



Pre-Service Teachers' Information Security Awareness: An Analysis Based on the Knowledge—Attitude—Behavior Model

Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları: KAB Modeline Dayalı bir Analiz

Ali İhsan BENZER¹
Yasemin KARAL²

¹Hatay Mustafa Kemal Üniversitesi,
İktisadi ve İdari Bilimler Fakültesi,
Yönetim Bilişim Sistemleri Bölümü,
Hatay, Türkiye

²Trabzon Üniversitesi, Fatih Eğitim
Fakültesi, Bilgisayar ve Öğretim
Teknolojileri Eğitimi Bölümü,
Trabzon, Türkiye

ABSTRACT

Information technologies have become an integral element of everyday life. Even slight vulnerability in the safe use of information technologies may expose individuals, institutions, and even communities to difficult situations. Therefore, the issue of safe Internet use, also referred to as information security, is considered important and it is thought that efforts should be initiated to raise awareness among all members of the society starting from the first stage of the basic education. In this context, for enlightenment of students about information security, teachers assume an important role. Therefore, the levels of information security awareness of pre-service teachers, who will be the teachers of the future, are important. This study has two main aims. These are (A) to develop a valid and reliable scale for information security awareness based on knowledge—attitude—behavior model and (B) examine the information security awareness of pre-service teachers in terms of various variables. The study was carried out with 350 pre-service teachers majoring in a variety of disciplines. As a result, a scale consisting of 71 items with 4 factors was obtained. It was found that there were positive correlations between the components of knowledge, attitude, and behavior that constitute the knowledge—attitude—behavior model adopted in the development of the scale. It was noted that the awareness levels of both female and male pre-service teachers were medium. It was revealed that male's awareness scores were significantly higher than females. Additionally, it was found that the awareness of pre-service IT teachers was higher than others.

Keywords: Information security awareness, cyber security, pre-service teacher, knowledge—attitude—behavior model, individual differences

ÖZ

Bilgi teknolojileri günlük hayatın ayrılmaz bir parçası haline gelmiştir. Bilgi teknolojilerinin güvenli kullanımında en ufak bir zafiyet dahi bireyleri, kurumları ve hatta toplulukları zor durumlara maruz bırakabilmektedir. Bu nedenle bilgi güvenliğinin önemli bir basamağı olan güvenli internet kullanımına önem verilmeli ve temel eğitimin ilk aşamasından başlayarak toplumun tüm bireylerinin bilinçlendirilmesine yönelik çalışmalar yürütülmelidir. Bu bağlamda öğrencilerin bilgi güvenliği konusunda aydınlatılmasında öğretmenlere önemli görevler düşmektedir. Bu nedenle geleceğin öğretmenleri olacak öğretmen adaylarının bilgi güvenliği farkındalık düzeyleri önemlidir. Bu çalışmanın iki temel amacı vardır: Bunlar: (A) Bilgi-Tutum-Davranış (KAB) modeline dayalı bilgi güvenliği farkındalığı için geçerli ve güvenilir bir ölçek geliştirmek ve (B) elde edilen veriler üzerinden öğretmen adaylarının bilgi güvenliği farkındalıklarını çeşitli boyutlarda incelemektir. Araştırma, çeşitli disiplinlerde eğitim gören 350 öğretmen adayı ile gerçekleştirilmiştir. Sonuç olarak dört faktörlü 71 maddeden oluşan bir ölçek elde edilmiştir. Ölçeğin geliştirilmesinde benimsenen KAB modelini oluşturan bilgi, tutum ve davranış bileşenleri arasında pozitif yönde ilişkiler olduğu tespit edilmiştir. Hem erkek hem de kadın öğretmen adaylarının farkındalık düzeylerinin orta düzeyde olduğu görülmüştür. Erkeklerin farkındalık puanlarının kadınlardan anlamlı düzeyde yüksek olduğu ortaya çıkmıştır. Ayrıca bilişim teknolojileri öğretmen adaylarının bilgi güvenliği farkındalık düzeylerinin diğer branşlarda öğrenim gören öğretmen adaylarına göre daha yüksek olduğu tespit edilmiştir.

Anahtar Kelimeler: Bilgi güvenliği farkındalığı, bireysel farklılıklar, KAB modeli, öğretmen adayı, siber güvenlik

Bu çalışmanın bir bölümü, 02-05 Mayıs 2018 tarihleri arasında Antalya Akdeniz Üniversitesi'nde düzenlenen Vth International Eurasian Educational Research Congress (EJER) kongresinde özet bildiriler olarak sunulmuştur.

Received/Geliş Tarihi: 09.12.2021

Accepted/Kabul Tarihi: 03.07.2022

Publication Date/Yayın Tarihi: 09.06.2023

Corresponding Author/Sorumlu Yazar:
Ali İhsan Benzer
E-mail: alibenzer@mku.edu.tr

Cite this article as: Benzer, İ. A. & Karal, Y. (2023). Pre-service teachers' information security awareness: an analysis based on the knowledge—attitude—behavior model. *Educational Academic Research*, (49), 10-22.



Content of this journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Introduction

Digital literacy, regarded as one of the crucial skills in the 21st century, refers to individuals' technical, cognitive, and socio-logical abilities to solve problems they might encounter during performance of their duties in digital settings and their ability to use these abilities. Digital literacy can be described as the skill to survive in the digital age (Eshet-Alkalai, 2004). Today, information security is considered as a sub-dimension of digital literacy (Burkell et al., 2015; Ferrari, 2012; Sonck et al., 2011).

The place of information and communication technologies in our daily life is getting more and more stable. Research in this area reveals that the use of the Internet and digital technologies is increasing for the user population of all ages by years (Pearson, 2015; Turkish Statistical Institute [TurkStat], 2021). Using information and communication technologies brings innovations and conveniences to social, cultural, and academic life; on the other hand, these changes sometimes expose users to a series of problems. These problems might be listed as:

- Password violations
- Malware
- Phishing attacks
- Ransomware
- Privacy violations

Password violations can be denoted as the chief security issue (Mamonov & Benbunan-Fich, 2018). Using the same password for multiple accounts (Jenkins et al., 2014), choosing weak passwords (Spafford, 1992), and sharing passwords with others (Cain et al., 2018) can cause security risks.

According to the Internet Security Report by Symantec, attacks on smart devices that can be connected to the Internet, which is also known as the Internet of Things, increased by 600% in 2017 compared to the previous year. Another growing menace is malicious software that uses computer resources to mine cryptocurrency without the user's authorization. Such malware consumes the computing power of the computer and produces cryptocurrency, which particularly affects corporate computer systems and networks adversely (Symantec, 2018).

The next major security threat is ransomware, which is usually transmitted from an unknown source by opening an e-mail attachment, which transmits to the computer system and demands a ransom from the user for encrypting the digital data. According to the FBI, ransomware overall caused damage of 24 million dollars in 2015, and this loss reached 209 million dollars in the first quarter of 2016 only (Metzger, 2017).

