**BRAIN. Broad Research in Artificial Intelligence and Neuroscience**
e-ISSN: 2067-3957 | p-ISSN: 2068-0473
Covered in: Web of Science (ESCI); EBSCO; JERIH PLUS (hkdir.no); IndexCopernicus; Google Scholar; SHERPA/RoMEO; ArticleReach Direct; WorldCat; CrossRef; Peeref; Bridge of Knowledge (mostwiedzy.pl); abcdindex.com; Editage; Ingenta Connect Publication; OALib; scite.ai; Scholar9; Scientific and Technical Information Portal; FID Move; ADVANCED SCIENCES INDEX (European Science Evaluation Centre, neredataltics.org); ivySCI; exaly.com; Journal Selector Tool (letpub.com); Citefactor.org; fatcat!; ZDB catalogue; Catalogue SUDOC (abes.fr); OpenAlex; Wikidata; The ISSN Portal; Socolar; KVK-Volltitel (kit.edu)
2026, Volume 17, Special Issue 1, pages: 73-85
*Submitted:* February 27th, 2026 | *Accepted for publication:* June 7th, 2026

# Assessment of Information Security and Privacy Awareness in the Age of Artificial Intelligence

**Gökmen Dagli**
Faculty of Education, University of Kyrenia, Kyrenia, Cyprus. gokmen.dagli@kyrenia.edu.tr,
https://orcid.org/0000-0002-4416-8310

**Ogunturk Yilmaz**
Military Training and Informatics Center, Turkiye.
oguntrkylmz@icloud.com,
https://orcid.org/0009-0009-7321-2833

**Fahriye Altinay**
Societal Research and Development Center, Faculty of Education, Near East University, Nicosia, Cyprus.
fahriye.altinay@neu.edu.tr,
https://orcid.org/0000-0002-8452-5992

**Zehra Altinay**
Societal Research and Development Center, Faculty of Education, Near East University, Nicosia, Cyprus.
zehra.altinaygazi@neu.edu.tr,
https://orcid.org/0000-0002-6786-6787

**Abstract:** *This study examines information security and privacy awareness from the perspectives of university administrators and faculty members in the age of artificial intelligence, where the rapid adoption of AI-supported digital technologies has introduced new cybersecurity and privacy challenges for higher education institutions. The qualitative study group consisted of 15 university administrators and faculty members. Qualitative data were collected using a semi-structured interview protocol. With the widespread use of digital data systems, universities process and store personal data and research findings belonging to students, academic staff, and administrative staff over large networks. This has led to an increase in cyber threats and data breaches that have serious consequences for the reputation and legal responsibilities of institutions. The research results show that students generally have a high level of information security and privacy awareness, but they are unable to reflect this awareness in their daily digital behaviour. These findings are particularly important in the age of artificial intelligence, where the increasing use of AI-supported educational technologies requires stronger information security awareness and data protection practices in higher education institutions. Furthermore, it was determined that students lack sufficient knowledge about the institutional support structure they can turn to when facing cyber threats. In conclusion, it has been determined that regular training, seminars, the establishment of reporting mechanisms, and sustainable practices are necessary to improve information security and privacy awareness.*

**Keywords:** *information security; information security awareness; digital privacy; artificial intelligence; cyber threats.*

**How to cite:** Dagli, G., Yilmaz, O., Altinay, F., & Altinay, Z. (2026). Assessment of information security and privacy awareness status in the age of artificial intelligence. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 17*(Special Issue 1), 73-85. https://doi.org/10.70594/brain/17.S1/7

## 1. Introduction

Today, information and communication technologies offer opportunities in almost every aspect of life and greatly facilitate our daily lives. The internet holds a significant position among these technologies, which play a crucial role in the production, collection, sharing, and preservation of information. Through the internet, it has become possible to access information globally, share information, and achieve various goals (Avcı & Oruç, 2020). The introduction of the internet has made it possible to carry out many activities online. The development of digitalisation is causing a major transformation in work, communication, and meeting daily needs (Fallows, 2004).

The use of digital tools and the internet is rapidly increasing in areas such as education. The use of digital technologies for various purposes, from information access to commerce, from education to social interaction, further expands the scope of the internet. The internet is a global communication network. Through this network, many computer systems are connected to each other, making it highly beneficial for information access, communication, and other services (Tekerek & Mart, 2010). With the expansion of digital networks and the opportunities provided by the internet, the number of people using these technologies is constantly increasing. Today, the number of telephone subscribers has exceeded six billion. This number is expected to surpass 7.5 billion in 2027 (Ericsson, 2022). Both globally and in Türkiye, the number of individuals using digital technologies and the internet is rapidly increasing.

