*International Journal of Turkish Education Sciences,*
2026, Advanced Online Publication
https://doi.org/10.46778/goputeb.1811659

ISSN: 2148-2314

# Investigation of pre-service teachers' information security knowledge and information security awareness through canonical correlation analysis

Neşe Sevim Cirak [a] Ayşe Gökçe Ulutaş [b] Vesile Gül Başer Gülsoy [c]

[a] *Burdur Mehmet Akif Ersoy University, Türkiye, nsevim@mehmetakif.edu.tr*

[b] *Burdur Mehmet Akif Ersoy University, Türkiye, ayseulutas@mehmetakif.edu.tr*

[c] *Burdur Mehmet Akif Ersoy University, Türkiye, vbaser@mehmetakif.edu.tr*

**ABSTRACT**

The purpose of this study was to examine the relationship between pre-service teachers' information security knowledge and information security awareness. In this context, a correlational research design, one of the general survey models, was used in the study. The sample consisted of a total of 284 pre-service teachers, 112 from the Department of Elementary Mathematics Education and 172 from the Department of Early Childhood Education. In the study, data were collected using the Information Security Knowledge Scale and the Information Security Awareness Scale. Descriptive statistics and canonical correlation analysis were used to analyze the data. The results indicated that pre-service teachers' information security awareness levels were high across the total scale and sub-dimensions. In contrast, their information security knowledge levels were moderate across the total scale and sub-dimensions. In addition, a significant positive relationship was found between pre-service teachers' information security knowledge and awareness. As a result of the canonical correlation analysis, the Information Security Awareness variable set explained 16.2% of the variance in the Information Security Knowledge variable set. Conversely, the Information Security Knowledge variable set explained 5.5% of the variance in the Information Security Awareness variable set.

**Article Type**
Research

**Article Background**
Received:
January 12, 2026
Accepted:
March 30, 2026
Published Online:
July 20, 2026

**Keywords**
Information Security Knowledge, Information Security Awareness, Pre-service Teachers

**To cite this article**: Sevim Cirak, N., Gökçe Ulutaş, A., & Başer Gülsoy, V. G. (2026). Investigation of pre-service teachers' information security knowledge and information security awareness through canonical correlation analysis. *International Journal of Turkish Education Sciences.* Advanced Online Publication. https://doi.org/10.46778/goputeb.1811659

**Corresponding Author:** Neşe Sevim Cirak, e-mail: nsevim@mehmetakif.edu.tr

## Introduction

Information and communication technologies (ICT) have become an integral part of human life due to the opportunities they offer and the convenience they provide (Hakkari, 2022). Developments in ICT enable users to access, produce, share, and protect information (Avcı & Oruç, 2020; Hakkari, 2022). One of the main reasons ICT has assumed such an important place in everyday life is the internet, which allows individuals to connect with the world (Avcı & Oruç, 2020) and offers opportunities to learn about and explore it (Hakkari, 2022). According to the Household Information Technologies Usage Survey conducted by the Turkish Statistical Institute (TSI), 96.4% of households in Türkiye have internet access. Internet usage rates were reported as 92.2% for males and 85.4% for females, while overall internet usage among individuals aged 16–74 reached 88.8%, reflecting a steady increase compared to previous years (TSI, 2024). These findings indicate that internet use is highly prevalent, particularly among younger populations.

While technological developments facilitate daily life, they also increase threats and attacks targeting information security. In parallel with the growing volume of information produced in digital environments, various security threats directed at both information and information technologies have emerged (Gökçearslan et al., 2021; Kruger & Kearney, 2006). Despite high levels of internet use, many users have limited knowledge and awareness of the risks they may encounter in online environments (Aiken, 2019, as cited in Shillair et al., 2022). Similarly, although increased technology use enhances convenience, it has also led to various security problems, rendering information security an issue that requires careful consideration (Karaoğlan-Yılmaz & Çavuş-Ezin, 2017; Pontoan et al., 2023).

Information security is commonly defined as the prevention of unauthorized access to information and its protection against inappropriate access and use (Lugnet et al., 2020; Puhakainen, 2006). Similarly, it is described as preventing unauthorized access to information and ensuring that information is transmitted between the sender and the receiver in accordance with security principles (Ünver et al., 2011). In a broader sense, Whitman and Mattord (2009) define information security as the protection of information itself, the components that create it, and the systems and hardware that enable its creation, storage, and distribution. Consistent with these definitions, information security can also be understood as safeguarding information against unauthorized access, use, modification, damage, or destruction (Çetinkaya et al., 2017). Information security is built upon three fundamental components: confidentiality, integrity, and availability (Puhakainen, 2006; Weippl & Ebner, 2008). Confidentiality refers to protecting information from unauthorized access; integrity involves preventing unauthorized modification or deterioration; and availability ensures that authorized users can access and use information whenever needed (Baykara et al., 2013; von Solms & Niekerk, 2013; Wang, 2022). The absence of any of these components may result in significant information security risks (Çetinkaya et al., 2017).

