Educational Research & Implementation

PEGEM AKADEMİ

ISSN: 3023-6568 (Print) 3023-6576 (Online) Journal webpage: https://www.edure.net

Check for updates

Title:

Investigation of pre-service teachers' digital data security awareness in terms of various variables

Author(s):

Mehmet Emre Sezgin, Sevda Uğuz

To cite this article:

Sezgin, M. E. & Uğuz, S. (2025). Investigation of pre-service teachers' digital data security awareness in terms of various variables. *Educational Research & Implementation, 2*(2), 99-106. https://doi.org/10.14527/edure.2025.08

Educational Research & Implementation, 2(2), 2025, 99-106

www.edure.net/

Investigation of pre-service teachers' digital data security awareness in terms of various variables

Mehmet Emre Sezgin [*a], **Sevda Uğuz** [b]

Article Information

DOI: 10.14527/edure.2025.08

Article History:
Received 16 June 2025
Revised 14 July 2025
Accepted 03 September 2025
Online 26 September 2025

Keywords:
Digital data security,
Awareness,
Pre-service teachers,
Information security.

Article Type:
Research paper

Abstract

This study examined pre-service teachers' digital data security awareness and investigated whether this awareness differed according to gender, grade level, and academic department. Employing a descriptive survey design, data were collected from pre-service teachers enrolled in various teacher education programs at a public university. Participants completed an online questionnaire based on a validated digital data security awareness scale. Descriptive statistical analyses were conducted to determine overall awareness levels, while inferential statistical analyses were used to examine differences across the selected variables. The findings revealed that pre-service teachers demonstrated an awareness level above the moderate range, indicating a generally adequate sensitivity to the protection of digital information in educational contexts. No statistically significant differences were found in awareness levels based on gender, suggesting comparable digital data security awareness among male and female participants. However, awareness levels differed significantly by grade level, with senior students exhibiting higher awareness than first-year students, pointing to a developmental progression throughout undergraduate education. In addition, significant differences were observed across academic departments, with candidates from technology-oriented programs showing higher awareness levels than those from other disciplines. These results suggest that increased exposure to digital learning environments, as well as curricular engagement with technology- and security-related content, contributes positively to the development of digital data security awareness. Accordingly, the study underscores the importance of integrating digital data security, privacy, and information ethics as systematic and compulsory components of teacher education curricula across all programs, in order to equip future teachers with the competencies necessary to protect student data and foster secure digital learning environments.

Introduction

Rapid and continuous developments in information technologies have led to significant transformations in education, economy, and social life by facilitating access to information. While the transfer of educational processes to digital environments has made teaching and learning activities more flexible and accessible, it has also introduced new risks related to the protection of personal and institutional data. Today, data are considered not merely as technical records but as strategic assets that constitute the digital identities of individuals and institutions. Consequently, digital data security has become one of the most critical issues of contemporary information societies (Gökmen & Akgün, 2015). In recent years, this issue has gained further importance due to the rapid expansion of digital education practices following the COVID-19 pandemic, which significantly increased the volume and sensitivity of educational data processed in online environments (Miao & Holmes, 2023; OECD, 2022).

In the information security literature, the fundamental theoretical framework for protecting digital data is based on the principles of confidentiality, integrity, and availability. These principles, commonly referred to as the "CIA triad," represent the protection of information from unauthorized access, the preservation of its accuracy and completeness, and its accessibility to authorized users when needed (McCumber, 2004). A violation of any of these

* **Corresponding author e-mail:** esezgin@cu.edu.tr
[a] Faculty of Education, Çukurova University, Adana, Türkiye
[b] Çukurova Science and Art Center, Adana, Türkiye

components may weaken information security and lead to serious material and moral consequences. Therefore, ensuring security in digital environments requires not only robust technical infrastructures but also a high level of awareness among users regarding these principles (Keser & Güldüren, 2015). Recent studies emphasize that the CIA triad remains conceptually valid; however, its application in educational contexts has become more complex due to cloud-based systems, learning analytics, and large-scale data sharing practices (Jones et al., 2025).