According to the research, 90% of women and 97% of men communicate via telephone (International Telecommunication Union, 2022).

Similarly, research conducted by the national statistical institute reported that in 2021, 92% of households in Türkiye had internet access. Research conducted by the Turkish Statistical Institute (TÜİK, 2022) indicated that internet use continued to increase, with 85.0% of individuals aged 16–74 using the internet. In addition, 96% of young people have internet access.

At the beginning of 2022, 68.9 million people in Türkiye were using social media. According to a study conducted between 13 January 2022 and 10 March 2022 among individuals aged 18–64, 81% regularly used social media (Statista, 2022). The average time spent online was 8 hours per day, with approximately 3.5 hours spent on a computer and about 3 hours spent on social media, 95.5% of internet access occurred via mobile phones, with 4 hours and 16 minutes spent on mobile devices, whereas time spent on computers and tablets was 3 hours and 44 minutes. 53.4% of daily internet usage time was spent on mobile devices (DataReportal, 2022). Globally, watching videos online, using email, and accessing social media are among the most common internet activities. Approximately half of the world's web traffic was generated through mobile devices (StatCounter, 2022).

Considering all these factors, digital technologies and the internet play a very important role in our daily lives. With the continued development of digital technologies and the widespread use of the internet, people are spending increasing amounts of time in cyberspace. This situation increases cybersecurity risks. Security concerns also increase with the use of digital devices such as smartphones, computers, and tablets (Talan & Aktürk, 2021).

While the security infrastructure of digital technologies is becoming more robust, people using these technologies remain the weakest link.

Individuals are the source of many information security breaches. Research shows that the human factor should be taken into consideration when reducing information security risks. Many studies have revealed that human behaviour or actions affect information security. Therefore, it is important for individuals to have information security awareness and understanding (Nezgitli &Gökçearslan, 2022).

In light of the above, the purpose of this study is to evaluate information security and privacy awareness from the perspectives of university administrators, faculty members, and students. With the acceleration of digitalisation processes, information security and protection of personal data have become an important necessity in higher education institutions. In this respect, the aim of the research is to evaluate students' information security and privacy awareness based on the opinions

of university administrators and faculty members and to provide recommendations reflecting the current situation. The rapid integration of artificial intelligence (AI) technologies into higher education has fundamentally transformed the ways universities collect, process, store, and manage digital information. While AI-supported educational systems provide significant opportunities for teaching, learning, and institutional management, they also introduce new challenges related to data privacy, cybersecurity, algorithmic transparency, and the protection of personal information. Consequently, strengthening information security and privacy awareness has become an essential requirement for ensuring the responsible and secure use of AI technologies in higher education institutions (UNESCO, 2023; OECD, 2023).

## 2. Method

### *2.1. Research Model*

This research used a qualitative research method to evaluate the information security and privacy awareness levels of university administrators, faculty members, and students (Büyüköztürk et al., 2020; Creswell & Guetterman, 2018). In the qualitative dimension of the research, a semi-structured interview technique was applied to university administrators and faculty members. In the qualitative dimension of the study, the interview data were analysed using thematic content analysis based on participants' views and experiences (Braun & Clarke, 2006; Creswell & Guetterman, 2018).

### *2.2. Study Group*

In the qualitative dimension of the research, the study group consisted of university administrators and faculty members working at the university. In the qualitative data collection process, participants were selected from among those who could share their views and experiences regarding information security and privacy issues in line with the purpose of the research. In this context, semi-structured interviews were conducted with 15 participants.Through these interviews, the participants' views on information security and privacy awareness were explored in depth. In qualitative research, the principle of data saturation is commonly used to determine the size of the study group. Data saturation refers to the point at which the data obtained during the research process begin to repeat themselves and no longer generate new information. Accordingly, the number of interviews was planned within a specific range, and data saturation was the primary consideration during the data collection process (Creswell & Guetterman, 2018; Yıldırım & Şimşek, 2021).

### *2.3. Data Collection Tools*

#### *2.3.1. Semi-Structured Interview Form*

A semi-structured interview form was used as a qualitative data collection tool in the research to explore the opinions, experiences, and evaluations of university administrators and faculty members regarding information security and privacy. This interview technique is defined as a data collection method based on questions prepared in advance by the researcher; however, additional questions may be asked when necessary to allow participants to explain their views in greater detail (Yıldırım & Şimşek, 2021; Polat, 2022).