Ensuring information security requires the integrated consideration of people, processes, and technology (Eminağaoğlu & Gökşen, 2009). Accordingly, information security should not be addressed solely through technical and infrastructural measures; the human factor must also be taken into account, and appropriate precautions should be implemented by identifying users' levels of information security awareness (ISA) (Çetinkaya & Öktelik, 2022; Rezgui & Marks, 2008). Factors such as unconscious or improper technology use, insufficient awareness levels, and the increasing

diversity of threat types further complicate efforts to ensure information security (Güldüren et al., 2020; Öğütçü et al., 2016). In this context, it can be argued that ensuring information security at both personal and institutional levels requires all users to possess a certain level of information security awareness. Similarly, the literature emphasizes that one key measure for maintaining information security is to provide users with training and inform them about security-related issues (Canbek & Sağıroğlu, 2007). Furthermore, Avcı and Oruç (2020) state that ISA can be developed through education and that such awareness should be fostered from early childhood.

The role of the human factor in information security is closely related to users' knowledge and behaviors (Kruger et al., 2010). Knowledge refers to users' understanding of situations, concepts, and practices related to information security. To ensure information security, users need to understand the core principles of confidentiality, integrity, and availability, and recognize their relationships. Such knowledge enables individuals to make more informed decisions and adopt safer behaviors in digital environments (Kruger et al., 2010). In this regard, it can be argued that users' levels of knowledge regarding information security are critical for ensuring information security at both the individual and institutional levels.

Information Security Awareness (ISA) is defined as individuals' awareness of situations that threaten information security and their engagement in behaviors aimed at preventing such threats (Siponen, 2000). According to McCormac et al. (2017), ISA is closely associated with users' knowledge of security rules and their compliance with these rules in practice. Thomson et al. (2006) classified users as either competent or incompetent in terms of information security. They further indicated that incompetent users may either be aware of their deficiencies or remain unaware of them. The most critical situation arises when users lack competence in information security and are unaware of their own deficiencies. Therefore, by helping users recognize their information security shortcomings, it becomes possible to improve their skills and promote safer behaviors (Thomson et al., 2006). In this context, Kruger and Kearney (2006) developed a model based on knowledge, attitude, and behavior to examine ISA and the relationships among these components. According to this model, increases in users' knowledge positively influence their attitudes toward information security, which, in turn, lead to changes in their behavior. Supporting this perspective, Benzer and Karal (2023) found a positive relationship between pre-service teachers' information security knowledge and their security-related attitudes and behaviors. In other words, users' information security knowledge plays a significant role in shaping their attitudes and behaviors toward information security.

The literature includes several studies on ISA and ISK (Information Security Knowledge). Previous studies have reported varying levels of ISA and knowledge among students. Findings related to ISA indicate high levels (Avcı & Oruç, 2020; Göldağ, 2021; Hakkari, 2022), moderate levels (Benzer & Karal, 2023; Erdoğmuş, 2017; Gültekin & Özel, 2023; Sağır et al., 2018), or basic levels (Wang, 2022) among university students and pre-service teachers. For instance, Hakkari (2022) found that associate degree students demonstrated a certain level of awareness regarding information security. In contrast, Ndiege and Okello (2018) concluded that university students' information security awareness was insufficient. Similarly, findings related to ISK reveal predominantly low levels (Erdoğmuş, 2017) or moderate levels (Benzer & Karal, 2023; Hakkari, 2022) among university students and pre-service teachers. A review of the literature indicates that studies simultaneously examining both ISK and ISA among pre-service teachers are limited. In this respect, the present study is significant in that it addresses the relationship between these variables and helps fill an important gap in the literature.

Developments in information and communication technologies (ICT) affect not only daily life but also teaching and learning processes. Digital applications, tools, systems, and learning environments are increasingly used to enhance the effectiveness of educational practices. Within the process of technology integration in education, information security occupies a critical position and requires comprehensive preparation and investment (Wang, 2022). In addition, teachers are expected to possess a certain level of digital competence in order to use these digital platforms effectively in educational settings (Kılıç, 2022). In this sense, it can be argued that teachers—and pre-service teachers as future educators—should demonstrate behaviors aimed at protecting information by possessing adequate levels of ISK and ISA in order to prevent potential security breaches in digital environments. A review of the relevant literature indicates a notable lack of studies that address pre-service teachers' ISK and ISA simultaneously. Based on this gap, the present study is expected to contribute to the literature by identifying pre-service teachers' levels of ISK and ISA. Accordingly, the purpose of this study is to determine pre-service teachers' levels of ISK and ISA and to examine the relationship between these constructs. In line with this purpose, the following research questions were addressed:

What are the levels of pre-service teachers' ISK and ISA?

Is there a statistically significant relationship between pre-service teachers' ISK and ISA levels?

To what extent does the ISK variable set explain the variables in the ISA dataset?

To what extent does a single variable within the ISK dataset contribute to predicting the combined variables of the ISA dataset?

## Method

### Research Design

The purpose of this study is to examine the relationship between pre-service teachers' Information Security Awareness (ISA) levels and Information Security Knowledge (ISK) levels. In line with this purpose, a correlational research design, one of the general survey models, was employed. Correlational research designs allow researchers to determine the direction and strength of relationships between variables and to describe existing conditions as they naturally occur. In this design, the researcher does not intervene in or manipulate the variables; instead, the relationships among variables in their existing conditions are analyzed using statistical methods. Although correlational studies reveal relationships among variables, they are not intended to establish direct causal conclusions (Creswell & Creswell, 2018; Fraenkel et al., 2011).

