47) and ECVI value (8.94 <83.91) were calculated respectively (Erkorkmaz, Etikan, Demir, Özdamar & Sanisoğlu, 2013).

Table 3. Examined Fit Indexes and Calculated Values

Fit Indexes	NV	AV	CV	Results
X^2 - Chi-Square	p > 0.05		1226,12	
df - Degrees of Freedom			515	
X^2/df - Chi-Square Goodness of Fit	≤ 2.50	3 ≤ X^2/df ≤ 5	2,381	PF
RMSEA - Root Mean Square Error of Approximation	≤ 0.05	0.05≤ RMSEA≤.010	0,094	AF
GFI - Goodness of Fit Index	>=0.90	0.85 ≤ GFI ≤ 0.90	0,680	WF
AGFI - Adjusted Goodness of Fit Index	>= 0.95	0.85 ≤ AGFI ≤ 0.95	0,630	WF
RMR - Root Mean Square Residuals	≤ 0.05	0.05≤ RMR ≤.010	0,140	WF
SRMR - Standardized Root Mean Square Residuals	≤ 0.08	0.08≤ SRMR ≤.010	0,093	AF
CFI - Comparative Fit Index	>= 0.95	0.95 ≤ CFI ≤ 1.00	0,950	PF
NFI - Normed Fit Index	>=0.90	0.85 ≤ NFI ≤ 0.90	0,910	PF
NNFI - Non-normed Fit Index	>= 0.95	.90 ≤ NFI ≤ .95	0,940	AF
IFI - Incremental Fit Index	>= 0.95	0.90 ≤ NNFI ≤ 0.95	0,950	PF
RFI - Relative Fit Index	>=0.90	0.85 ≤ RFI ≤ 0.90	0,900	PF
PNFI - Parsimony Normed Fit Index	>=0.90	0.80 ≤ RFI ≤ 0.90	0,830	AF
PGFI - Parsimony Goodness of Fit Index	>=0.90	0.80 ≤ RFI ≤ 0.90	0,590	WF
AIC-Model - Akaike Information Criterion	AIC Model < Independence AIC		1386.13 < 13006.77	A
CAIC-Model - Consistent Akaike Information Criterion	CAIC Model < Independence CAIC		1710.12 < 13144.47	A
ECVI-Model - Expected Cross-Validation Index	ECVI < Independence ECVI		8.94<83.91	A

NV: Normal Value, AV: Acceptable Value, HD: Calculated Value

PF: Perfect Fit, AF: Acceptable Fit, WF: Weak Fit, A: Acceptance

The parameter values for the observed values are significant at the level of 0.05 if t values exceed 1.96, and at the level of 0.01 if they exceed 2.56 (Çokluk vd., 2010:304). When the t values presented in Table 2 are analyzed, it is calculated that all the values vary between 6.46 and 14.41 and are significant at the level of 0.01 significance.

Another important criterion is the R2 value, which expresses the variance explained for each observed variable, and reveals how much of the change in the latent variable can be explained (Şimşek, 2007:86). When the t and R2 values of the model are examined, the highest contribution to the assessment of the level of information security awareness is 35 (R2 = 0.83), 36 (R2 = 0.81), 17 (R2 = 0.80), 18 (R2 = 0.75) and 30 (R2 = 0.75). It was observed that 22 (R2 = 0.25), 51 (R2 = 0.28), 03 (R2 = 0.33), 25 (R2 = 0.34) and 49. (R2 = 0.36) items provided the lowest contribution, respectively. These findings confirm the findings obtained in EFA.

3.3. Reliability and Item Analysis

It is critical each item in the scale measures the desired feature and the level of competence in distinguishing individuals. For this purpose, the first corrected item-total correlation values were calculated. Secondly, independent samples t-test was applied for the upper 27 percent and lower 27 percent groups according to the total score. In addition, Cronbach alpha internal consistency coefficient was calculated to determine the reliability of the scale. The analysis results are presented in Table 4.