Before the data collection process, the semi-structured interview guide and interview protocol were reviewed by experts in the fields of educational management and qualitative research to ensure their content validity, clarity, and relevance. Based on the experts feedback, minor revisions were made to improve the clarity, wording, and organisation of the interview questions.

During the preparation of the interview form, the purpose and sub-objectives of the research were taken into consideration, and open-ended questions were developed regarding information security policies, the protection of personal data, the level of institutional awareness, digital security

practices, security problems encountered, and proposed solutions. The interview questions were structured to allow participants to express their views in detail. The use of open-ended and clear questions in semi-structured interviews contributes to the collection of richer and more natural data from participants (Polat, 2022).

A total of 15 participants took part in semi-structured interviews. During the interviews, notes were taken with the participants' permission, and the data obtained were recorded for subsequent analysis. A content analysis approach was used to analyse the interview data. Content analysis is an analytical method that allows similar opinions to be grouped into specific themes and the data to be interpreted systematically (Yıldırım & Şimşek, 2021).

*2.3.2. Interview Protocol and Thematic Structure*

The semi-structured interview protocol was developed to obtain comprehensive and in-depth information regarding information security and privacy awareness in higher education institutions. During the development of the interview questions, the objectives of the study, the research questions, and the relevant literature on information security, digital privacy, and cybersecurity awareness were carefully considered. The interview guide was designed to provide sufficient flexibility for participants to express their experiences while ensuring consistency across all interviews (Creswell & Guetterman, 2018; Yıldırım & Şimşek, 2021).

To improve methodological transparency and facilitate systematic qualitative analysis, the interview questions were organised into thematic clusters. Each thematic cluster represented a specific dimension of the research and served as a guiding framework during both data collection and the subsequent content analysis process. The thematic structure of the interview protocol is presented in Table 1 (Braun & Clarke, 2021).

*Table 1. Interview Protocol and Thematic Structure*

| Thematic Cluster | Purpose | Representative Interview Question |
|---|---|---|
| **Digital Security and Privacy Awareness** | To explore participants' perceptions of students' awareness of wireless network security, online privacy, cookies, and website certificates. | *How do you evaluate students' knowledge of wireless network security, online privacy, cookies, and website certificates? Do you think their awareness is sufficient?* |
| **Cyber Threat Awareness** | To examine participants' observations regarding students' awareness of phishing, social engineering, spyware, and identity theft. | *How do you observe students' awareness of phishing, social engineering, spyware, and identity theft? Do you think this awareness is reflected in their daily behaviors?* |
| **Basic Information Security Practices** | To evaluate students' adoption of essential cybersecurity practices. | *To what extent do students adopt basic security practices such as screen locking, password management, secure USB usage, and protection of institutional data?* |
| **Cyberbullying and Support Mechanisms** | To investigate awareness of cyberbullying risks and institutional support services. | *How do you evaluate students' awareness of cyberbullying and cybersecurity risks? Do you think adequate support mechanisms are available at the university?* |
| **Institutional Awareness and Reporting Processes** | To examine participants' opinions regarding institutional guidance and reporting mechanisms. | *How do you evaluate students' knowledge of where and to whom they should report information security incidents?* |
| **Educational Needs and Recommendations** | To identify institutional priorities for improving information security awareness. | *In your opinion, which areas should universities prioritize to improve students' information security and privacy awareness?* |

The interview protocol was designed to ensure that each thematic cluster directly corresponded to the objectives of the study and the subsequent stages of qualitative analysis. During data analysis, participants' responses were initially coded according to these thematic clusters. Similar codes were subsequently grouped into subthemes and synthesised into broader themes that formed the basis of the qualitative findings presented in the Results section. This systematic procedure enhanced the transparency, consistency, and trustworthiness of the qualitative analysis (Braun & Clarke, 2006; Lincoln & Guba, 1985).