The literature consistently emphasizes that a significant proportion of information security breaches result from human-related factors rather than technical deficiencies. Siponen (2000) defines information security awareness as individuals' ability to recognize information security risks, understand the potential consequences of these risks, and develop secure behaviors accordingly. From this perspective, even the most advanced security systems may become ineffective if users lack sufficient awareness. Similarly, Safa et al. (2016) argue that information security has not only a technical dimension but also a behavioral one, highlighting the critical role of the human factor in cybersecurity (Mart, 2012). More recent research supports this view by demonstrating that emerging threats such as AI-driven social engineering, phishing attacks, and misuse of personal data disproportionately exploit human vulnerabilities rather than system-level weaknesses (ENISA, 2023; Hadlington, 2017).

Educational institutions are environments in which personal and sensitive data belonging to students and teachers are intensively processed, stored, and shared, making information security particularly significant. Teachers and pre-service teachers are responsible not only for protecting their own digital data but also for safeguarding students' personal information (Kaşıkçı et al., 2014). However, teacher education programs often address digital data security indirectly, with a primary focus on technology use and digital content production. Recent international policy documents and studies highlight that this indirect approach is insufficient and call for the explicit integration of data privacy, cybersecurity, and digital ethics into teacher education curricula (European Commission, 2022; OECD, 2024). Nevertheless, teachers' ability to act ethically, securely, and consciously in digital environments and to guide their students accordingly constitutes a professional necessity.

A review of the national literature reveals various studies examining information and digital security awareness. Research conducted with pre-service teachers and university students indicates that digital security awareness may differ significantly depending on demographic variables (Karayücel Efe, 2019; Gündüzalp, 2021). However, the continuous evolution of technological threats and the increasing integration of digital tools into educational settings necessitate the re-examination of this awareness using up-to-date data. Given the rapid changes in digital education practices after 2020, findings based on pre-pandemic data may no longer fully reflect current awareness levels and risk perceptions.

The widespread adoption of distance education during the COVID-19 pandemic has further intensified pre-service teachers' use of digital platforms, making their awareness of digital data security even more critical. As future educators, pre-service teachers are expected to internalize digital data security not merely as a technical competence but as an ethical and professional responsibility. In this context, identifying pre-service teachers' levels of digital data security awareness and examining these levels in relation to various variables are considered essential steps toward improving teacher education programs and fostering a safer educational ecosystem. Accordingly, the present study contributes to the literature by providing updated empirical evidence on pre-service teachers' digital data security awareness in a post-pandemic educational context.

Method

Research Design

The study employed a descriptive survey research design, which is a type of research conducted with relatively large samples and aims to identify participants' opinions or characteristics such as interests, skills, abilities, and attitudes related to a particular topic or phenomenon (Cohen, Manion, & Morrison, 2018; Fraenkel, Wallen, & Hyun, 2012).

Participants

The sample of the study consists of students enrolled in the 1st, 2nd, 3rd, and 4th years of various departments of the Faculty of Education at Çukurova University. The participants were selected through purposive sampling (Cohen, Manion, & Morrison, 2018; Fraenkel, Wallen, & Hyun, 2012; Sönmez & Alacapınar, 2014).

Purposive sampling was employed based on specific inclusion criteria aligned with the aim of the study. Participants were required to a) be actively enrolled in a teacher education program, b) regularly use digital platforms such as learning management systems and online communication tools as part of their coursework, and c) engage in digital data processing activities related to educational practices (e.g., accessing student information systems, submitting assignments online, or using digital instructional materials). These criteria ensured that the selected participants constituted an information-rich group with direct and relevant experience in digital learning environments, making them suitable for examining digital data security awareness within the context of teacher education.

Data Collection Materials

In this study, the Digital Data Security Awareness Scale developed by Yılmaz et al. (2015) was used as the data collection instrument. The scale is a five-point Likert-type instrument consisting of 32 items grouped under a single factor and demonstrates a high level of internal consistency ($\alpha = .945$) with an explained variance of 36.1%.