As reported by Kaspersky Lab (2015), cybercriminals have stolen 1 billion dollars from financial institutions worldwide in 2 years. When bank employees click on fake phishing e-mail attachments sent by cybercriminals, malicious software is installed on the user's computer and the computer is controlled by cybercriminals. Bank personnel continue performing usual banking transactions without even being aware of the infected computer. In the meanwhile, cyber criminals interfere with transactions and steal the remittances. Another important problem is the increasing threats to mobile devices as a result of the common use of mobile devices such that the number of malicious software for mobile devices increased by 54% in 2017 compared to the previous year (Symantec, 2018).

More than 95% of security violations are caused by human error (IBM, 2015). Therefore, it can be safely argued that the human factor plays a major role in ensuring information security (Colwill, 2009; Metalidou et al., 2014). An inadequate level of awareness regarding how to provide information security in digital environments is viewed as one of the most important reasons for unwanted incidences (Aslay, 2017; Aydaner et al., 2017). As end users, individuals are defined as persons who use computer applications for their everyday needs (Smith 2012) and are regarded as the weakest link in the security chain (Aloul, 2012; Whitman & Mattord, 2012). Current research reveals a lower level of information security awareness (ISA) among end users (Akgün & Topal, 2015; Gökmen & Akgün, 2015a, 2015b; Gökmen & Akgün, 2016; Tekerek & Tekerek, 2013). Defects in ISA of users may cause security breaches. Due to such breaches, institutions suffer from significant financial and reputation losses (IBM, 2015; Ki-Aries & Faily, 2017).

It is seen that measures against security threats can be two types as investment in information security technologies and raising the consciousness of the public. While information security was heavily regarded as a technical matter focused on technology in the previous years, it is now seen as a human-oriented matter (Eminağaoğlu et al., 2009). Because information security is not merely a technical issue and it is unlikely to overcome this problem by investing in technology only (Glaspie & Karwowski, 2017). Thus, one of the most effective precautions against information security issues seems to be running training and activities to raise awareness of the public concerning information security (Albrechtsen & Hovden, 2010; Domínguez et al., 2010; Eminağaoğlu et al., 2009). Nowadays, institutions are conducting in-house information security programs and training and trying to build a positive information security culture inside in order to raise their employees' ISA to avoid losses due to security breaches (Glaspie & Karwowski, 2017).

According to the international standard ISO/IEC (2005), information security is defined as protection of the integrity, confidentiality, and availability of information, while Whitman and Mattord (2012) describe information security as protection of information and systems that use, store, and transfer information. The ISA is defined as each employee's level or degree of appreciating the importance of information security (attitude), understanding the information security levels in their institution of affiliation and their own individual security responsibilities (knowledge) and acting accordingly (behavior) by the Information Security Forum (ISF, 2002).

The rapid development of technology and increased amount of time spent on the Internet (Cavus & Ercag, 2016; Tekerek & Tekerek, 2013) made it compulsory to conduct activities serving to exploration and development of individuals' ISA. Research on teachers and pre-service teachers is considered particularly important because, as in many other subjects, it is important and necessary that teachers should be a role model for students about information security and safe Internet use (Çakır et al., 2015b; Cavus & Ercag, 2016; Gökmen & Akgün, 2016; ISTE, 2008).

The survey of literature shows that ISA is regarded as a significant issue for teachers. In parallel with this baseline, it seems at least as important to determine the ISA levels of pre-service teachers since they are future teachers. However, the review of literature ended up with only a few studies on pre-service teachers'

awareness of information security (e.g., Akgün & Topal, 2015; Çakır et al., 2015a, 2015b; Gökmen & Akgün, 2015a, 2015b; Gökmen & Akgün, 2016). Agamba and Keengwe (2012) studied the pre-service teachers' attitudes and perceptions about information security. Pusey and Sadera (2011) examined pre-service teachers' awareness of information security in the context of knowledge. Akgün and Topal (2015) investigated ISA of senior students of education faculties in the context of behavior and knowledge. Çakır et al. (2015a, 2015b) examined pre-service teachers' ISA within the scope of social network usage behaviors. Gökmen and Akgün (2015a, 2015b) conducted studies on the last graders in the computer and instructional technologies department to find out their ISA in the context of knowledge of information security. As a result of the literature review on ISA for pre-service teachers, it was seen that studies examine ISA in the context of either only one or two of the components of knowledge, attitude, or behavior.

Many scales are available in the literature which measure ISA. One of the most remarkable scales was developed by Kruger and Kearney (2006) in order to examine ISA among employees working in an international mining company. The authors benefited from the factors that constitute information security and the theories in social psychology for preparing their scale. According to Kruger and Kearney (2006), ISA consists of three components as

- i. Knowledge: What does the individual know about the subject?
- ii. Attitude: What does the individual think about the subject?
- iii. Behavior: What does the individual do?

Kruger and Kearney's (2006) model takes theories of social psychology as basis, and relies on emotional, behavioral, and cognitive building blocks of a positive or negative reaction to any object. Kruger and Kearney (2006) later elaborated their model in the framework of three components as knowledge, attitude, and behavior. Regarding the components that make up the model, McCormac et al. (2017) stated that all of the components of knowledge, attitude, and behavior are interrelated. If individuals' knowledge about information security increases, their attitudes toward information security will eventually improve and thus they will be able to act in increased compliance with the information security rules. This model is also known as KAB, which stands for knowledge–attitude–behavior, or KAP, which stands for knowledge—attitude—practice, has been used to investigate levels of awareness in many studies covering various areas so far (e.g., Lin et al., 2007; McCormac et al., 2017; Parsons et al., 2014; Tolvanen et al., 2012; Xu et al., 2010).

Nevertheless, the current literature provides no single study which discusses awareness of pre-service teachers in relation to the components of knowledge, attitude, and behavior. The aim of this study was two-fold: to develop a valid and reliable scale for ISA based on KAB model and to examine the ISA of pre-service teachers through the data obtained.

Method

Participants

The participants of the research were 350 pre-service teachers. The distribution of this sample group by major and gender is shown in Tables 1 and 2.

As stated in Table 1, the largest groups of participants were Classroom Teaching and the Computer Education and Instructional Technology majors. Others refer to participants studying Physics,

Journalism, Statistics, Chemistry, Mathematics, Art, and Basic Education, or attending pedagogical formation training.

As can be seen in Table 2, in the study, 68.6% of the participants were females and 31.1% were males.

Data Collection Tool and Data Collection Procedure

In this research, a scale was developed by the researchers for evaluating the pre-service teachers' ISA. The scale is based on the KAB model and Kruger and Kearney's (2006) methodology. The process of scale development took place as follows:

Drafting scale items: The literature on the ISA was examined. Focus areas were determined for the draft scale through the literature review. The focus areas determined are Internet use, e-mail use, social media use, password use, wireless network use, personal device care and security, and incident reporting. After that, items were written under components of knowledge, attitude, and behavior of each focus area. At first, the draft scale included 57 items about behavior, 57 about attitude, and 31 about knowledge. Based on a determined focus area, sample items under the three components are presented in Table 3.

- *Taking expert opinions:* Changes were made to the pool of draft items by following the advice of two faculty members. This second draft included a total of 107 items consisting of 40 items on behavior, 40 on attitudes, and 27 on knowledge information a second draft.