### Participants

The study sample consisted of 284 pre-service teachers, including 209 females (73.6%) and 75 males (26.4%), enrolled in the Faculty of Education at a public university located in the Mediterranean region of Türkiye during the fall semester of the 2024–2025 academic year. Participants were selected using convenience sampling, a non-probability sampling method in which the sample comprises individuals who are easily accessible to the researcher; therefore, it is widely used in social science research (Clark, 2007; Etikan et al., 2016). Fraenkel et al. (2011) note that convenience sampling may limit the representativeness of the target population and, consequently, the external validity of the study. To address this limitation and enhance transparency, participants' demographic

characteristics are presented in detail. Accordingly, Table 1 summarizes the demographic characteristics of the pre-service teachers included in the study.

Table 1

*Demographic Characteristics of the Participants*

| | | *N* | % |
|---|---|---|---|
| Gender | Female | 209 | 73.6 |
| | Male | 75 | 26.4 |
| Grade | 1 | 51 | 18.0 |
| | 2 | 125 | 44.0 |
| | 3 | 29 | 10.2 |
| | 4 | 79 | 27.8 |
| Department | Elementary Mathematics Education | 112 | 39.4 |
| | Early childhood education | 172 | 60.6 |
| Years of Internet Use | 1 to <4 years | 23 | 8.1 |
| | 4 to <6 years | 27 | 9.5 |
| | 6 years or more | 234 | 82.4 |
| Daily Internet Use | Less than 1 hour | 10 | 3.5 |
| | 1 to <2 hours | 33 | 11.6 |
| | 2 to <4 hours | 107 | 37.7 |
| | 4 hours or more | 134 | 47.2 |
| Internet Usage Skill | Beginner | 11 | 3.9 |
| | Intermediate | 184 | 64.8 |
| | Advanced | 89 | 31.3 |
| Total | | 284 | 100 |

**Data Collection Instruments**

In this study, data were collected using the Information Security Awareness Scale and the Information Security Knowledge Scale. Both scales have been shown to be reliable and valid in previous research. Participants completed the scales voluntarily, and their responses were kept confidential to protect their privacy.

*Information Security Awareness Scale:* The Information Security Awareness Scale, developed by Erdoğmuş (2017), consists of 18 items rated on a five-point Likert scale and comprises five sub-dimensions: Internet Security (5 items), Social Media Use (4 items), Web Browser and Network Security (3 items), Password Creation (3 items), and Social Media Traps (3 items). Total scores obtained from the scale range from 18 to 90, with higher scores indicating higher levels of information security awareness. In the original scale development study, the internal consistency coefficient (Cronbach's alpha) for the overall scale was reported as .96. Reliability coefficients for the sub-dimensions were .90 for Internet Security, .94 for Social Media Use, .87 for Web Browser and Network Security, .86 for Password Creation, and .91 for Social Media Traps (Erdoğmuş, 2017).

In the present study, the Cronbach's alpha coefficient for the overall scale was calculated as .90. The reliability coefficients for the sub-dimensions were found to be .76 for Internet Security, .81 for Social Media Use, .75 for Web Browser and Network Security, .75 for Password Creation, and .77 for Social Media Traps. These results indicate acceptable internal consistency for all dimensions.

*Information Security Knowledge Scale:* The Information Security Knowledge Scale, developed by Erdoğmuş (2017), consists of 13 items rated on a five-point Likert scale and comprises two sub-dimensions: Threats (7 items) and Precautions (6 items). Total scores obtained from the scale range

from 13 to 65, with higher scores indicating higher levels of information security knowledge. In the original scale development study, the internal consistency coefficient (Cronbach's alpha) for the overall scale was reported as .94, while the reliability coefficients were .91 for the Threats sub-dimension and .91 for the Precautions sub-dimension (Erdoğmuş, 2017). In the present study, the Cronbach's alpha coefficient for the overall scale was calculated as .93, with reliability coefficients of .87 for the Threats sub-dimension and .90 for the Precautions sub-dimension, indicating high internal consistency.

**Data Analysis**

Descriptive statistics were used to determine pre-service teachers' levels of ISA and ISK. Mean scores were interpreted as follows: 1.00–2.33 = low, 2.34–3.67 = moderate, and 3.68–5.00 = high. In addition, Canonical Correlation Analysis (CCA) was employed to examine the multivariate relationships between the ISA dataset, comprising Internet Security, Web Browser and Network Security, Social Media Traps, Social Media Use, and Password Creation, and the ISK dataset, comprising Threats and Precautions. The analyses were conducted using SPSS 25.

Canonical correlation analysis is a multivariate statistical technique that maximizes the relationships between two sets of variables by deriving canonical functions (Tabachnick & Fidell, 2013). The primary purposes of canonical correlation analysis are to: (1) examine relationships between multiple dependent and independent variable sets, (2) maximize the correlations between these variable sets through canonical functions, and (3) evaluate the relative contribution of each variable to the canonical functions (Tabachnick & Fidell, 2013). This technique also reduces the probability of committing a Type I error when examining relationships among multiple variables (Thompson, 2005). For these reasons, canonical correlation analysis was deemed appropriate for the present study.