Data Collection Procedure

The scale was administered online to first-, second-, third-, and fourth-year students enrolled in the Departments of German Language Teaching, Computer Education and Instructional Technologies, Philosophy Teaching, Science Teaching, French Language Teaching, English Language Teaching, Mathematics Teaching, Preschool Education, Guidance and Psychological Counseling, Art Education, Primary School Teaching, Social Studies Teaching, and Turkish Language Teaching at the Faculty of Education of Çukurova University. Data were collected on a voluntary basis during the 2023-2024 Fall, following ethical approval. The survey link was shared with the students by the course instructors of the relevant departments via Microsoft Teams, which is used for online courses at the university. Participants completed the scale anonymously and were informed that their responses would be used solely for scientific research purposes.

Data Analysis

The data obtained from the study were analyzed using the Statistical Package for the Social Sciences (SPSS). Prior to the analyses, the dataset was examined for missing values, outliers, and assumptions of normality. Descriptive statistics, including frequency, percentage, mean, and standard deviation values, were calculated to determine the digital data security awareness levels of the participants.

To examine whether digital data security awareness levels differed significantly according to gender, an independent samples t-test was conducted. Differences based on grade level and department were analyzed using one-way analysis of variance (ANOVA). When statistically significant differences were detected, post hoc tests were performed to identify the source of the differences. The significance level was set at $p < .05$ for all statistical analyses.

In addition to significance values, effect sizes were calculated to determine the practical significance of the findings. Cohen's d was reported for t-test results, and eta squared (η^2) was reported for ANOVA results, following conventional interpretation guidelines.

Results

The first finding of the study revealed that the overall digital data security awareness level of pre-service teachers was above the moderate level. The mean digital data security awareness score of the participants was 3.87 (SD = 0.56) on a five-point Likert scale. Of the participants, 62.6% (n = 214) were female and 37.4% (n = 128) were male. In terms of grade level, 24.6% (n = 84) were first-year students, 23.1% (n = 79) were second-year students, 26.6% (n = 91) were third-year students, and 25.7% (n = 88) were fourth-year students. The descriptive statistics related to the demographic characteristics of the participants are presented in Table 1. As shown in Table 1, the participants were relatively evenly distributed across grade levels, while female students constituted a higher proportion of the sample.

Table 1.
Descriptive Statistics of the Participants.

Variable	Category	N	%
Gender	Female	214	62.60
	Male	128	37.40
Total		342	100.00
Grade Level	1st Year	84	24.60
	2nd Year	79	23.10
	3rd Year	91	26.60
	4th Year	88	25.70
Total		342	100.00

Differences in Digital Data Security Awareness by Gender

An independent samples t-test was conducted to examine whether pre-service teachers' digital data security awareness levels differed significantly according to gender. The results indicated that there was no statistically significant difference between female and male participants in terms of their digital data security awareness scores ($p > .05$). Descriptive statistics and t-test results are presented in Table 2.

Table 2.
Independent Samples t-test Results for Digital Data Security Awareness by Gender.

Grade Level	N	$\overline{X}$	SD
1st Year	84	3.71	.59
2nd Year	79	3.80	.54
3rd Year	91	3.92	.53
4th Year	88	4.03	.50

To identify the source of the significant difference, a post hoc Tukey test was conducted. The results indicated that fourth-year students had significantly higher digital data security awareness scores compared to first-year students ($p < .05$). No other significant pairwise differences were found.

These findings demonstrate that digital data security awareness tends to increase as pre-service teachers progress through their undergraduate education.

Differences in Digital Data Security Awareness by Department

A one-way ANOVA was also conducted to examine whether digital data security awareness levels differed according to department. The results showed a statistically significant difference among departments ($F(12, 329) = 3.18$, $p < .05$). To identify the source of the significant difference, a post hoc Tukey test was conducted. The results and mean scores indicated that students enrolled in the Computer Education and Instructional Technologies department had higher digital data security awareness levels compared to students from other departments ($\eta^2=.01$).