According to the findings; the corrected item-total correlation values for the 'Privacy and Safe Navigation' factor are ranged from r = 0.50 to r = 0.69. The corrected item-total correlation values for the 'Attacks and Threats' factor are ranged from r = 0.55 to r = 0.77. The corrected item-total correlation values for the 'General Security' factor are ranged from r = 0.42 to r = 0.77. The corrected item-total correlation values for the 'Cyber Bullying' factor are ranged from r = 0.74 to r = 0.86. As a proof of scale item reliability, the corrected item-total correlation value is suggested as 0.30 and above (Nunnally & Bernstein, 1994). When Table 2 is examined, it realizes that the corrected item-total correlation values are higher than 0.30. These findings prove the reliability of the scale items. Besides, it is observed that the t-test values for item average scores of the lower 27 percent and upper 27 percent groups ranged between 5.49-20.49 and all of them are significant (p <.001). The average scores of all the items in the upper 27 percent group are significantly higher than the average scores of the lower 27 percent group. According to these findings, the items in the scale measure similar behavior and distinguish the participants with different awareness levels significantly. The analysis results show that article 28 has the highest discrimination, while article 15 has the lowest discrimination.

The Cronbach Alpha internal consistency coefficient was calculated to confirm the reliability of the scale. In general, the reliability coefficient of 0.70 or higher is recognized as sufficient (Nunnally, 1978). The Cronbach alpha internal consistency coefficient was 0.949 for the whole scale, while it was calculated as PSB: 0.927, AT: 0.923, GS: 0.821, and CS: 0.898 for the sub-scales, respectively. Spearman-Brown split-half reliability coefficient was 0.861 for the whole scale, while it was calculated as PSB: 0.833, AT: 0.871, GS: 0.801, and CS: 0.887 for the sub-scales, respectively. All findings prove that the scale provides satisfactory reliability. Besides, the height of the adjusted item-total correlation values also proves the strength of the internal consistency of the scale.

Table 4. Item Analysis Results

Sub-Factor	Item	Lower %27 X	Upper %27 X	t L/U %27 (2, 3)	CTIC (1)	p
Privacy and Safe Browsing	B49	2,35	4,20	14,69	0,62	< 0.000
	B50	2,40	4,23	15,61	0,68	<0.000
	B51	3,21	4,46	9,18	0,50	<0.000
	B52	2,38	4,19	14,62	0,69	<0.000
	B53	2,21	4,03	14,16	0,67	<0.000
	B54	2,47	4,38	16,68	0,69	<0.000
	B55	2,35	4,23	15,25	0,67	<0.000
	B56	2,33	4,23	15,14	0,68	<0.000
	B57	2,39	4,28	15,68	0,67	<0.000
	B58	1,96	4,06	19,48	0,69	<0.000
	B59	2,08	4,08	17,00	0,63	<0.000
	B60	2,03	4,06	17,99	0,63	<0.000
	B65	2,11	4,11	15,66	0,62	<0.000
	B66	2,14	4,18	15,76	0,63	<0.000
	B67	2,11	4,17	16,59	0,66	<0.000
Attacks and Threats	B22	1,87	3,48	10,97	0,55	<0.000
	B25	1,76	3,92	18,42	0,70	<0.000
	B26	1,66	3,71	16,89	0,75	<0.000
	B27	1,94	4,14	19,60	0,70	<0.000
	B28	1,87	4,09	20,49	0,77	<0.000
	B29	2,03	3,93	15,09	0,71	<0.000
	B30	1,68	3,45	13,36	0,72	<0.000
	B31	1,66	3,59	15,40	0,76	<0.000
	B32	1,60	3,35	13,44	0,73	<0.000
	B33	1,66	3,32	12,12	0,68	<0.000
General Security	B03	3,39	4,33	6,86	0,42	<0.000
	B15	3,68	4,37	5,49	0,52	<0.000
	B16	3,01	4,24	10,23	0,66	<0.000
	B17	2,87	4,36	13,79	0,77	<0.000
	B18	2,81	4,29	14,56	0,65	<0.000
	B44	2,95	4,39	11,70	0,53	<0.000
Cyber Bullying	B34	2,61	4,17	10,93	0,74	<0.000
	B35	2,17	4,17	14,39	0,86	<0.000
	B36	2,18	3,95	12,49	0,80	<0.000
Scale and sub-factors	Cronbach's Alpha	Split-half parallel reliability				

Information Security Awareness Scale (ISAS)	,949	0,861
Privacy and Safe Browsing (PSB)	,927	0,833
Attacks and Threats (AT)	,923	0,871
General Security (GS)	,821	0,801
Cyber Bullying (SB)	,898	0,887