The number of canonical functions that can be extracted depends on the number of variables in each dataset, with the maximum number determined by the dataset containing the fewest variables (Thompson, 2005). In this study, the ISA dataset included five variables, whereas the ISK dataset consisted of two variables. Accordingly, two canonical functions (roots) were extracted and examined.

**Assumptions of Canonical Correlation Analysis**

Prior to conducting Canonical Correlation Analysis (CCA), several statistical assumptions must be examined (Tabachnick & Fidell, 2013). These assumptions include sample size adequacy, univariate and multivariate normality, linearity, absence of multicollinearity among variables, and homoscedasticity. Violations of these assumptions can lead to biased or unreliable results; therefore, they were assessed before conducting the analysis.

Regarding sample size, Stevens (2009) recommends that the number of participants should be at least 20 times the total number of variables included in the analysis. In the present study, the ISA dataset consisted of five variables. In comparison, the ISK dataset included two variables, resulting in a minimum required sample size of 140 participants. As the study included 284 participants, the sample size exceeded the recommended minimum for performing a canonical correlation analysis.

Univariate normality was assessed by examining skewness and kurtosis values, histograms, and Q–Q plots. The results indicated that skewness and kurtosis values for all variables fell within the

acceptable range of -1.5 to +1.5 (Tabachnick & Fidell, 2013). Visual inspection of histograms and Q–Q plots further supported the assumption of normal distribution.

To assess multivariate normality and identify potential outliers, Mahalanobis distance values were calculated. The analysis revealed that none of the distance values exceeded the critical value of 24.32, indicating the absence of multivariate outliers (Pearson & Hartley, 1958). Therefore, the data were considered suitable for Canonical Correlation Analysis.

Canonical correlation analysis also requires linear relationships among variables. To evaluate this assumption, scatterplots for each pair of variables were examined for outliers and curvilinear patterns. The inspection indicated meaningful and linear relationships among the variables.

The assumption of the absence of multicollinearity was examined by calculating Pearson correlation coefficients among the variables. All correlation coefficients were below .90, suggesting no multicollinearity issues (Tabachnick & Fidell, 2013). In addition, the Variance Inflation Factor (VIF) and tolerance values were examined. The results showed that tolerance values were greater than .10 and VIF values were less than 10, confirming that multicollinearity was not a concern (O'Brien, 2007).

Finally, homoscedasticity, which refers to the assumption that the variance of error terms is constant across all levels of the independent variables, was evaluated. Examination of the relevant scatterplots indicated that this assumption was satisfied. Thus, it can be concluded that the data met all the necessary assumptions for conducting Canonical Correlation Analysis.

### Ethical Approval

Ethical principles were strictly observed in the present study, and the necessary ethical approval was obtained prior to data collection. This study was approved by Burdur Mehmet Akif Ersoy University institutional ethics committee; approval number: GO 2022/891; approval date: 05.10.2022.

## Findings

### Levels of Pre-service Teachers' Information Security Awareness and Information Security Knowledge

Descriptive statistics, including means and standard deviations for each sub-dimension, were calculated to provide an overview of the participants' ISA and ISK levels. These statistics help to identify patterns and variations in the data before conducting further analyses. The findings related to pre-service teachers' ISA and ISK levels are presented in Table 2.

As shown in Table 2, pre-service teachers demonstrated high levels of information security awareness across the overall scale and all sub-dimensions. In contrast, their information security knowledge levels were moderate across the overall scale and its sub-dimensions. Within the ISA dataset, pre-service teachers obtained the highest mean score in the Web Browser and Network Security sub-dimension ($M$ = 4.36, $SD$ = 0.71), whereas the lowest mean score was observed in the Social Media Use sub-dimension ($M$ = 4.08, $SD$ = 0.59). Regarding the ISK dataset, pre-service teachers demonstrated higher mean scores in the Precautions sub-dimension ($M$ = 3.09, $SD$ = 0.87) compared to the Threats sub-dimension ($M$ = 2.80, $SD$ = 0.88).

Table 2

*Levels of Pre-service Teachers' Information Security Awareness and Knowledge*

| Variables | *N* | Min | Max | *X* | *SD* | Level |
|---|---|---|---|---|---|---|
| Information Security Awareness (Total) | 284 | 2.50 | 5.00 | 4.21 | 0.50 | High |
| Internet Security | 284 | 2.40 | 5.00 | 4.26 | 0.55 | High |
| Social Media Use | 284 | 2.50 | 5.00 | 4.08 | 0.59 | High |
| Web Browser and Network Security | 284 | 2.33 | 5.00 | 4.36 | 0.71 | High |
| Password Creation | 284 | 2.00 | 5.00 | 4.12 | 0.70 | High |
| Social Media Traps | 284 | 2.00 | 5.00 | 4.15 | 0.70 | High |
| Information Security Knowledge (Total) | 284 | 1.00 | 5.00 | 2.94 | 0.82 | Moderate |
| Threats | 284 | 1.00 | 5.00 | 2.80 | 0.88 | Moderate |
| Precautions | 284 | 1.00 | 5.00 | 3.09 | 0.87 | Moderate |

**Canonical Correlation Analysis Results**

CCA was conducted to examine the relationship between the ISA and the ISK dataset. The ISA dataset consisted of five dimensions: Internet Security, Web Browser and Network Security, Social Media Traps, Social Media Use, and Password Creation. The ISK dataset consisted of two dimensions: Threats and Precautions.