Table 1.
Sample Group by Major

Major	f	%
Classroom Teaching	63	18.0
Computer Education and Instructional Technology	60	17.1
Special Education	41	11.7
Sciences Teaching	32	9.1
English Language Teaching	31	8.9
Elementary Mathematics Education	28	8.0
Physical Education	20	5.7
Turkish Language Teaching	19	5.4
Pre-School Education	14	4.0
Psychological Counseling and Guidance	14	4.0
Social Studies Teaching	7	2.0
Music Teaching	5	1.4
Other	12	3.4
Not specified	4	1.1
Total	350	100

Table 2.
Sample Group by Gender

Gender	f	%
Male	109	31.1
Female	240	68.6
Not specified	1	.3
Total	350	100

Table 3.
Example Items in Components of Knowledge—Attitude—Behavior Model for the Focus Area of Personal Device Care and Safety

Component	Personal Device Care and Safety
Knowledge	I know how to install an anti-virus program on the computer.
Attitude	I think using anti-virus software is important for information security.
Behavior	I use an anti-virus program.

- *Pilot study:* In order to check comprehensibility and response time of the scale items, the draft was applied to 10 students in their second year in Computer Technologies Department at a state university's vocational school. The scale was prepared as a form and given to students. In the pilot study, the response time was noted as 15–20 minutes. After filling of the scale, the students were asked whether there are any unclear items. But no unclear items were detected. Thus, the pilot study was completed with no changes to the scale.
- *Performing the main study:* Reliability and validity of the scale were checked by applying the form to 350 pre-service teachers. The data of the research were collected in the 2017–2018 academic year.

Data Analysis

The purpose of this research is two-fold: to put forward a valid and reliable measure of ISA for pre-service teachers and to perform statistical analyses on the data obtained during the scale development procedure. The scale consists of items in different types of Likert. The items regarding knowledge component are 3-point Likert type with responses as “yes,” “partially yes,” and “no” to determine the rating of the level between 3 and 1. As for the component of attitude, the items are 5-point Likert type as “strongly agree,” “agree,” “undecided,” “disagree,” and “strongly disagree” rated between 5 and 1. Lastly, behavior is measured with 5-point Likert-type items with “always,” “very frequently,” “occasionally,” “quite rarely,” and “never” scored from 5 to 1. Validity and reliability of the scale were checked by means of exploratory factor analysis (EFA), item analysis, and confirmatory factor analysis (CFA). The Pearson correlation analysis, *t*-test and ANOVA were used to examine the ISA of pre-service teachers, another purpose of the research.

Ethics

Since the data in this research were collected before 2020 the Ethics Committee Approval. Certificate was not obtained.

Results

Results on Reliability and Validity of the Scale

Before EFA, the collected data were checked for suitability for EFA, by applying Kaiser–Meyer–Olkin (KMO) and Bartlett Sphericity tests. As a rule, a KMO value of smaller than .50 requires discontinuation of EFA. The values between .80 and .90 refer to “good” compliance. Values greater than .90 refer to “excellent” level of suitability for analysis (Çokluk et al., 2016). The KMO test coefficient was found as .889, which means a significant Bartlett Sphericity test.

In order to determine the factor structure, principal component analysis was carried out along with Varimax rotation technique, and the results were examined. In the EFA, the following criteria were taken into consideration during the selection of the items:

- Field (2009) proposes examining the correlation matrix before starting EFA. This matrix shows the correlation values among the scale items. In this matrix, each item must show correlation of .3 or above with at least several items. Field (2009) states that items that do not correlate with a sufficient number of items at .3 or above must be omitted. As a result of the correlation matrix, five of the items were found not to have correlation with a sufficient number of items at the value of .3 or above and thus were excluded from factor analysis.
- The factor load value of items can be set to a value between .30 and .59 (Büyüköztürk, 2002). In this study, the lowest factor load value was set as .30 (threshold value) and those below the threshold were omitted.
- If there is a difference of smaller than .10 between the two highest values of the items (cross-loaded items) that give meaningful loads to more than one factor, those items were eliminated (Büyüköztürk, 2017).
- An item-total correlation equal to or above .30 means that the distinctive feature of the item is good (Büyüköztürk, 2017). Therefore, those items with item-total correlations less than .30 were deleted.

As a result of the EFA, a four-factor scale was obtained which explained 40% of the total variance of 71 items as shown in Table 4. While declared variance equal to or higher than 30% can be regarded sufficient for single-factor designs, this value is expected to be higher in multi-factor designs (Büyüköztürk, 2017).

In the scale, factor 1 was titled “attitude toward information security,” factor 2 as “knowledge about information security,” factor 3 as “behavior of information security,” and the last as “attitude toward personal device security.” As a result of the EFA, the items under the components of knowledge and attitude were gathered around the factor under their respective headings, whereas the items under behavior component were divided into two different factors.

After the EFA, the reliability coefficients of the entire scale and each scale factor were calculated separately and the results were presented in Table 4. The reliability coefficient of the entire 71 items was calculated as .95. As for the attitudes toward information security, the reliability coefficient was found to be .86. The dimensions regarding knowledge and behavior yielded reliability at the level of .91 and .84, respectively. Lastly, reliability coefficient was calculated as .79 for behaviors regarding personal device security.

Table 4.
Factors, Declared Variance Percentages, and Reliability Coefficients

Name of Factor	Declared Variance %	Number of Items	Reliability Coefficient
Attitude toward information security	24.32	34	.86
Knowledge about security information	8.87	19	.91
Behavior of information security	4.18	15	.84
Behavior of personal device security	2.99	3	.79
Total	40.37	71	.95

Such values equal to or greater than .70 are considered satisfactory for the reliability of the test scores (Büyükoztürk, 2017).

In another method for item analysis, the differences between item scores of 27% upper and lower groups based on the total test scores are calculated by applying independent *t*-tests. The analysis results of *t*-test are presented in Table 5.

As seen in Table 5, item score averages for all items in the upper 27% proved significantly higher than those of the 27% lower group. The *t*-test values were between 4.54 and 13.11 all being significant ($p < .001$). In this case, the items in the scale measure the ISA of pre-service teachers and participants can be significantly differentiated at different levels of awareness.

For assessing the model resulting from EFA, CFA was performed with the AMOS software. Kline (2005) proposes to report at least chi-square, Standardized Root Mean Square Residual (SRMR), Root Mean Square Error of Approximation (RMSEA), and Comparative Fit Index (CFI) fit indices for CFA. In this study, chi-square (χ^2/df), SRMR, RMSEA, and CFI fit indices were taken into account for model fit. The analysis, taking into account the recommended modification indices, yielded the following results: [chi-square (χ^2/df)=1.91, SRMR=.058, RMSEA=.051, CFI=.798]. The chi-square (χ^2/df) is seen to be 1.91. According to Schermelleh-Engel et al. (2003) that type of value less than or equal to 2 implies that the model has a good fit. The SRMR value is .058 and the RMSEA value is .051. According to Schermelleh-Engel et al. (2003), these values indicate an acceptable fit. The CFI value is seen to be .798. According to Raykov and Marcoulides (2006), the CFI value must be greater than .90 for a good fit. The fact that the CFI value is close to 0.90 indicates that the model fits relatively well. The CFI value is close to 0.90, indicating a relatively good fit.