*2.3.3. Data Collection Process*

In the qualitative phase of the research, interviews were conducted to explore the opinions of university administrators and faculty members regarding information security and privacy. Ethical approval for this study was obtained from the Near East University Scientific Research Ethics Committee (Approval No. YDÜ/EB/2026/1267, 17 February 2026). The interviews were conducted face-to-face with the participants at times deemed appropriate, based on their voluntary participation. During the interview process, participants were informed about the purpose of the research, and it was stated that the participants' opinions would only be used for scientific purposes (Yıldırım & Şimşek, 2021). Ethical principles were followed throughout the data collection process, and participation was entirely voluntary. Participant confidentiality was protected, and the data obtained were analysed solely for the purposes of the study. Furthermore, the anonymity of the data obtained from the participants during the research process was protected, and care was taken not to share personal information with third parties (Creswell & Guetterman, 2018). The data obtained from the quantitative and qualitative data collection processes were organised, classified, and prepared for analysis in line with the research objectives.

**Data Analysis and Interpretation**

**Analysis of Qualitative Data**

The qualitative data obtained from the semi-structured interviews were analysed using thematic content analysis. The analysis was conducted through a systematic and sequential process to ensure methodological transparency, consistency, and trustworthiness (Braun & Clarke, 2006; Creswell & Guetterman, 2018).

Initially, all interview recordings were transcribed verbatim and reviewed several times to ensure familiarity with the data and the accuracy of the transcripts. During the first stage of analysis, meaningful statements related to the research objectives were identified and assigned initial codes. This open coding process enabled the systematic identification of recurring concepts and participant perspectives.

In the second stage, conceptually similar codes were grouped into subcategories based on their shared meanings and characteristics. These subcategories were subsequently examined and synthesised into broader themes reflecting the major dimensions of information security and privacy awareness. Throughout the analytical process, the thematic clusters established during the development of the interview protocol served as the primary analytical framework, ensuring consistency between the research questions, data collection, and qualitative findings.

Finally, the themes were interpreted in accordance with the objectives of the study, and the findings were reported by synthesising participants' shared perspectives within each thematic cluster. This systematic analytical procedure strengthened the transparency, dependability, and trustworthiness of the qualitative analysis (Lincoln & Guba, 1985; Braun & Clarke, 2021).

**3. Findings and Interpretations**

This section analyses the qualitative findings obtained from semi-structured interviews conducted with university administrators and faculty members. The data obtained were examined using content analysis; similar statements were coded and classified into common themes.

### *3.1. Findings Regarding Students' Awareness of Digital Security and Privacy*

Based on interviews conducted with university administrators and faculty members, participants indicated that students' awareness of information security issues, such as wireless network security, online privacy, cookies, and website certificates, is generally insufficient**.** The vast majority of participants stated that students have a basic level of knowledge; however, this knowledge is not sufficiently reflected in their daily digital behaviours.

In particular, participants reported limited awareness regarding the use of unsecured wireless networks, website security, HTTPS certificate verification, and the protection of personal data. Participants also stated that students frequently use free public Wi-Fi networks without paying adequate attention to digital security risks.

Participants stated that although students use digital technologies intensively, their safe usage habits are not sufficiently developed and that more awareness-raising activities are needed regarding information security. One participant stated that students have basic knowledge but lack technical details as follows:

**Participant (K5):** *"I think students have basic knowledge on the topics mentioned. However, there are shortcomings in technical details, and their awareness needs to be increased."*

Similarly, another participant stated that students' knowledge level remained at the theoretical level and was not sufficiently reflected in their daily usage behaviour:

**Participant (K9):** *"Awareness often remains at the theoretical level and is not sufficiently reflected in daily usage behaviour."*

The findings indicate that students' information security awareness should be strengthened not only by improving their theoretical knowledge but also by promoting the application of secure digital practices in their everyday behaviours. Furthermore, there is a need for practical training activities that will enable university students to respond more consciously to the cybersecurity risks they may encounter in their daily lives.

### *3.2. Findings on Awareness of Cyber Threats*

Based on interviews conducted with university administrators and faculty members, participants indicated that students' awareness of cyber threats such as phishing, social engineering, spyware, and identity theft, as well as digital security in general, was insufficient. Participants stated that students were familiar with these threat concepts to a certain extent; however, this awareness was not sufficiently reflected in their daily digital behaviour. It was noted that students sometimes exhibit careless behaviour, especially in situations such as fake links, untrusted applications, opening unknown files, and sharing personal information.