Table 3

*Canonical Correlation Analysis Results*

| Roots | *rc* | $rc^2$ | Eigenvalue | Wilks' Lambda | *F* | *Df* | *p* |
|---|---|---|---|---|---|---|---|
| 1 | .43 | .187 | .229 | .790 | 6.935 | 10 | .000 |
| 2 | .17 | .029 | .030 | .971 | 2.103 | 4 | .081 |

As shown in Table 3, the first canonical function was statistically significant, with a canonical correlation coefficient of .43, corresponding to 18.7% shared variance (Wilks' $\Lambda$ = .790, $F(10, 554) = 6.935$, $p < .001$). In contrast, the second canonical function was not statistically significant (canonical correlation = .17, shared variance = 2.9%; Wilks' $\Lambda$ = .971, $F(4, 278) = 2.103$, $p = .081$). Therefore, only the first canonical function was retained for interpretation, consistent with the recommendations of Tabachnick and Fidell (2013).

Canonical Loadings and Explained Variance

Table 4 presents the standardized canonical weights and canonical loadings for the variables in each variable set. The canonical loadings were used to interpret the variables most strongly associated with the first canonical variate.

As shown in Table 4, Web Browser and Network Security (−.75) and Internet Security (−.70) exhibited the strongest canonical loadings in Set 1, indicating that these variables were most strongly associated with the first canonical variate. In contrast, Social Media Use (−.08) showed the weakest canonical loading. In Set 2, both Threats (−.98) and Precautions (−.88) exhibited very strong canonical loadings, indicating that both variables were strongly associated with the first canonical variate, with Threats showing a slightly stronger association than Precautions. The first canonical variate explained 29.7% of the variance in the ISA variable set and 87.0% of the variance in the ISK variable set.

Table 4

*Standardized Canonical Weights and Canonical Loadings for Each Variable Set*

| Variable | Canonical Weights (Standardized) | Canonical Loading |
|---|---|---|
| Set 1- Information Security Awareness | | |
| Internet Security | -.66 | -.70 |
| Social Media Use | .73 | -.08 |
| Web Browser and Network Security | -.63 | -.75 |
| Password Creation | -.03 | -.34 |
| Social Media Traps | -.20 | -.57 |
| Explained Variance (%) | | 29.7 |
| Set 2– Information Security Knowledge | | |
| Threats | -.72 | -.98 |
| Precautions | -.33 | -.88 |
| Explained Variance (%) | | 87 |

Based on the standardized canonical weights presented in Table 4, the canonical variate equations were formed as follows:

Set 1 (Information Security Awareness) = –.66(Internet Security) + .73(Social Media Use) – .63(Web Browser and Network Security) – .03(Password Creation) – .20(Social Media Traps)

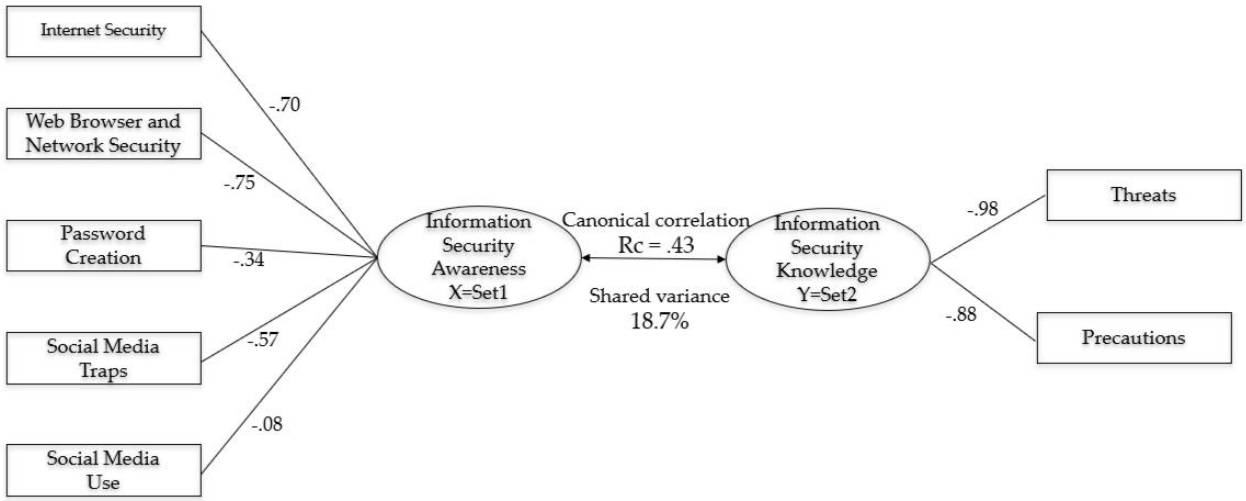
Set 2 (Information Security Knowledge) = –.72(Threats) – .33(Precautions)

**Canonical Loadings and the Relationship Between the Canonical Variates**

Canonical loadings represent the correlation between each observed variable and its respective canonical variate. The variance explained by a canonical variate is calculated by averaging the squared canonical loadings of the variables within that dataset. The canonical loadings and the correlation between the first canonical function are illustrated in Figure 1.