Results Obtained From the Scale

As earlier mentioned, another aim of this study is to perform statistical analysis for the following purposes on the scale data obtained as a result of the scale development work.

- Studying the relationship among the scale components of knowledge, attitude, and behavior.
- Calculating and evaluating the scale scores.
- Examination of ISA scores according to major and gender.

Results on Relationships Among Knowledge—Attitude—Behavior Components

Pearson correlation analysis was conducted to examine the relationships between the components of knowledge, attitude, and behavior that constitute the KAB model adopted in the development of the ISA scale. The findings are presented in Table 6.

As seen in Table 5, there is a moderate, positive relationship between knowledge and attitude ($r = .327$; $p < .001$), knowledge and behavior ($r = .517$; $p < .001$), and attitude and behavior ($r = .571$; $p < .001$). It can be inferred that the components in the scale are positively related and affect each other.

Results on Calculation and Evaluation of the Scale Score

In the calculation of the overall score of ISA, the components of knowledge, attitude, and behavior account for 30%, 20%, and 50%, respectively (Kruger & Kearney, 2006). In this scoring method, the highest contribution is extended by the component of behavior. Table 7 shows the ratio of contribution by each of the knowledge, attitude, and behavior components to the overall evaluation.

In this study, the level thresholds and nomenclature specified by Kruger and Kearney (2006) were used for appointing the levels of overall ISA obtained from the calculation in Table 6. The levels and ranges of overall ISA are given in Table 8.

For completing the calculations given in Tables 7 and 8, the average scores obtained from each of the four factors in the information security scale were converted to centesimal points.

Results on the Relationship Between Information Security Awareness and Gender

The *t*-test was performed to find out if there is a significant difference between gender and each of the four factors and also the overall score scale. The results are shown in Table 9.

In view of the overall scores obtained by males and females, it is seen that the former group has a higher level of ISA ($M = 75.20$) than the latter ($M = 71.29$) as in Table 8. When the entire scale is evaluated, a significant difference can be seen between two genders in favor of the males [$t(347) = 2.892$, $p < .01$]. One-by-one examination of the factors under the scale reveals a significant difference in Knowledge of Information Security between the two genders in favor of the males [$t(347) = 8.252$, $p < .01$], Attitude toward Information Security in favor of the females [$t(347) = -2.402$, $p < .05$], and behavior of personal device security attributing the superiority to the males back [$t(347) = 2.068$, $p < .05$]. As one exception, no gender difference is seen at a significant level under the factor Behavior of Information Security [$t(347) = .827$, $p > .05$]. On the whole, the overall awareness levels of both male and female pre-service teachers correspond to the “medium” level.

Results on the Relationship Between Information Security Awareness and Major

Table 10 displays the average overall scores of the respondents regarding ISA by their field of study.

As seen in Table 9, the mean of the scores obtained from the entire scale of ISA is $M = 72.54$. This figure implies that the pre-service teachers in the current study have a “medium” level of ISA. The highest average score ($M = 81.11$) was recorded by Computer Education and Instructional Technology (CEIT), which is at a “good” level of awareness. As a result of the scale development works, the overall scale scores were analyzed by using ANOVA to find out whether there are any differences between fields of study. Also, Scheffe test, a type of post hoc, was performed to spot the ends of such differences, if any. Levene test proved that the condition of homogeneity of variance was met ($LF = 0.775$; $p > .05$). Scheffe test is more sensitive to errors of type 1 and is preferred in cases of unequal number of participants in groups. The results of ANOVA test are shown in Table 11.

As shown in Table 11, the mean scores about overall ISA differ greatly against majors in the ANOVA test [$F(13.336) = 4.911$; $p < .01$]. According to the Scheffe test, there is a significant difference between the overall awareness scores of CEIT and Elementary Mathematics Education and also between CEIT and Classroom Teaching.

Discussion

According to the literature, while research on ISA was started at an international scale during the first quarter of the 2000s, it has been introduced in Turkey only recently.

Table 5.
Item and Factor Analysis

Item No*	Factor Common Variance	Item-Total Correlations**	t (Lower%27-Upper%27)***	Factor1	Factor2	Factor 3	Factor 4
A1	0.494	0.53	8.545****	.591			
A2	0.477	0.56	11.031****	.626			
A4	0.498	0.52	9.989****	.625			
A5	0.318	0.50	11.617****	.506			
A7	0.399	0.54	9.612****	.574			
A8	0.37	0.54	11.358****	.537			
A9	0.414	0.55	11.462****	.502			
A12	0.339	0.49	9.284****	.511			
A13	0.433	0.54	8.753****	.618			
A14	0.245	0.43	7.167****	.454			
A15	0.398	0.53	10.265****	.607			
A17	0.504	0.60	13.108****	.591			
A18	0.437	0.59	12.424****	.574			
A19	0.528	0.61	12.03****	.702			
A20	0.402	0.51	8.789****	.587			
A21	0.277	0.43	8.888****	.433			
A22	0.378	0.54	9.878****	.573			
A23	0.358	0.54	11.055****	.544			
A24	0.478	0.62	12.873****	.645			
A25	0.427	0.58	10.796****	.605			
A26	0.443	0.54	10.704****	.541			
A27	0.36	0.46	10.535****	.457			
A28	0.521	0.56	10.27****	.681			
A30	0.362	0.45	7.703****	.590			
A31	0.432	0.59	11.532****	.604			
A32	0.47	0.50	7.914****	.680			
A33	0.373	0.48	10.161****	.592			
A34	0.488	0.56	11.756****	.659			
A35	0.411	0.46	9.596****	.635			
A36	0.406	0.50	8.593****	.628			
A37	0.374	0.48	9.035****	.521			
A38	0.405	0.51	9.655****	.567			
A39	0.437	0.53	9.51****	.636			
A40	0.505	0.58	10.223****	.686			
K1	0.586	0.42	6.984****		.581		
K2	0.549	0.38	7.021****		.620		
K3	0.503	0.43	7.622****		.564		
K4	0.325	0.31	6.043****		.525		
K5	0.359	0.35	6.352****		.566		
K8	0.396	0.37	6.027****		.569		
K9	0.5	0.39	7.235****		.689		
K10	0.417	0.31	6.664****		.535		
K11	0.448	0.38	7.988****		.615		
K12	0.403	0.41	7.156****		.603		
K13	0.503	0.37	6.447****		.701		
K15	0.371	0.44	8.098****		.552		

(Continued)

Table 5.
Item and Factor Analysis (Continued)