CITC: Corrected item-total correlation

4. DISCUSSION AND CONCLUSION

The finding obtained from the literature review is that studies on information security are predominantly directed towards information security and information security management systems. These studies focus on raising the information security awareness of human, which is the weakest link. The sources reviewed provide various recommendations and measures to be taken for information security awareness. Within the scope of the reached resources, only one study was found to measure the awareness abroad. Within the scope of the reached studies for the country; studies on faculty members, teachers and secondary school students were found. Within the scope of this research, primarily information security awareness categories and indicators were identified from the literature. Based on the pool of items created, a new scale was developed to determine the level of information security awareness of university students.

At the end of the construct validity analysis, the scale consists of four factors and 34 items, and the total variance that it can explain is 50,42%. This total variance value is recognized as sufficient for a multi-factor scale structure. The total variance explained by the first factor called 'privacy and safe browsing' is 17.18 percent. The total variance explained by the second factor named as 'attacks and threats' is 16.03 percent. The total variance explained by the third factor called 'general security' is 12.20 percent. The total variance explained by the fourth factor called 'cyberbullying' is 5.01 percent. In the item analysis, a strong relationship is determined between the adjusted item-total correlation scores.

The Cronbach Alpha internal consistency coefficient and the Spearman-Brown split-half reliability coefficient were calculated to confirm the reliability of the scale. The Cronbach alpha internal consistency coefficient is 0.949 and the Spearman-Brown split half reliability coefficient is 0.861 for the entire scale. The values for each sub-factor are presented respectively: PSBand: 0.927 / 0.833, AT: 0.923 / 0.871, GS: 0.821 / 0.801, and CS: 0.898 / 0.887. The item analysis was conducted to examine the power of predicting the total score and the power of discrimination of scale items. The scale should be considered reliable considering the adjusted item-total correlation values and internal consistency coefficients (5.49<=t<=20.49, p <.001).

The goodness of fit indexes and standard values revealed by the confirmatory factor analysis indicate the fitness of the multi-factor structure reported by exploratory factor analysis. Especially considering the X2/df, CFI, NFI, IFI, RFI, AIC Model, CAIC Model, and ECVI Model values, it shows that the structure has a perfect fit. Given the RMSEA, SRMR, NNFI and PNFI values, it reveals that the structure has an acceptable fit. Given the GFI, AGFI, RMR, and PGFI values, it reveals that the structure has a weak fit. When the literature is examined, it is emphasized that these index values are affected by the sample size. At this point, it can be declared that it is due to the number of DFA samples used in the research as a limitation. Therefore, it is concluded that the indexes that show a value below the acceptable limit in the confirmatory factor analysis may be affected by the limitation of the research group.

Another limitation of the research is students who are reluctant to participate in such studies. Not to devote enough time to the research subject and the intensive curriculum of the students is considered as the reason for this situation. It is thought that this reluctance may also be effective in some changes in the statistical parameters obtained as a result of the analyses. Besides, the size of the study group can be considered as a limitation that may affect the values obtained by a factor analysis. It is thought that it will be useful to review the factor structure of the scale on larger participant groups in the future.

This study shows that the psychometric properties of the scale are valid and reliable. Typically, students between the ages of 18 and 24 are high-risk and attractive targets for security attacks. It is important to increase the awareness of university students about information security awareness to avoid the risk of losses, misuses of personal data, identity falsification, information leakage, etc. The awareness levels of university students can be determined with this scale in order to design the studies for awareness education..

5. REFERENCES

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, I(1), 25-33.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer and Security,* 26(4), 276-289.

Al-Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences,* 6(1), 61-69.

Akgün, Ö. E., and Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya üniversitesi eğitim fakültesi örneği. *Sakarya University Journal of Education,* 5(2), 98-121.

Balcı, A. (2009). *Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler.* (7.b.). Ankara: Pegem Akademi.

Berman, M. (2004). *Katı olan her şey buharlaşıyor* (Çev. Ümit Altuğ, Bülent Peker). İstanbul: İletişim Yayınları.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research*. New York: Guilford.

Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı.

Kuram ve Uygulamada Eğitim Yönetimi. Cilt 32, 470-483.

Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabı* (13. b.). Ankara: Pegem Akademi.

Byrne, B. M. (1994). Structural equation modeling with EQS and EQS/Windows: Basic concepts, applications, and programming. Thousand Oaks, CA: Sage.

Caruso, J. B. (2003). *Information technology security: Governance, strategy, and practice in higher education.* Wisconsin, Madison: EDUCAUSE Center For Applied Research ECAR.

Chen, C. C., Shaw, R., and Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning and Performance Journal*, 24(1), 1-14.

Cox, A., Connolly, S., and Currall, J. (2001). Raising information security awareness in the academic setting, *VINE.* Vol.31 Iss:2, pp.11-16, Glasgow, United Kingdom. doi:10.1108/03055720010803961.

Çakmak, E. Kılıç, Çebi, A. and Kan, A. (2014). E-öğrenme ortamlarına yönelik 'sosyal bulunuşluk ölçeği' geliştirme çalışması. *Kuram ve Uygulamada Eğitim Bilimleri*, 14(2), 755-768.

Çokluk, Ö., Şekercioğlu, G. and Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik spss ve lisrel uygulamaları*. Ankara: Pegem Akademi.

Erkorkmaz, Ü., Etikan, İ., Demir, O., Özdamar, K. and Sanisoğlu, S. Y. (2013). Doğrulayıcı faktör analizi ve uyum indeksleri. *Türkiye Klinikleri*, 33(1), 210-223.

Foster, A. L. (2004). Insecure and unaware. *Chronicle of Higher Education*, 50(35), 33-35.

Furnell, S. and Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers and Security,* 31(8).

Guilford, J. P. (1954). *Fundamental statistics in psychology and education*. New York, NY: McGraw-Hill.

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi*. Yayımlanmamış doktora tezi, Ankara Üniversitesi, Ankara.

Güldüren, C., Çetinkaya, L. and Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online,* 15(2), 682-695.

Gökmen, Ö. F., and Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. *İlköğretim Online,* 14(4).

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği.* Yayımlanmamış yüksek lisans tezi, Yıldız Teknik Üniversitesi, İstanbul.

Haeussinger, F., and Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. *Thirty Fourth International Conference on Information Systems,* Milan 2013.

Ilhan, M., and Cetin, B. (2014). Development of classroom assessment environment scale: Validity and reliability study. *Education and Science,* 39(176), 31–50. https://doi.org/10.15390/EB.2014.3334

Jeeger, L. (2018). Information security awareness: Literature review and integrative framework. *Proceedings of the 51 st Hawaii International Conference on System Sciences.* p.4703-4712.

Jöreskog, K. G., and Sörbom, D. (1993). LISREL 8: Structural equation modeling with the SIMPLIS command language. Chicago: SSI Scientific Software International Inc.

Karaoğlan Yılmaz, G., Yılmaz, R., and Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199.

Kjorvik, H. (2010). *Implementing and improving awareness in information security.* Unpublished master's thesis, University of Agder, Grimstad.

Kline, P. (1994). *An easy guide to factor analysis.* New York, NY: Routledge.

Kline, P. (2000). *The hand book of psychological testing (2nd Ed.).*London: Taylor and Francis Group.

Kline, P. (2005). *Principles and practice of structural equation modelling: a researcher's guide.* London: Sage.

Kritzinger, E. and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computer and Security,* 27, 224-231.

Kruger, H. A. and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer Security*, 25(4).

Lawshe, C. H. (1975). Aquantitative approach to content validity. *Personnel Psychology*, 28, 563–575.

Mahabi, V. (2010). *Information security awareness: System administrators and end-user perspectives at florida state university.* Unpublished doctoral dissertation, The Florida State University, Florida.

Mathisen, J. (2004). *Measuring information security awareness - A survey showing the Norwegian way to do it.* Unpublished master's thesis, Gjovik University, Hogskolen.

Nunually, J. C. (1978). *Psychometric theory (2nd ed.).* New York, NY: McGraw-Hill.

Nunnally, J. C., and Bernstein, I. (1994). *Psychometric theory.* New York: McGraw-Hill.

Özcan, B. (2009). *Kurumsal bilgi güvenliği ve COBIT.* Yayımlanmamış yüksek lisans tezi, Haliç Üniversitesi, İstanbul.