Table 4.
ANOVA Results for Digital Data Security Awareness by Department.

Source of Variance	SS	df	MS	F	p
Between Groups	8.94	12	.74	3.18	.001
Within Groups	76.58	329	.23		
Total	85.52	341			

Discussion

The present study aimed to investigate pre-service teachers' digital data security awareness levels and to examine whether these levels differed according to gender, grade level, and department. The findings revealed that the overall digital data security awareness level of the participants was above the moderate level. This result indicates that pre-service teachers possess a generally adequate level of awareness regarding the protection of digital data, which is encouraging considering their future roles as educators responsible for managing both their own and their students' digital information. However, an above-moderate awareness level should not be interpreted as sufficient preparation for the complex and evolving cybersecurity challenges faced in contemporary educational environments, particularly in light of rapidly advancing technologies and increasingly sophisticated cyber threats.

The finding that pre-service teachers' digital data security awareness was above the moderate level is consistent with previous studies conducted with university students and pre-service teachers. Similar research has reported moderate to high levels of digital or information security awareness among pre-service teachers (Cavus & Ercag, 2014; Gündüzalp, 2021; Karayücel Efe, 2019). This consistency may be attributed to the increasing integration of digital technologies into daily life and educational practices, which has made individuals more conscious of issues related to data protection, privacy, and cybersecurity risks. Nevertheless, recent literature suggests that heightened exposure to digital technologies does not always translate into deep or behaviorally consistent security awareness, as users may overestimate their competence while remaining vulnerable to emerging threats such as AI-driven social engineering deepfake-based manipulation, and adaptive phishing attacks that exploit human trust rather than technical vulnerabilities.

Contrary to some expectations, the results of the independent samples t-test indicated that digital data security awareness did not differ significantly according to gender. This finding aligns with several studies reporting no significant gender-based differences in information security or digital awareness (Yılmaz et al., 2015; Safa et al., 2016). One possible explanation is that access to digital technologies and exposure to online environments have become largely similar for male and female students, reducing traditional gender gaps in technology-related competencies and awareness. Alternatively, this result may suggest that gender alone is no longer a meaningful explanatory variable in digital security research, and that factors such as training quality, institutional policies, and regulatory awareness experience, and curricular exposure may play a more decisive role.

On the other hand, the study revealed a significant difference in digital data security awareness according to grade level. The post hoc analysis showed that fourth-year students had significantly higher awareness levels than first-year students. This finding suggests that digital data security awareness tends to develop progressively throughout undergraduate education. As students advance in their academic programs, they are more likely to encounter digital platforms, online learning environments, academic information systems, and data-related responsibilities, which may contribute to increased awareness. This result is supported by previous studies indicating that experience and prolonged exposure to digital technologies positively affect information security awareness (Gündüzalp, 2021; Siponen, 2000). However, this developmental increase may not occur automatically; rather, it may be indirectly fostered through repeated exposure to digital systems rather than through explicit instruction. This is particularly critical given that recent data protection regulations increasingly require educators to actively manage, process, and safeguard personal data in compliance with legal standards.

In addition, the results demonstrated a significant difference in digital data security awareness across departments. Pre-service teachers enrolled in the Computer Education and Instructional Technologies department exhibited higher awareness levels compared to students from other departments. While this finding is consistent with previous research (Safa et al., 2016; Yılmaz et al., 2015), it also highlights a structural imbalance within teacher education curricula, as digital data security topics are more explicitly addressed in technology-oriented programs. Rather than reflecting differences in students' abilities or motivation, these departmental differences may be explained by unequal curricular exposure to digital data security concepts and practices.

The findings of the present study highlight the importance of integrating digital data security topics more explicitly into teacher education curricula. Although overall awareness levels were above moderate, the observed differences based on grade level and department suggest that digital data security awareness is not uniformly developed among all pre-service teachers. From a policy and curriculum design perspective, this indicates a need for a standardized and compulsory approach to digital data security education across all teacher training programs, rather than limiting such content to technology-oriented departments or advanced years of study. Such training should also address

contemporary issues such as AI-based cyber threats, data privacy regulations, and ethical decision-making in digital educational environments.