Item No*	Factor Common Variance	Item-Total Correlations**	t (Lower%27-Upper%27)***	Factor1	Factor2	Factor 3	Factor 4
K16	0.336	0.39	7.049****		.538		
K17	0.381	0.34	5.752****		.608		
K19	0.469	0.45	8.12****		.597		
K23	0.457	0.37	6.582****		.636		
K25	0.343	0.30	4.541****		.580		
K26	0.401	0.33	6.266****		.599		
K27	0.377	0.35	6.28****		.549		
B8	0.28	0.37	7.051****			.459	
B15	0.3	0.49	10.643****			.419	
B17	0.395	0.41	8.415****			.611	
B18	0.327	0.41	7.941****			.537	
B21	0.293	0.38	7.214****			.491	
B22	0.332	0.52	11.045****			.377	
B26	0.321	0.35	7.244****			.533	
B27	0.369	0.36	8.01****			.596	
B31	0.496	0.54	12.307****			.505	
B33	0.279	0.44	8.662****			.429	
B34	0.338	0.34	7.937****			.549	
B35	0.358	0.51	10.218****			.430	
B37	0.255	0.38	7.394****			.434	
B39	0.27	0.47	9.658****			.377	
B40	0.288	0.41	8.592****			.474	
B1	0.5	0.47	10.33****				.557
B2	0.519	0.49	10.313****				.570
B3	0.457	0.45	9.42****				.535

Note: *A = attitude; B = behavior; K = knowledge.
n = 350, *n1 = n2 = 95, ****p < .001.

Table 6.
Relationships among Knowledge, Attitude, and Behavior Components

Component	n	r	p
Knowledge—attitude	350	0.327*	.000
Knowledge—behavior		0.517*	.000
Attitude—behavior		0.571*	.000

The present study serves to put forth a valid and reliable scale to examine the three aspects of ISA, which are knowledge, attitude, and behavior, on pre-service teachers. Within the scope of the validity check, EFA yielded a four-factor scale which explained

Table 7.
Relative Contribution of Knowledge, Attitude, and Behavior to Overall ISA

Component of Awareness	Contribution (%)
Knowledge	30
Attitude	20
Behavior	50

Note: ISA = Information Security Awareness.

Table 8.
Levels and Ranges of Overall Information Security Awareness

Level of Overall ISA	Range (Percentage)
Good	80–100
Medium	60–79
Poor	59 and below

Note: ISA = Information Security Awareness.

40% of the total variance of 71 items. Factor 1 was titled “attitude toward information security,” factor 2 was titled as “knowledge of information security,” factor 3 as “behavior of information security,” and the last one as “behavior of personal device security.” After the EFA of the scale, the reliability coefficients were calculated for the entire scale and individual factors of the scale. The reliability coefficient of the entire scale was found as .95. The reliability coefficients of the factors were .86, .91, .84, and .79, respectively. Considering the reliability coefficients, the scale was considered to be reliable. Then CFA was performed to verify the structure obtained from the EFA. Chi-square (χ^2/df), SRMR, RMSEA, and CFI fit indices were taken into account for model fit. Considering the model fit index values, it can be stated that the model has a good fit.

Table 9.
T-test on the Relationship Between Information Security Awareness and Gender

Factor	Gender*	n	M	sd	df	t	p
Knowledge of information security	M	109	86.95	10.97	347	8.252	.000
	F	240	75.04	15.35			
Attitude toward information security	M	109	78.49	13.06	347	-2.402	.017
	F	240	81.94	12.11			
Behavior of information security	M	109	66.81	14.55	347	.827	.409
	F	240	65.42	14.57			
Behavior of personal device security	M	109	66.97	22.71	347	2.068	.039
	F	240	61.64	22.16			
Entire scale	M	109	75.20	11.16	347	2.892	.004
	F	240	71.29	11.95			

Note: *M = male; F = female.

Table 10.
Average Scores for the Entire Scale Against Major

Major	M
A Classroom Teaching	71.03
B Computer Education and Instructional Technology	81.11
C Special Education	70.57
D Sciences Teaching	72.28
E English Language Teaching	72.14
F Elementary Mathematics Education	64.36
G Physical Education	71.77
H Turkish Language Teaching	72.11
I Pre-School Education	68.08
J Psychological Counseling and Guidance	67.34
K Social Studies Teaching	78.62
L Music Teaching	74.90
M Other	71.35
N Not specified	69.24
Total	72.54

Table 11.
Results of ANOVA on Distribution of Scale Scores Against Major

Source of Variance	SS	df	MS	F	p	Significant Difference
Between groups	7792.12	13	599.39	4.911	.000	B - F, B - A
Within groups	41012.09	336	122.06			
Total	48804.21	349				

The current study varies substantially from studies in the literature since it targets pre-service teachers attending a variety of fields and examines the phenomenon of awareness by relying on KAB model. So far, the literature has provided no single study that addresses both of these major goals in one place. However, the present study stands out as an exception in this direction. Also, our scale on ISA provides the most items without compromising validity or reliability, in the context of Turkey. This situation is expected to let surveyors collect and analyze data more deeply.

In general, the measurement instruments based on the KAB model discuss if components of the model correlate in some way. For example, Parsons et al. (2014) developed a scale to measure the ISA of employees which is based on the KAB model. The results from the scale were processed with correlation analysis, which revealed a significant relationship between the components of knowledge, attitude, and behavior. As another example, McCormac et al. (2017) conducted a research to investigate the relationship between ISA and individual differences such as gender, age, character, and risk-taking tendency. The study targeted employees and the participants' ISA was searched by using the scale based on the KAB model. As a result of the correlation analysis of the data obtained, there was a significant relationship between the components of knowledge, attitude, and behavior. Also, Ngoqo and Flowerday (2015) examined university students' ISA with particular relation to mobile devices by means of the method mentioned by Kruger and Kearney (2006). Correlation analysis was performed on the data, which also yielded a meaningful relationship between knowledge, attitude, and behavior. Another study was carried out by Wahyudiwan et al. (2017), which explores employees' ISA by using the scale relying on the KAB model. They reported a significant relationship between knowledge, attitude, and behavior components of ISA. Likewise, in our study, a significant positive relationship was noted between knowledge, attitude, and behavior as the main components of the model which is the foundation of our scale. This result seems to actualize McCormac et al.'s (2017) proposition that increased levels of individuals' knowledge about information security will improve attitudes toward information security and eventually they will act more appropriately to codes of information security. This finding is in compliance with findings of McCormac et al. (2017), Ngoqo and Flowerday (2015), Parsons et al. (2014), and Wahyudiwan et al. (2017).