An examination of the interview forms revealed that although students have a certain level of theoretical knowledge, there are deficiencies in translating this knowledge into behavioural patterns. One participant evaluated students' awareness of these threats as follows:

**Participant (K4):** *"Although students have general knowledge about threats such as phishing and social engineering, they cannot always reflect this in their behaviour."*

Similarly, another participant stated that even though students have theoretical knowledge, they can exhibit behaviours that can lead to various security vulnerabilities in practice:

**Participant (K1):** *"Careless behaviour is frequently observed, especially regarding fake links and unreliable applications."*

These findings suggest that expanding practical training, case-based learning activities, and cybersecurity awareness programmes would significantly enhance students' ability to recognise and respond to cyber threats. Participants also emphasised that information security should be treated not only as a technical issue but also as a matter of individual responsibility and corporate culture, and that practices that translate theoretical knowledge into behaviour will contribute to the development of an information security culture.

### *3.3. Findings Regarding Basic Information Security Behaviours*

Based on interviews conducted with university administrators and faculty members, the findings revealed that students' adoption of basic information security practices, such as screen locking, secure password use, the secure use of USB drives, and the protection of institutional data, was generally insufficient. Participants stated that some students apply basic security measures; however, there are various shortcomings in transforming these practices into sustainable and conscious digital behaviours. It was noted that negligence could occur, particularly regarding the use of strong passwords, device security, data protection practices, and the secure use of portable storage devices. Participants stated that students often considered information security practices an individual preference rather than a mandatory requirement, and that this situation could pose risks to personal data security and institutional systems. It was emphasised that behaviours such as using simple passwords, sharing passwords, leaving devices unlocked, and using USB drives insecurely create information security vulnerabilities. One participant expressed their opinion on the level of adoption of security practices by students as follows:

**Participant (K7):** *"While most students are aware of password usage, there are shortcomings in creating strong and unique passwords. Furthermore, there are occasional neglects regarding issues such as screen locking, secure use of USB drives, and the protection of school data."*

Similarly, another participant stated that students did not implement security measures regularly and systematically:

**Participant (K1):** *"Security measures are often seen as a personal preference rather than a mandatory requirement. This poses a risk to both personal data and university systems."*

The analysis revealed that students require continuous guidance and practical support to develop sustainable information security behaviours. These findings suggest that universities should expand training and awareness initiatives focusing on password security, screen protection, data privacy, and the secure use of portable storage devices.

#### *3.4.1. Findings Regarding Cyberbullying and Support Mechanisms*

According to the views of university administrators and faculty members, students demonstrated a moderate level of awareness regarding cyberbullying; however, they had limited knowledge of the institutional support mechanisms and reporting procedures available within the university. Participants stated that students generally know the concept of cyberbullying; however, they do not have sufficient knowledge about contacting appropriate units or individuals regarding cyber risks encountered in the university environment.

Participants stated that students often consider cyberbullying and cybersecurity breaches as an individual problem and may be hesitant to seek professional support. In addition, opinions were expressed that there are certain support mechanisms within the university; however, the visibility of these mechanisms and the level of awareness among students are insufficient. One participant expressed this situation as follows:

**Participant (K12):** *"Awareness of cyberbullying has increased, but I think students are not sufficiently knowledgeable about support mechanisms."*

Similarly, another participant stated that students do not fully know how to report the risks they encounter and which units they can get support from:

**Participant (K10):** *"A significant number of students do not fully know how to report the risks they encounter or the support mechanisms."*

Similarly, another participant stated,

**Participant (K2):** *"Students do not have sufficient knowledge about cyberbullying. They can normalize what they do, they can see it as a joke."*.

The findings highlight the need to increase the visibility of institutional support mechanisms for cyberbullying and digital security incidents and to provide students with regular guidance regarding available reporting procedures. In particular, it is understood that it is important to expand

training and seminar activities that will increase the awareness levels of students regarding safe digital environment use and combating cyberbullying.

*3.4.2. Findings Regarding Institutional Information and Application Processes on Information Security*

The findings indicate that universities should strengthen the visibility of institutional support mechanisms, improve reporting procedures, and provide coordinated technical, psychological, and administrative support for information security incidents. It is understood that it is especially important to disseminate training and guidance activities that will increase students' awareness of safe digital media use and combating cyberbullying. Participants stated that students often do not know which unit to turn to for problems related to information security and that current information activities should be given a more systematic structure. It was stated that the duties and responsibilities of technical support units, student affairs and IT units within the university should be more clearly introduced to students. One participant expressed this situation as follows:

**Participant (K3):** *"Most students do not know exactly where to turn when they have a problem. I think universities should be given more information on this issue."*

Similarly, another participant emphasised that multilingual information activities at universities could be beneficial:

**Participant (K4):** *"I think it would be beneficial to prepare informative brochures and organise seminars in common languages such as Turkish, English and Arabic through student affairs."*

Based on participants' perspectives, universities should establish more visible and systematic reporting procedures supported by orientation programmes, seminars, informational brochures, and digital guidance resources. These findings further emphasise the importance of expanding training programmes and awareness activities that promote safe digital practices and effective strategies for preventing cyberbullying.