Figure 1

*Canonical Loadings and Canonical Correlation for the First Canonical Function Between Information Security Awareness and Information Security Knowledge*



As shown in Figure 1, the correlation between the ISA and ISK canonical variates was .43, indicating a moderate positive relationship. According to Tabachnick and Fidell (2013), variables with canonical loadings greater than .30 are considered meaningful contributors to a canonical variate. Accordingly, within the ISA dataset, Internet Security (–.70), Web Browser and Network Security (–.75), Password Creation (–.34), and Social Media Traps (–.57) met this criterion, whereas Social Media Use (−.08) did not. Within the ISK dataset, both Threats (–.98) and Precautions (–.88) exceeded the threshold and were retained as meaningful contributors. Although all variables exhibited negative loadings, they were related in the same direction across both datasets, indicating that decreases in one canonical variate were associated with corresponding decreases in the other.

### Cross-Loadings

To better understand the relationships between the variables, the cross-loadings of each variable on the canonical variates were examined. Cross-loadings between the two canonical variates are presented in Table 5. The patterns observed in the cross-loadings indicate which variables contribute most strongly to the canonical relationships.

Table 5

*Cross-Loadings of Canonical Variables*

| Variable | Cross-Loading |
|---|---|
| Set 1: Information Security Awareness | Information Security Knowledge Variable Set |
| Internet Security | -.30 |
| Social Media Use | -.03 |
| Web Browser and Network Security | -.32 |
| Password Creation | -.15 |
| Social Media Traps | -.24 |
| Explained Variance (%) | 5.5 |
| Set 2: Information Security Knowledge | Information Security Awareness Variable Set |
| Threats | -.42 |
| Precautions | -.38 |
| Explained Variance (%) | 16.2 |

Table 5 shows that, in explaining ISK, the ISA variables demonstrated highest cross-loadings were Web Browser and Network Security (–.32) and Internet Security (–.30), followed by Social Media Traps (–.24), Password Creation (–.15), and Social Media Use (–.03). Collectively, the ISA dataset explained 16.2% of the variance in the ISK dataset. Conversely, in explaining ISA, the ISK variables Threats (–.42) and Precautions (–.38) accounted for 5.5% of the variance. These findings indicate an asymmetric explanatory relationship between the two datasets.

## Discussion, Conclusion, and Recommendations

### Discussion and Conclusion

This study aimed to determine pre-service teachers' Information Security Knowledge (ISK) and Information Security Awareness (ISA) levels and to examine the extent to which the ISK dataset explains the ISA dataset. For this purpose, data were collected from 284 pre-service teachers enrolled in the Faculty of Education at a public university during the fall semester of the 2024–2025 academic year.

The study's findings revealed that pre-service teachers' ISK was at a moderate level. Previous studies have reported varying results regarding university students' levels of ISK. Consistent with the present study's findings, Hakkari (2022) and Benzer & Karal (2023) noted that university students demonstrated moderate levels of ISK. In contrast, Erdoğmuş (2017) found that pre-service teachers' ISK was low. Taken together, these findings suggest that pre-service teachers' ISK may vary across contextual, institutional, and sample-related factors.

In addition, the present study found that pre-service teachers' ISAs were at a high level. This finding is largely consistent with previous studies. Avcı and Oruç (2020) found that undergraduate students exhibited high levels of ISA, and Hakkari (2022) reported similar findings among associate degree students. Similarly, Göldağ (2021) concluded that associate and undergraduate students had high levels of digital data security awareness. Nevertheless, the literature is not entirely consistent, with some studies reporting moderate or even low levels of ISA. Benzer & Karal (2023) and Erdoğmuş (2017) reported moderate levels of ISA among university students, while Sağır et al. (2018) found similar results among vocational school students. Likewise, Gültekin and Özel (2023) determined that associate, undergraduate, and graduate students demonstrated moderate levels of ISA. In contrast, Wang (2022) showed that university students had only basic-level ISA, while Ndiege and Okella (2018) concluded that university students' ISA was insufficient.

Overall, these findings suggest that university students' ISA levels vary across different contexts and samples and that there remains a clear need for further improvement. As emphasized by Avcı and Oruç (2020), integrating information security–related courses into academic curricula may be an effective strategy for enhancing users' awareness. In addition, educational interventions should include explicit instruction on information security threats to better inform users and promote safer behaviors in digital environments (Şahinaslan et al., 2009). In this regard, it can be argued that organizing targeted training programs to increase users' information security knowledge and awareness is essential, particularly given users' active role in ensuring information security.