In the literature, it is a subject of debate whether ISA varies depending on gender. Some of the studies (Akgün & Topal, 2015; Çakır et al., 2015a, 2015b; McCormac et al., 2017; Tekerek & Tekerek, 2013) reported higher awareness among females, while some others (Güldüren et al., 2016; Yılmaz et al., 2016) found the opposite. Unlike the foregoing, Öğütçü et al. (2016) found out that although the genders do not differ in protective behaviors, females have higher scores in relation to risky behaviors. Gökmen and Akgün (2015a) reached the conclusion that male pre-service teachers hold higher levels of knowledge than their female peers

when informatics security is in question. However, Karacı et al. (2017) revealed that there is no significant difference between two genders concerning information security behaviors. Back to our study, male participants recorded higher average scores than females in two particular sub-scales as “knowledge of information security” and “behavior of personal device security.” Conversely, females got higher average scores from the dimension “attitude toward information security” at a significant level. In relation to “knowledge of information security,” our results seem in conformity with Gökmen and Akgün (2015a). The other factor, “behavior of information security,” displayed no gender differences in our study. The finding shows harmony with the findings of Karacı et al. (2017). Strangely enough, the male participants in our study did not attain as high scores as expected in the behavior dimension although they reported higher levels of knowledge about the subject. It may be because male participants have a tendency to take more risks as Akgün and Topal (2015) stated that male pre-service teachers tend to take more risks when behaviors are concerned with information security. In this study, we spotted a significant difference in favor of males in view of the average scores obtained from the entire scale. Thus, it can be suggested that ISA levels of males are higher in comparison to females. This result representing the entire scale seems to be in consistency with the findings of Güldüren et al. (2016) and Yılmaz et al. (2016); at the same time, it contradicts McCormac et al. (2017), Akgün and Topal (2015), Tekerek and Tekerek (2013), Çakır et al. (2015a) and Çakır et al. (2015b). The divergence between the results regarding gender could be due to the fact that the data collection instruments about ISA include a differing number, quality, and weight of items measuring knowledge, attitude, and behavior. Different numbers, quality, and weight of items addressing ISA in the literature might affect the scale leading to inaccurate results.

Another topic of research debate is whether ISA varies depending on the educational background about the issue. In their study discussing university students’ ISA, Karacı et al. (2017) found out that pre-service teachers exhibit more successful behaviors regarding information security if they went through training to this end. On the other hand, Akgün and Topal (2015) carried out a study on senior students in classroom teaching, and Gökmen and Akgün (2015a) conducted a study on students attending Computer Education and Instructional Technology to shed light on their ISA. They found no difference between participants with dissimilar education background about the issue. In our study, distribution of the overall scores against majors proves the highest average in favor of Computer Education and Instructional Technology and the lowest scores for Elementary Mathematics Education. In the same scope, significant differences were found between CEIT and Elementary Mathematics Education and also between CEIT and Classroom Education. We think that the higher scores in CEIT could be owing to their initial learnings in the scope of informatics security branch in vocational high schools or higher education curriculum. This result seems in compliance with Karacı et al. (2017). However, it is at variance with findings of Akgün and Topal (2015) as well as Gökmen and Akgün (2015a).

Conclusion and Suggestions

With this research, a valid and reliable scale was developed for ISA based on the KAB model. The scale consists of 71 items with

4 factors. It has been determined that there are positive relations between the knowledge, attitude, and behavior components that make up the KAB model adopted in the development of the scale. It was seen that the awareness levels of both male and female pre-service teachers were at a moderate level. It was concluded that men’s awareness scores were significantly higher than women’s. In addition, it has been determined that the ISA levels of the information technology pre-service teachers are higher than the teacher candidates studying in other majors.

The current results can pave the way for similar studies in the future or guide designing, developing, implementing and evaluating programs on information security for beneficiaries. The participants in this research were pre-service teachers. A new study can be planned for university students studying engineering or in different fields. Also, it can be carried out with qualitative studies that will examine the reasons for the difference between women and men in ISA.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – A.İ.B., Y.K.; Design – A.İ.B., Y.K.; Supervision – Y.K.; Materials – A.İ.B., Y.K.; Data Collection and/or Processing – A.İ.B., Y.K.; Analysis and/or Interpretation – A.İ.B., Y.K.; Literature Review – A.İ.B., Y.K.; Writing – A.İ.B., Y.K.; Critical Review – Y.K.

Declaration of Interests: The authors declare that they have no competing interest.

Funding: The authors declare that this study had received no financial support.

Hakem Değerlendirmesi: Dış bağımsız.

Yazar Katkıları: Fikir – A.İ.B., Y.K.; Tasarım – A.İ.B., Y.K.; Denetleme – Y.K.; Kaynaklar – A.İ.B., Y.K.; Veri Toplanması ve/veya İşlemesi – A.İ.B., Y.K.; Analiz ve/veya Yorum – A.İ.B., Y.K.; Literatür Taraması – A.İ.B., Y.K.; Yazıyı Yazan – A.İ.B., Y.K.; Eleştirel İnceleme – Y.K.

Çıkar Çatışması: Yazarlar, çıkar çatışması bildirmemişlerdir.

Finansal Destek: Yazarlar, bu çalışma için finansal destek almadıklarını beyan etmişlerdir.

References

- Agamba, J. J., & Keengwe, J. (2012). Pre-service teachers’ perceptions of information assurance and cyber security. *International Journal of Information and Communication Technology Education*, 8(2), 94–101. [\[CrossRef\]](#)
- Akgün, Ö. E., & 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. [\[CrossRef\]](#)
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, 29(4), 432–445. [\[CrossRef\]](#)
- Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176–183. [\[CrossRef\]](#)
- Aslay, F. (2017). Cyber attack methods and current situation analysis of Turkey’s cyber safety. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24–28.
- Aydaner, G., Çelik, U., & Nart, S. (2017). Public and private sector cooperation for cyber security. In *Proceeding of the X. International conference on information security and cryptology* (pp. 57–67). Ankara, Turkey.
- Burkell, J. A., Fortier, A., Di Valentino, L., & Roberts, S. T. (2015). *Enhancing key digital literacy skills: Information privacy, information security, and copyright/intellectual property*. FIMS Publications. <https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1038&context=fimspub>