### *3.5. Suggestions for Increasing Information Security and Privacy Awareness*

As a result of the interviews with university administrators and faculty members, it was evaluated that more systematic, sustainable and application-based education processes are needed in universities in order to increase students' information security and privacy awareness levels. Participants stated that theoretical knowledge alone is insufficient; they emphasised that priority should be given to practical training, awareness activities, and institutional guidance that encourage safe digital behaviours as part of everyday practice. Participants emphasised that issues such as digital privacy, safe internet use, protection of personal data, phishing attacks, social engineering and password security should be made more visible at the university level.

Among the suggestions most frequently expressed by the participants are regular awareness seminars, applied training programmes, workshops, case studies and awareness-raising activities that will ensure the active participation of students. It has been stated that training, especially through real-life examples, will contribute to students' understanding of information security risks more concretely. In addition, it was emphasised that information security and digital privacy issues should be given more attention in university orientation processes.

One participant expressed their opinion on increasing information security awareness as follows:

**Participant (K2):** "It is important for students to learn not only theoretical knowledge but also how to take precautions against risks they may encounter in daily life. Therefore, I think that organising practical training, seminars, and awareness studies would be beneficial."

Similarly, another participant emphasised the need to spread a security culture at the corporate level with the following statements:

**Participant (K8):** *"It is thought that information security should be addressed not only as a technical issue but also as a matter of individual responsibility and corporate culture."*

Similarly, another participant stated,

**Participant (K11):** *"Regarding virtual privacy and information security, it is essential that there is an organisation at the university that will provide support in this regard."*

The findings indicate that universities should adopt sustainable, practice-oriented educational models that actively engage students in developing secure digital behaviours and long-term information security awareness. In addition, it is understood that it is important for information activities to not be limited to certain periods; they should gain continuity through orientation processes, seminars, digital training content, and corporate information mechanisms.

*Table 2. Theme, Code, and Frequency Distributions for Qualitative Findings.*

| Theme | Code | f |
|---|---|---|
| **Digital Security and Privacy Awareness** | Insufficient awareness | 11 |
| | Lack of knowledge about secure/insecure wireless networks | 8 |
| | Lack of knowledge about cookies and website certificates | 9 |
| | Sufficient awareness | 3 |
| **Cyber Threat Awareness** | Limited awareness of phishing and social engineering | 10 |
| | Inability to respond appropriately to cyber threats | 11 |
| | Lack of awareness regarding institutional reporting procedures | 11 |
| | Sufficient awareness | 3 |
| **Basic Information Security Practices** | Weak password practices | 9 |
| | Insufficient USB security awareness | 11 |
| | Low awareness of institutional data protection | 10 |
| | Screen-lock usage | 8 |
| **Cyberbullying and Support Mechanisms** | Limited awareness of cyberbullying | 10 |
| | Lack of knowledge about available support services | 11 |
| | Lack of knowledge about reporting procedures | 11 |
| | Sufficient awareness | 3 |
| **Institutional Support and Reporting Processes** | Limited knowledge of reporting mechanisms | 10 |
| | Insufficient institutional guidance | 9 |
| | Lack of visibility of support units | 2 |
| **Educational Needs and Recommendations** | Regular awareness training | 13 |
| | Practical cybersecurity training | 9 |
| | Establishment of institutional support units | 8 |
| | Increasing legal awareness | 4 |

Note: Frequency (f) indicates the number of participants who expressed views corresponding to each code. Multiple responses were permitted; therefore, frequencies exceed the total number of participants (N = 15).

Theme, code, and frequency distributions for qualitative findings are presented in Table 2. Examining the theme, code, and frequency values in Table 2, it is seen that the vast majority of opinions obtained from participants indicate that students have a low level of awareness regarding information security and privacy. Here, the lack of knowledge about mechanisms to be used after

exposure to cyber threats (f=11), the need for training, seminars, and conferences to raise awareness among students in the field of information security and privacy (f=13), and the need for information on phishing and digital privacy are particularly prominent. Despite this, a small number of participants stated that students have a sufficient level of awareness regarding information security and privacy.