Öztemiz and Yılmaz (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası,* 14(1), 87-100.

Penmetsa, M. K. (2010). *A methodology for measuring information security maturity in norwegian and indian MSME's with special focus on people factor.* Unpublished master's thesis, Gjovik University, Hogskolen.

Puhakainen, P. (2006). *A Design theory for information security awareness.* Unpublished master's thesis, Acta University of Oulu, Oulu.

Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computer and Security,* 27, 241-253.

Rotvold, G. (2008). How to create a security culture in your organization? *The Information Management Journal*, 42(6), 32-38.

Runtuwene, J. P., Mege, R. A., Palilingan, V. R., and Batmetan, J. R. (2018). Information security awareness on data privacy in higher education, *Advances in Social Science, Education and Humanities Research.* V172, p.172.174.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security,* 8(1), 31-41.

Siponen, M. T. (2001, June). Five Dimensions of Information Security Awareness. *Computer and Society,* s. 24-29.

Sümer, N. (2000). Yapısal eşitlik modelleri: Temel kavramlar ve örnek uygulamalar. *Türk Psikoloji Yazıları*, 3(6), 49-74.

Straub, D. W., and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly,* 22(4), 441-469.

Şahinaslan, E., Kandemir, R. and Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *Akademik Bilişim 09 - XI. Akademik Bilişim Konferansı Bildirileri,* (s. 189- 194). Urfa.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. and Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim 09 - XI. Akademik Bilişim Konferansı Bildirileri,* (s. 597-602). Şanlıurfa.

Şimşek, Ö. F. (2007). *Yapısal eşitlik modellemesine giriş: Temel ilkeler ve LISREL uygulamaları*. Ankara: Ekinox.

Tabachnick, B. G. and Fidell, S. L. (2007). *Using multivariate statistics (5th ed.)*. Boston, MA: Pearson/Allyn and Bacon.

Tavşancıl, E. and Keser, H. (2002). Development of a likert type attitude scale towards internet usage. *Educational Science and Practice,* 1(1), 79-100.

Tavşancıl, E. (2005). *Tutumların ölçülmesi ve SPSS ile veri analizi*. Ankara: Nobel.

Tekerek, M., and Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education,* 2(3).

Tezbaşaran, A. (2008). *Likert tipi ölçek geliştirme kılavuzu*. Ankara: Türk Psikologlar Derneği.

Thomson, M. E., and von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management and Computer Security*, 6(4), 167-173.

Thompson, B. (2004). Exploratory and confirmatory factor analysis: Understanding concepts and applications. Washington, DC: American Psychological Association.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008). *İnvestigating information security awareness: research and practice gaps*. Information Security Journal: A Global Perspective, 207-227.

Vardar, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması.* Yayımlanmaış doktora tezi, Gazi Üniversitesi, Ankara.

Veiga, A. d. (2008). *Cultivating and assessing information security culture.* Unpublished doctoral dissertation, University of Pretoria, Pretoria.

Veneziano L. and Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21(1), 67-70.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri.* Yayımlanmamış yüksek lisans tezi. Gazi Üniversitesi, Ankara

Vural, Y. and Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Gazi Üniversitesi Mimarlık Mühendislik Fakültesi Dergisi*. 26(1), 89-103.

Yıldırım, N., and Varol, A. (2013). Sosyal ağlarda güvenlik: Bitlis eren ve fırat üniversitelerinde gerçekleştirilen bir alan çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi,* 6(1).

Wilson, S. R. (2016). *Information security awareness in higher education: A qualitativecase study investigation.* Unpublished doctoral dissertation, Capella university, Minneapolis, Minnesota.

YÖK. (2020). *Yükseköğretim bilgi yönetim sistemi istatistikleri.* 01 Mayıs 2020 tarihinde https://istatistik.yok.gov.tr/ adresinden erişildi.

Yurdagül, H. (2005). Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması. *XVI. Ulusal Eğitim Bilimleri Kongresi* içerisinde (s.1-6). Pamukkale Üniversitesi Eğitim Fakültesi. Denizli.

Zwick, W. R. and Velicer, W. F. (1986). Comprasion of five rules for determining the number of components to retain. *Psychological Bulletin*, 99(3),432-442.