- Büyüköztürk, Ş. (2002). Factor analysis: Basic concepts and using to development scale. *Educational administration. Theory and into Practice*, 8(4), 470–483.
- Büyüköztürk, Ş. (2017). *Sosyal Bilimler için Veri Analizi El Kitabı [Handbook of data analysis for social sciences]*. Pegem Publishing.
- Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. [CrossRef]
- Çakır, H., Hava, K., Gülen, Ş. B., & Özüdoğru, G. (2015a). An investigation of pre-service teachers' security awareness on social networking sites—Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *International Journal of Human Sciences*, 12(1), 887–902. [CrossRef]
- Çakır, H., Özüdoğru, G., Bozkurt, Ş. B., & Hava, K. (2015b). An investigation of pre-service teachers' privacy awareness on social networking sites. *Journal of Kırşehir Education Faculty*, 16(2), 235–249.
- Cavus, N., & Ercag, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology*, 47(1), 76–90. [CrossRef]
- Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2016). *Sosyal Bilimler için Çok Değişkenli İstatistik SPSS ve LISREL Uygulamaları [Multivariate statistics for social sciences: SPSS and LISREL applications]*. Pegem Publishing.
- Colwill, C. (2009). Human factors in information security: The insider threat—Who can you trust these days? *Information Security Technical Report*, 14(4), 186–196. [CrossRef]
- Domínguez, C. M. F., Ramaswamy, M., Martínez, E. M., & Cleal, M. G. (2010). A framework for information security awareness programs. *Issues in Information Systems*, 11(1), 402–409.
- Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*, 14(4), 223–229. [CrossRef]
- Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93–106.
- Ferrari, A. (2012). Digital competence in practice: An analysis of frameworks. *Sevilla: JRC IPTS*. [CrossRef]
- Field, A. (2009). *Discovering statistics using SPSS* (3rd ed). Sage Publication.
- Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A Literature review. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity* (pp. 269–280). Springer. [CrossRef]
- Gökmen, Ö. F., & Akgün, Ö. E. (2015a). Analysis of computer education and instructional technology teacher candidates' efficacy perceptions to teach information security. *Elementary Education Online*, 14(4), 1208–1221. [CrossRef]
- Gökmen, Ö. F., & Akgün, Ö. E. (2015b). An analysis of computer education and instructional technology student teachers' knowledge of information security according to several variables. *Çukurova University Faculty of Education Journal*, 44(1), 61–84.
- Gökmen, Ö. F., & Akgün, Ö. E. (2016). Teacher candidates' experiences of cyber crime and their views for the information security course content. *Mustafa Kemal University Journal of Social Sciences Institute*, 13(33), 178–193.
- Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Development of information security awareness scale (ISAS) for secondary education students. *Elementary Education Online*, 15(2), 682–695. [CrossRef]
- IBM. (2015). *IBM 2015 cyber security intelligence index for financial services*.
- ISF. (2002). *Effective security awareness – Workshop report*. Information Security Forum.
- ISO/IEC. (2005). *ISO/IEC 27002: Code of practice for information security management*.
- ISTE. (2008). *ISTE standards: Teachers*. https://id.iste.org/docs/pdfs/20-14_ISTE_Standards-T_PDF.pdf
- Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20(2), 196–213. [CrossRef]
- Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Investigation of cyber security behaviors of university students. *Kastamonu Education Journal*, 25(6), 2079–2094. [CrossRef]
- Kaspersky Lab (2015). The Great Bank Robbery: Carbanak cybergang steals \$1bn from 100 financial institutions worldwide. https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals-1bn-from-100-financial-institutions-worldwide.
- Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers and Security*, 70, 663–674. [CrossRef]
- Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). Guilford Press.
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289–296. [CrossRef]
- Lin, W., Yang, H. C., Hang, C. M., & Pan, W. H. (2007). Nutrition knowledge, attitude, and behaviour of Taiwanese elementary school children. *Asia Pacific Journal of Clinical Nutrition*, 16(Suppl. 2), 534–546.
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviours. *Computers in Human Behavior*, 83, 32–44. [CrossRef]
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017) Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156. [CrossRef]
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia – Social and Behavioral Sciences*, 147, 424–428. [CrossRef]
- Metzger, M. (2017). *FBI says Ransomware soon becoming a billion dollar business*. Scientia Media UK. <https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-billion-dollar-business/article/1475539>
- Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers and Security*, 53, 132–142. [CrossRef]
- Öğütçü, G., Cırakoğlu, O. C., & Cula, S. (2016). Information security in the world of digital natives: How internet addiction, sensation seeking and information security behaviours are related. *International Journal of Management and Applied Science*, 2(9), 79–84.
- 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 and Security*, 42, 165–176. [CrossRef]
- Pearson (2015). *Pearson student mobile device survey*. <https://www.pearsoned.com/wp-content/uploads/2015-Pearson-Student-Mobile-Device-Survey-College.pdf>.
- Pusey, P., & Sadara, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, 28(2), 82–85. [CrossRef]
- Raykov, T., & Marcoulides, G. A. (2006). *A first course in structural equation modeling* (2nd ed). Erlbaum.
- Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research*, 8(2), 23–74.
- Smith, G. T. (2012). *Impact of security awareness programs on end-user security behaviour: A quantitative study of federal workers* [Doctoral Dissertation]. Capella University.
- Sonck, N., Livingstone, S., Kuiper, E., & de Haan, J. (2011). Digital literacy and safety skills. EU Kids Online, London School of Economics & Political Science. <http://eprints.lse.ac.uk/33733/>
- Spafford, E. H. (1992). Opus: Preventing weak password choices. *Computers and Security*, 11(3), 273–278. [CrossRef]

- Symantec. (2018). *Executive summary 2018 Internet security threat report (ISTR-23)*. <https://docs.broadcom.com/doc/istr-23-executive-summary-en>
- Tekerek, M., & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, 2(17341), 61–70. [CrossRef]
- Tolvanen, M., Lahti, S., Miettunen, J., & Hausen, H. (2012). Relationship between oral health-related knowledge, attitudes and behaviour among 15–16-year-old adolescents - A structural equation modeling approach. *Acta Odontologica Scandinavica*, 70(2), 169–176. [CrossRef]
- Turkish Statistical Institute [TurkStat]. (2021). *Information and communication technology (ICT) usage survey on households and individuals*. [https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-\(ICT\)-Usage-in-Households-and-by-Individuals-2021-37437](https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2021-37437).
- Wahyudiwan, D. D. H., Suchahyo, Y. G., & Gandhi, A. (2017). Information security awareness level measurement for employee: Case study at Ministry of Research, Technology, and Higher Education. In *Proceeding of the 3rd International Conference on Science in Information Technology (ICSITech)* (pp. 654–658). Bandung, Indonesia. [CrossRef]
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Course Technology Press.
- Xu, W., Sun, G., Lin, Z., Chen, M., Yang, B., Chen, H., & Cao, K. (2010). Knowledge, attitude, and behaviour in patients with atrial fibrillation undergoing radiofrequency catheter ablation. *Journal of Interventional Cardiac Electrophysiology*, 28(3), 199–207. [CrossRef]
- Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Digital data security awareness of teachers. *Sakarya University Journal of Education*, 6(2), 26–45. [CrossRef]

Genişletilmiş Özet

Giriş

21. yüzyılın önemli becerilerinden biri olarak kabul edilen dijital okuryazarlık becerisi, bireylerin, dijital ortamlarda görevlerini yerine getirirken karşılaşılabilecekleri sorunları çözebilecek teknik, bilişsel ve sosyolojik becerilere sahip olmalarını ve bu becerileri kullanmaları için gereklidir. Dijital okuryazarlık becerisi, dijital çağda hayatta kalma becerisi olarak da görülmektedir. Günümüzde bilgi güvenliği, dijital okuryazarlık becerilerinin bir alt boyutu olarak değerlendirilmektedir.

Yaşanan hızlı teknolojik gelişmeler, oluşan yeni durum ve şartlar, bilgi ve iletişim teknolojilerini günlük yaşantımızın vazgeçilmez bir unsuru haline getirmiştir. Bu durum bilgiye hızlı ve kolay ulaşma, sosyal, kültürel ve akademik yaşantıda yenilikler getirme avantajlarının yanında bilgi güvenliği kurallarına dikkat edilmemesi durumunda bir takım bireysel ve toplumsal sorunların ortaya çıkmasına neden olmaktadır. Yapılan araştırmalar bilgi güvenliği sorunlarının altında yatan temel nedenin insan hatası olduğunu rapor etmektedir. Dijital ortamlarda bilgi güvenliğinin nasıl sağlanacağı ile ilgili farkındalığın yeterli düzeyde olmaması olumsuz durumların yaşanmasının en önemli sebeplerinden biri olarak gösterilmektedir. Bu sorunların önüne geçebilmek için ilkokuldan itibaren öğrencilerde ve velilerde bilgi ve iletişim teknolojilerinin kullanımıyla ilgili bilgi güvenliği farkındalığı oluşturulmalıdır. Öğrencilerin, bilgi güvenliği farkındalığı hususunda bilinçlendirilmesinde, öğretmenler önemli görevler üstlenebilir. Bundan dolayı, gelecekte öğretmenlik mesleğini yürütecek günümüz öğretmen adaylarının bilgi güvenliği konusunda bilinçlendirilmesi oldukça önemlidir.