## 4. Discussion

The findings of the present study indicate that although university students possess a basic level of awareness regarding information security and privacy, this awareness is not consistently translated into secure digital behaviours. According to the evaluations of university administrators and faculty members, students demonstrate notable deficiencies in recognising phishing attacks, social engineering techniques, password security practices, digital privacy protection, and institutional reporting mechanisms. These findings suggest that information security awareness should not be evaluated solely in terms of knowledge acquisition but also in terms of individuals' ability to apply this knowledge in their daily digital practices. Similar observations have been reported in previous studies emphasising that awareness alone is insufficient unless it is reinforced through continuous education, practical training, and institutional support mechanisms (AlGhamdi et al., 2020; Nezgitli & Gökçearslan, 2022; Hobbs, 2023).

The growing adoption of artificial intelligence technologies further reinforces the significance of these findings. AI-powered educational platforms increasingly rely on large volumes of personal and institutional data, making information security awareness a critical competency for both students and higher education institutions. Recent international guidance emphasises that universities should complement technological innovation with comprehensive policies addressing data protection, cybersecurity awareness, ethical AI use, and institutional governance to ensure the responsible implementation of AI-supported educational systems (UNESCO, 2023; OECD, 2023).

Another important finding of this study is that many students are unaware of the institutional support mechanisms available when they encounter cybersecurity incidents. Although participants acknowledged that students possess a certain level of theoretical knowledge regarding information security, they emphasised that many students do not know where to seek assistance or how to report cybersecurity incidents within the university. This finding indicates that establishing a strong information security culture in higher education requires not only technological safeguards but also visible institutional policies, accessible reporting procedures, and continuous awareness activities. Recent studies similarly argue that higher education institutions should integrate awareness programmes with organisational policies and structured cybersecurity training frameworks to improve institutional resilience.

The findings also reveal that participants perceive practical cybersecurity education as more effective than theoretical instruction alone. Regular awareness programmes, orientation training, seminars, workshops, and simulation-based activities were frequently recommended as effective strategies for improving students' cybersecurity behaviours. This observation supports recent research demonstrating that experiential and continuous cybersecurity education contributes significantly to the development of secure digital habits among university students and promotes long-term behavioural change.

From an institutional perspective, this study contributes to the existing literature by examining information security awareness through the evaluations of university administrators and faculty members rather than relying exclusively on students' self-reported perceptions. This perspective provides a broader understanding of information security awareness by emphasising the interaction between individual awareness, institutional practices, and organisational support mechanisms. Rather than considering cybersecurity awareness solely as an individual responsibility, the findings support the view that universities should develop comprehensive institutional strategies combining governance, continuous education, technological safeguards, and accessible support services to establish a sustainable cybersecurity culture.

Overall, the findings demonstrate that improving information security awareness is not limited to increasing theoretical knowledge but also requires transforming awareness into secure digital behaviour through continuous education, institutional commitment, and effective communication strategies. As cyber threats continue to evolve within higher education environments, universities should adopt integrated cybersecurity awareness programmes that combine educational, technological, and organisational approaches to strengthen both individual responsibility and institutional resilience.

## 5. Limitations of the Study

This study has several limitations that should be considered when interpreting the findings.

First, the study was conducted with a relatively small qualitative sample consisting of 15 university administrators and faculty members from a single higher education institution. Therefore, the findings should not be generalised to all universities or higher education systems.

Second, the study relied on participants' self-reported opinions. As with most interview-based qualitative research, participants may have provided socially desirable responses or responses influenced by institutional expectations.

Finally, this article focuses exclusively on the qualitative dimension of the research. Future research should validate these findings across different higher education institutions and cultural contexts using larger and more heterogeneous samples.

## 6. Conclusion and Recommendations

This study demonstrated that, according to the evaluations of university administrators and faculty members, university students possess a basic level of awareness regarding information security and privacy; however, this awareness is not consistently reflected in their everyday digital behaviours. In particular, deficiencies were identified in areas such as phishing awareness, social engineering, digital privacy, password security, and knowledge of institutional reporting mechanisms.

The findings indicate that information security awareness should not be considered merely the acquisition of technical knowledge. Rather, sustainable information security requires the integration of individual awareness, secure digital behaviours, institutional policies, and continuous educational initiatives.