In conclusion, this study underscores the need to view digital data security not merely as a technical issue but as a fundamental professional competence for teachers. As digital learning environments become increasingly complex and data-driven, teachers must be equipped not only with awareness but also with critical judgment and ethical responsibility regarding data protection.

Conclusion

This study demonstrated that pre-service teachers' digital data security awareness is generally above a moderate level, indicating an adequate sensitivity to the protection of digital information within teacher education contexts. While awareness levels did not differ significantly by gender, notable differences were observed across grade levels and academic departments. Specifically, awareness increased across undergraduate years, with fourth-year students exhibiting significantly higher levels than first-year students, suggesting a cumulative developmental effect of academic experience. Moreover, departmental differences indicated that candidates enrolled in Computer Education and Instructional Technologies programs attained the highest awareness levels, highlighting the influence of program-specific exposure to technology-oriented coursework. Taken together, these findings suggest that digital data security awareness is not uniformly cultivated across teacher education programs but is shaped by both cumulative academic progression and curricular emphasis. Accordingly, the results underscore the need for teacher education curricula to integrate digital data security, privacy, and information ethics in a more explicit, systematic, and comprehensive manner across all departments and year levels. Such integration is essential to ensure that all prospective teachers graduate with the competencies required to safeguard student data and to maintain secure and ethically responsible digital learning environments.

Limitations

This study has several limitations that should be taken into consideration when interpreting the findings. First, the research employed a descriptive survey design, which is non-experimental in nature. Therefore, although the results reveal relationships between digital data security awareness and certain demographic variables, causal inferences cannot be made.

Second, the sample of the study was limited to pre-service teachers enrolled in the Faculty of Education at Çukurova University. Although participants from different departments and grade levels were included, the findings may not be fully generalizable to all pre-service teachers in Türkiye or to students from other faculties and universities. Future studies conducted with larger samples from different geographical regions and institutional contexts may enhance the generalizability of the results.

Third, data were collected using a self-report measurement tool. While the Digital Data Security Awareness Scale demonstrated high internal consistency, self-report instruments may be subject to social desirability bias and may not fully reflect participants' actual behaviors in digital environments. Complementary qualitative methods such as interviews or observations could provide deeper insights into pre-service teachers' digital data security practices.

Finally, the study focused solely on demographic variables such as gender, grade level, and department. Other potentially influential factors such as prior training in information security, frequency of technology use, or personal experiences with digital security incidents were not examined. Future research incorporating these variables may contribute to a more comprehensive understanding of digital data security awareness among pre-service teachers.

Suggestion

Based on the findings of the present study, several concrete and stage-based curricular recommendations can be proposed for teacher education programs. Given that first-year pre-service teachers demonstrated significantly lower digital data security awareness compared to fourth-year students, it is essential to introduce digital data security training early and systematically within undergraduate teacher education.

In the first year, introductory courses on educational technologies should explicitly include fundamental concepts of digital data security, such as personal data protection, password management, safe use of online platforms, and awareness of common cyber threats. At this stage, the primary aim should be to establish basic awareness and ethical sensitivity regarding digital data use in educational contexts.

In the second year, digital data security topics can be integrated into courses related to instructional technologies and digital literacy. Practical activities, such as analyzing real-life security breaches in educational settings or identifying risks in commonly used educational platforms, may help students translate theoretical knowledge into practice.

In the third year, more advanced and applied content should be introduced. This stage may focus on institutional data security, legal responsibilities of teachers, and compliance with data protection regulations in education. Case-based learning and scenario-based discussions can be used to develop pre-service teachers' critical judgment and decision-making skills when confronted with data security dilemmas.

In the fourth year, digital data security training should be reinforced through teaching practice and internship courses. Pre-service teachers can be encouraged to reflect on data security practices observed in schools, evaluate potential risks, and develop strategies for protecting student data in real classroom environments. This stage should emphasize professional responsibility and the role of teachers as models of ethical and secure digital behavior.