Çalışmada bilgi güvenliği farkındalığını incelemek için Kruger ve Keaney'in çalışmasında kullandığı sosyal psikolojideki Bilgi-Tutum-Davranış (KAB) modelinden yararlanılmıştır. Modele göre farkındalık aşağıdaki bileşenlerden oluşmaktadır.

- i. Bilgi: Konu hakkında birey ne biliyor?
- ii. Tutum: Konu hakkında birey ne düşünüyor?
- iii. Davranış: Birey bu konuda ne yapıyor?

Literatüre göre bilgi, tutum ve davranış bileşenleri birbiriyle ilişkilidir.

Mevcut literatürde öğretmen adaylarının bilgi, tutum ve davranış bileşenleriyle ilgili farkındalıklarını inceleyen herhangi bir çalışmaya rastlanmamıştır. Bu çalışma ile KAB modeline dayalı bilgi güvenliği farkındalığı için geçerli ve güvenilir bir ölçek geliştirmek ve elde edilen verilerle öğretmen adaylarının bilgi güvenliği farkındalıklarını incelemek amaçlanmıştır.

Yöntem

Araştırmanın katılımcıları 350 öğretmen adaydır. Bu çalışmada, öğretmen adaylarının bilgi güvenliği farkındalıklarını değerlendirmek için araştırmacılar tarafından ölçek geliştirilmiştir. Ölçek, KAB modeline dayanmaktadır. BGF ölçeğini geliştirme aşamaları aşağıdaki gibidir.

- Taslak maddelerin oluşturulması
- Uzman görüşlerinin alınması
- Pilot çalışmanın yapılması
- Asıl çalışmanın yapılması

Ölçeğin geçerliliği ve güvenilirliği açımlayıcı faktör analizi (AFA), madde analizi ve doğrulayıcı faktör analizi (DFA) ile kontrol edilmiştir. Araştırmanın bir diğer amacı olan öğretmen adaylarının bilgi güvenliği farkındalıklarını incelemek için korelasyon analizi, bağımsız gruplar t-testi ve tek yönlü varyans analizi (ANOVA) kullanılmıştır.

Bulgular ve Tartışma

Ölçeğin faktör yapısını belirlemek için Varimax döndürme tekniği ile birlikte yapılan temel bileşenler analizi sonucu, 71 maddeden oluşan toplam varyansın % 40'ını açıklayan dört faktörlü bir yapı elde edilmiştir. Maddelerin içerikleri ile uyumlu olacak şekilde; birinci faktör "bilgi güvenliğine yönelik tutum," ikinci faktör "bilgi güvenliği ile ilgili bilgi," üçüncü faktör "bilgi güvenliğine yönelik davranış" ve dördüncü faktör "kişisel cihaz güvenliğine yönelik davranış" olarak adlandırılmıştır. 71 maddelik ölçeğin tamamının güvenilirlik katsayısı 0,95 olarak hesaplanmıştır. Daha sonra AFA'dan elde edilen yapıyı doğrulamak için DFA yapılmıştır. Model uyumu için Ki-Kare (χ^2)/df, SRMR, RMSEA ve CFI uyum indeksleri dikkate alınmıştır. Model uyum indeksi değerleri dikkate alındığında modelin iyi bir uyuma sahip olduğu ifade edilebilir.

Ölçeğin geliştirilmesinde temel alınan KAB modeli bileşenlerinden bilgi, tutum ve davranış arasında anlamlı bir ilişkinin olup olmadığını araştırmak için korelasyon analizi gerçekleştirilmiştir. Korelasyon analizi sonuçları bilgi, tutum ve davranış bileşenleri arasında pozitif ve anlamlı bir ilişkinin var olduğunu ortaya çıkarmıştır. Dolayısıyla bireylerin bilgi güvenliğine yönelik bilgi düzeyleri arttıkça tutumları ve davranışları olumlu olarak etkilenebileceği söylenebilir.

Hem erkek hem de kadın öğretmen adaylarının bilgi güvenliği farkındalık düzeylerinin orta seviye olduğu görülmüştür. Çalışmada, bilgi güvenliği farkındalığında cinsiyet farklılığı olup olmadığı t-testi analizi ile incelenmiştir. T-testi sonuçları, ölçeğin tamamı için erkeklerin lehine anlamlı bir farklılığın olduğunu göstermiştir.

Bilgi güvenliği farkındalığının bölümlere göre farklılık gösterip göstermediği ANOVA testi ile incelenmiştir. ANOVA testi sonuçlarında, Bilgisayar ve Öğretim Teknolojileri Öğretmenliği bölümü öğretmen adayları lehine anlamlı farklılıkların olduğu görülmüştür.

Sonuç ve Öneriler

Bu çalışma ile Bilgi-Tutum-Davranış (KAB) modeline dayalı bilgi güvenliği farkındalığı için geçerli ve güvenilir bir ölçek geliştirilmiştir. Ölçek dört faktörlü 71 maddeden oluşmaktadır. Ölçeğin geliştirilmesinde benimsenen KAB modelini oluşturan bilgi, tutum ve davranış bileşenleri arasında olumlu ilişkilerin olduğu tespit edilmiştir. Hem erkek hem de kadın öğretmen adaylarının farkındalıkları orta düzeydedir. Bununla beraber, erkeklerin farkındalık puanlarının kadınlara göre anlamlı olarak daha yüksek olduğu sonucuna varılmıştır. Ayrıca Bilgisayar ve Öğretim Teknolojileri Öğretmenliği bölümü öğretmen adaylarının bilgi güvenliği farkındalık düzeylerinin diğer branşlarda eğitim alan öğretmen adaylarına göre daha yüksek olduğu tespit edilmiştir.

Çalışmanın sonuçları, gelecekte yapılması düşünülen benzer çalışmalara veya verilmesi düşünülen bilgi güvenliği eğitim programının tasarlanması, geliştirilmesi, uygulanması ve değerlendirilmesi süreçlerine rehberlik edebilir. Bu araştırmanın katılımcıları öğretmen adaylarıdır. Mühendislik veya farklı alanlarda okuyan üniversite öğrencileri için yeni bir çalışma planlanabilir. Ayrıca bilgi güvenliği farkındalığı konusunda kadın ve erkek öğrenciler arasındaki farklılığın nedenlerini detaylı bir şekilde inceleyecek nitel veya karma araştırmalar gerçekleştirilebilir.

Etik Kurul Belgesi: Çalışmanın verileri 2020 yılından önce toplandığından dolayı Etik Kurul Onay Belgesi alınmamıştır.