This study contributes to the existing literature by examining information security awareness from the perspectives of university administrators and faculty members rather than relying solely on students' self-reported perceptions. Consequently, the findings provide an institutional perspective on strengthening the information security culture within higher education institutions.

Based on the findings, universities are encouraged to implement continuous cybersecurity awareness programmes, increase the visibility of institutional reporting mechanisms, expand practical awareness activities, and strengthen institutional information security policies.

Future research should include larger and more diverse samples from different higher education institutions, employ mixed-method research designs, and further investigate the psychological, behavioural, and organisational factors influencing information security awareness and secure digital behaviour.

Ultimately, strengthening information security and privacy awareness in the age of artificial intelligence requires a long-term institutional commitment that integrates technological innovation, continuous education, and secure digital practices across higher education institutions.

## References

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

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

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. Sage.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2020). *Bilimsel araştırma yöntemleri* [Scientific research methods] (28th ed.). Pegem Akademi.

Creswell, J. W., & Guetterman, T. C. (2018). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.). Pearson.

DataReportal. (2022). *Digital 2022: Turkey*. https://datareportal.com/reports/digital-2022-turkey

Ericsson. (2022, February 15). *Number of smartphone subscriptions worldwide from 2016 to 2021, with forecasts from 2022 to 2027 (in millions)* [Graph]. In *Statista*. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Fallows, D. (2004). *The internet and daily life*. Pew Internet & American Life Project. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2004/PIP_Internet_and_Daily_Life.pdf

Hobbs, J. (2023). Cybersecurity awareness in higher education: A comparative analysis of faculty and staff. *Issues in Information Systems, 24*(1), 159–169. https://doi.org/10.48009/1_iis_2023_114

International Telecommunication Union. (2022). *Percentage of individuals using the internet worldwide as of 2022, by region* [Graph]. In *Statista*. https://www.statista.com/statistics/333879/individuals-using-the-internet-worldwide-region/

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Sage.

Mouwers-Singh, C., & Musikavanhu, T. B. (2024). A narrative review on enhancing cybersecurity in higher education institutions: The role of continuous training and awareness. *Expert Journal of Business and Management, 12*(2), 67–73.

Nezgitli, S., & Gökçearslan, Ş. (2022). Kamu kurumu ve özel sektöre yönelik bilgi güvenliği farkındalığı üzerine bir inceleme [A review of information security awareness in public institutions and the private sector]. *Instructional Technology and Lifelong Learning, 3*(1), 19–44. https://doi.org/10.52911/itall.1115701

OECD. (2023). *OECD digital education outlook 2023: Emerging governance of generative AI in education*. OECD Publishing. https://www.oecd.org/en/publications/oecd-digital-education-outlook-2023_c74f03de-en.html

Polat, A. (2022). *Nitel Araştırmalarda Yarı-Yapılandırılmış Görüşme Soruları: Soru Form ve Türleri, Nitelikler ve Sıralama* [Semi-Structured Interview Questions in Qualitative Research: Question Forms and Types, Qualities and Order]. *Anadolu Üniversitesi Sosyal Bilimler Dergisi, 22*(Special Issue 2), 161–182. https://doi.org/10.18037/ausbd.1227335

StatCounter. (2022). *Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 2nd quarter 2022* [Graph]. In *Statista*. https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

Statista. (2022). *Social network usage by frequency in Turkey in 2022* [Graph]. In *Statista*. https://www.statista.com/forecasts/1002994/social-network-usage-by-frequency-in-turkey

Talan, T., & Aktürk, C. (2021). Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi [An examination of secondary school students' digital literacy and information security awareness levels]. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18*(1), 158–180. https://doi.org/10.33437/ksusbd.668255

Tekerek, M., & Mart, İ. (2010). Behavioral computer and web security awareness for K–8 level. In *4th Information Security and Cryptology Conference Proceeding Book* (pp. 254–258).

Turkish Statistical Institute. (2022). *Survey on Information and Communication Technology (ICT) Usage in Households and by Individuals, 2022*. https://veriportali.tuik.gov.tr/Bulten/Index?p=45587&dil=2

UNESCO. (2023). *Guidance for Generative AI in Education and Research.* UNESCO.

Yıldırım, A., & Şimşek, H. (2021). *Sosyal bilimlerde nitel araştırma yöntemleri* [Qualitative research methods in the social sciences] (12th ed.). Seçkin Yayıncılık.