Overall, integrating digital data security education as a compulsory and continuous component across all four years of teacher education programs may contribute to more balanced and sustainable awareness development among pre-service teachers. Such a structured approach would help ensure that all future teachers, regardless of their department, graduate with the necessary competencies to manage digital data securely and responsibly.

Ethical Considerations

This study was conducted in accordance with ethical research principles involving human participants. Ethical approval was obtained from the Çukurova University Ethics Committee prior to data collection (Approval No: 312643). Participation in the study was entirely voluntary, and informed consent was obtained from all participants. The participants were informed about the purpose of the study, the confidentiality of their responses, and their right to withdraw at any time without any negative consequences.

Consent for Publication

All participants were informed about the purpose of the study and their voluntary participation was obtained prior to data collection. Participants completed the questionnaire anonymously through an online platform, and no personally identifiable information was collected. By voluntarily completing the survey, participants provided their informed consent for the use of the data for scientific research and publication purposes.

Funding Statement

The authors received no financial support for the research, authorship, and/or publication of this article. This study was carried out without any funding from public, commercial, or non-profit organizations.

Declaration of Conflicting Interests

The authors declare that there are no conflicts of interest regarding the research, authorship, and publication of this article. The study was conducted independently without any personal, institutional, or financial relationships that could inappropriately influence the work reported in this paper.

Authors' Contributions

All authors contributed substantially to the conception and design of the study. Data collection and analysis were carried out collaboratively. The first author conducted the statistical analyses and drafted the methodology and results sections. The second author contributed to the theoretical framework, discussion, and interpretation of the findings. Both authors reviewed, revised, and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

References

Cavus, N., & Ercag, E. (2014). 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. https://doi.org/10.1111/bjet.12217

Cohen, L., Manion, L., & Morrison, K. (2018). *Research methods in education* (8th ed.). Routledge.

ENISA. (2023). *Threat landscape 2023*. European Union Agency for Cybersecurity.

European Commission. (2022). *Digital education action plan 2021–2027: Resetting education and training for the digital age.* Publications Office of the European Union.

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012*). How to design and evaluate research in education* (8th ed.). McGraw-Hill.

Gökmen, Ö. F., & Akgün, Ö. E. (2015). *Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi*. *İlköğretim Online, 14*(4), 1208–1221. https://doi.org/10.17051/io.2015.04635

Gündüzalp, C. (2021). *Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları.* Journal of Computer and Education Research, 9(18), 598–625. https://doi.org/10.18009/jcer.907022

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Jones, N., Whaiduzzaman, M., Jan, T., Adel, A., Alazab, A., & Alkreisat, A. (2025). A CIA triad-based taxonomy of prompt attacks on large language models. *Future Internet*, *17*(3), 113. https://doi.org/10.3390/fi17030113

Karayücel Efe, N. (2019). *Öğretmen adaylarının bilgi güvenliği farkındalığının incelenmesi* (Unpublished master's thesis). Ondokuz Mayıs University.

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim*, 39(171), 230–243.

Keser, H., & Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167–1184.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı* (Unpublished master's thesis). Kahramanmaraş Sütçü İmam University.

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*. Auerbach Publications.

Miao, F., & Holmes, W. (2023). *Guidance for generative AI in education and research*. Unesco Publishing.

OECD. (2022). *Education at a glance 2022: OECD indicators*. OECD Publishing. https://doi.org/10.1787/3197152b-en

OECD. (2024). *Shaping digital education: Enabling teachers and learners for the future*. OECD Publishing. https://doi.org/10.1787/bac4dc9f-en

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Sönmez, V., & Alacapınar, F. G. (2014). *Örneklendirilmiş bilimsel araştırma yöntemleri*. Anı Yayıncılık.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2015). Dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi. *AJIT-e: Bilişim Teknolojileri Online Dergisi, 6*(21), 23–40. https://doi.org/10.5824/1309-1581.2015.4.002.x

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