The findings of the present study revealed a significant and positive relationship between pre-service teachers' ISK and ISA. In other words, greater ISK is associated with higher ISA. This finding is consistent with previous research. Benzer and Karal (2023) reported a significant relationship between university students' ISK and their attitudes toward information security. Similarly, the same study found a significant positive relationship between ISK and information security behaviors.

According to the results of the canonical correlation analysis, a moderate positive canonical relationship was identified between pre-service teachers' ISA and ISK. To examine the relationship between these two constructs, a canonical correlation analysis was conducted, and the first canonical function was found to be statistically significant at $p < .001$. The first canonical function yielded a canonical correlation of .43, indicating that the ISA and ISK variable sets shared 18.7% of their variance.

Further examination of the relationship between the two datasets showed that ISA explained 16.2% of the variance in ISK. In contrast, ISK explained 5.5% of the variance in ISA. These findings suggest that the linear combinations of the variables in the two datasets are meaningfully related. Accordingly, it can be argued that as pre-service teachers' ISA increases, their ISK is likely to increase as well.

## Limitations and Recommendations for Future Research

Although the present study provides insights into pre-service teachers' information security knowledge and awareness, it has several limitations that should be acknowledged. First, the data were collected solely through self-report questionnaires, and it was assumed that participants responded voluntarily and honestly. Therefore, the findings may be subject to potential response bias. Additionally, there is a gender imbalance among participants, with females accounting for more than 73% of the sample. This may limit the generalizability of the findings.

Another limitation is that the study sample consisted only of pre-service teachers enrolled in the Elementary Mathematics Education and Early Childhood Education programs at a single public university. This may also limit the generalizability of the findings. Future studies may address this limitation by including pre-service teachers from different academic departments and comparing results across disciplines. Similarly, conducting studies with samples drawn from multiple universities may enhance the generalizability of the findings.

Future research may also incorporate additional variables related to information security knowledge and awareness in order to examine more complex relationships among variables. Moreover, intervention-based studies implementing information security training programs for pre-service teachers may be conducted to enhance their information security knowledge, awareness, and related behaviors. The effects of such educational interventions could then be examined and compared with findings reported in the existing literature.

In addition, qualitative studies may be conducted to provide in-depth insights into pre-service teachers' perceptions and experiences regarding information security. Mixed-methods research designs may also be employed to explore cause better–and–effect relationships and to provide a more comprehensive understanding of information security knowledge and awareness in educational contexts. Such approaches strengthen the validity and reliability of research findings by supporting participants' perspectives with quantitative data.

## Declarations

**Ethics statement:** This study was approved by the Ethics Committee of Burdur Mehmet Akif Ersoy University. The ethics approval was granted on October 5, 2022 under the protocol number GO 2022/891. All procedures involving human participants were conducted in accordance with institutional and national ethical standards, the Helsinki Declaration, and applicable regulations. Informed consent was obtained from all participants.

**Author Contributions (CRediT):** N. Sevim Cirak: Methodology, Writing- Original Draft Preparation. A. Gökçe Ulutaş: Data Curation, Writing- Original Draft Preparation. V. G. Başer Gülsoy: Writing- Original Draft Preparation, Reviewing and Editing

**Funding:** This research received no specific grant from any funding agency.

**Conflict of Interest:** The authors declare no conflict of interest.

**AI Tools Disclosure:** During the preparation of this work the author(s) used ChatGPT for the purpose of language editing. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

**Data Availability Statement:** Data are available from the corresponding author upon reasonable request.

## References


Avcı, Ü., & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi [Investigation of the students' personal cyber security behavior and information security awareness]. *İnönü Üniversitesi Eğitim Fakültesi Dergisi, 21*(1), 284–303. https://doi.org/10.17679/inuefd.526390

Baykara, M., Daş, R., & Karadoğan, İ. (2013, May 20-21). *Examination of the tools used in information security systems* [Conference presentation]. 1st International Symposium on Digital Forensics and Security. Elazığ. Turkiye.

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. https://doi.org/10.5152/AUJKKEF.2023.1034562

Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği [Computer and internet security for children and teenagers]. *Gazi Üniversitesi Politeknik Dergisi, 10*(1), 33–39.

Clark, R. (2007). Convenience sample. *The Blackwell encyclopedia of sociology*, 1–2. https://doi.org/10.1002/9781405165518.wbeosc131.pub2

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması [Development of information security awareness scale (ISAS) for teachers]. *Millî Eğitim Dergisi*, 216, 33–52.

Çetinkaya, L., & Öktelik, B. (2022). Ortaokul düzeyi öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme çalışması [Development of an information security awareness scale for secondary school learners]. *Cumhuriyet International Journal of Education, 11*(4), 696–708. https://doi.org/10.30703/cije.1131545

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri [Information security; what is and what is not, information security problems in Turkey and some related solutions]. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1–15.

Erdoğmuş, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımlarının farkındalıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği [An analysis of the effects of university students' information security knowledge on their levels of awareness: Afyon Kocatepe University sample]* [Unpublished master's thesis]. Afyon Kocatepe University.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Fraenkel, J. R., Wallen, N. E., & Hyun, H. (2011). *How to design and evaluate research in education* (8th ed.). McGraw-Hill.

Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi [Examining the information security awareness of secondary school students]. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi, 18*(1), 354–373. https://doi.org/10.33711/yyuefd.867015

Göldağ, B. (2021). Investigation of the relationship between digital literacy levels and digital data security awareness levels of university students. *E-International Journal of Educational Research, 12*(3), 82–100. https://doi.org/10.19160/e-ijer.950635

Güldüren, C., Keser, H., & Erçağ, E. (2020). Ortaöğretim kurumlarındaki öğrencilerin bilgi güvenliği farkındalık düzeylerinin incelenmesi [Investigation of information security awareness levels of students in secondary schools]. *International Social Sciences Studies Journal, 6*(60), 1516–1527. https://doi.org/10.26449/sssj.2268

Gültekin, V., & Özel, N. (2023). Üniversite öğrencilerinin bilgi güvenliği farkındalığı: Ankara Üniversitesi örneği [Information security awareness of university students: Example of Ankara University]. *Bilgi Yönetimi, 6*(2), 310–331. https://doi.org/10.33721/by.1366855

Hakkari, F. (2022). Ön lisans öğrencilerinin bilgi güvenliği kazanımı ve farkındalık düzeylerinin belirlenmesi: Kırıkhan Meslek Yüksekokulu örneği [Determination of information security acquisition and awareness levels of associate degree students: Kırıkhan Vocational School sample]. *Bilgi ve İletişim Teknolojileri Dergisi, 4*(1), 66–86. https://doi.org/10.53694/bited.1121085

Karaoğlan-Yılmaz, F. G., & Çavuş-Ezin, Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi [The study of parents' awareness of information security]. *Eğitim Teknolojisi Kuram ve Uygulama Dergisi, 7*(2), 41–57. https://doi.org/10.17943/etku.288874

Kılıç, R. (2022). Öğrenme, öğretme ve değerlendirme süreçlerinin dijitalleştirilmesi [Digitalization of learning, teaching, and assessment processes]. In Çavuşoğlu, B., & Küçük, S. (Eds.), *Dijital üniversite dönüşümünün yol haritası [Digital university transformation roadmap]* (pp. 57-79). Atatürk Üniversitesi Yayınları.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316–327. https://doi.org/10.1108/09685221011095236

Lugnet, J., Ericson, A., Lundgren, M., & Wenngren, J. (2020, August). *On the design of playful training material for information security awareness* [Conference presentation]. Proceedings of the International Conference on Design Creativity, Oulu, Finland.

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. https://doi.org/10.1016/j.chb.2016.11.065

Ndiege, J. R., & Okello, G. O. (2018). Information security awareness amongst students. *The African Journal of Information Systems, 10*(3), 204-221.

O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity, 41*(5), 673–690.

Öğütçü, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Pearson, E. S., & Hartley, H. O. (1958). *Biometrika tables for statisticians.* Cambridge University Press.

Pontoan, M., Sihotang, J., & Lompoliu, E. (2023). Information security analysis of online education management systems using information technology infrastructure library version 3. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 22*(2), 207–216. https://doi.org/10.30812/matrik.v22i2.2474

Puhakainen, P. (2006). *A design theory for information security awareness* [Academic dissertation]. University of Oulu, Faculty of Science, Department of Information Processing Science, Finland. http://jultika.oulu.fi/Record/isbn951-42-8114-4

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Sağır, M., Doğruluk, S., Mutluay, Y., & Emlik, H. (2018). Meslek yüksekokulu öğrencilerinin bilgi güvenliği farkındalık düzeylerinin incelenmesi [An analysis of the vocational college students' awareness levels regarding information security]. *Akademik Sosyal Araştırmalar Dergisi, 6*(74), 566–582. https://doi.org/10.16992/ASOS.13954

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, Article 102756. https://doi.org/10.1016/j.cose.2022.102756

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

Stevens, J. P. (2009). *Applied multivariate statistics for the social sciences.* Routledge.

Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009, February 11-13). *Bilgi güvenliği farkındalık eğitimi örneği [An example of information security awareness training]* [Conference presentation]. XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa, Türkiye.

Tabachnick, B. C., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Pearson.

Thompson, B. (2005). Canonical correlation analysis. In B. Everitt & D. Howell (Eds.), *Encyclopedia of statistics in behavioral science* (pp. 192-196). Wiley.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 10*, 7–11.

Turkish Statistical Institute (TSI). (2024). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2024 [Household Information Technology (IT) Usage Survey]*. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2024-53492

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2011). *Siber güvenliğin sağlanması: Türkiye'de mevcut durum ve alınması gereken tedbirler [Ensuring cybersecurity: Current situation in Turkey and measures to be taken]*. Bilgi Teknolojileri ve İletişim Kurumu.

von Solms, R. V., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, X. (2022). Exploring Chinese college students' awareness of information security in the COVID-19 era. *European Journal of Education (EJED), 5*(2), 20–34.

Weippl, E. R., & Ebner, M. (2008, November 17-21). *Security privacy challenges in e-learning 2.0* [Conference presentation]. E-Learn Conference, Las Vegas, United States.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security* (3rd ed.). Thomson Course Technology.