Journal of Studies in Advanced Technologies
[İleri Teknolojilerde Çalışmalar Dergisi]
e-ISSN: 2980-2695

Research Article

Measuring Digital Data Security Awareness: The Case of Higher Education Institution

Salih Serkan Kaleli[1]*

[1] Vocational School of Social Sciences, Ardahan University, 75002, Ardahan, Türkiye

* Correspondence: salihserkankaleli@gmail.com

Received: 26 November 2024; Accepted: 14 December 2024; Published: 31 December 2024

Abstract: Digital data security is of critical importance for individuals and institutions today and encompasses a range of practices and policies aimed at ensuring the confidentiality, integrity and accessibility of digital data. This study aimed to examine the awareness levels of students as well as academic and administrative staff at Ardahan University regarding digital data security and the factors affecting this awareness. A digital data security awareness scale was applied to 324 participants within the scope of the study. The digital data security awareness scale measures the participants' knowledge and behaviors on issues such as password security, safe internet use, data backup and software updates. The data obtained show that the participants generally have a medium to high level of awareness regarding digital data security. It is thought that the results of the research are important in terms of showing that students, as well as academic and administrative staff working at the university, are aware of the protection and security of digital data. In addition, the study reveals the current status of digital data security awareness throughout the university by covering both academic and administrative staff as well as students. This broad scope is intended to help universities better understand the needs of different groups when creating their digital data security policies.

Keywords: Digital data, digital data security, information security, awareness

Araştırma Makalesi

Dijital Veri Güvenliği Farkındalığının Ölçümlenmesi: Yükseköğretim Kurumu Örneği

Öz: Dijital veri güvenliği, günümüzde bireyler ve kurumlar için kritik bir öneme sahip olup, dijital verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamayı hedefleyen bir dizi uygulamayı ve politikayı kapsamaktadır. Bu çalışma, Ardahan Üniversitesi'ndeki akademik ve idari personelin yanı sıra öğrencilerin dijital veri güvenliği konusundaki farkındalık düzeylerini ve bu farkındalığı etkileyen faktörleri incelemeyi amaçlamıştır. Çalışma kapsamında 324 katılımcıya dijital veri güvenliği farkındalık ölçeği uygulanmıştır. Dijital veri güvenliği farkındalık ölçeği, katılımcıların parola güvenliği, güvenli internet kullanımı, veri yedekleme ve yazılım güncelleme gibi konulardaki bilgi ve davranışlarını ölçmektedir. Elde edilen veriler, katılımcıların dijital veri güvenliği konusunda genel olarak orta ila yüksek düzeyde farkındalığa sahip olduğunu göstermektedir. Araştırma sonuçlarının, üniversitede görev yapan akademik ve idari personelin yanı sıra öğrencilerin de dijital verilerin korunması ve güvenliği konusunda bilinçli olduklarını göstermesi açısından önemli olduğu düşünülmektedir. Ayrıca çalışma hem akademik hem de idari personelin yanı sıra öğrencileri de kapsayarak, üniversite genelinde dijital veri güvenliği farkındalığının mevcut durumunu ortaya koymaktadır. Bu geniş kapsamda, üniversitelerin dijital veri güvenliği politikalarını oluştururken farklı grupların ihtiyaçlarını daha iyi anlamalarına yardımcı olması amaçlanmaktadır

Anahtar Kelimeler: Dijital veri, dijital veri güvenliği, bilgi güvenliği, farkındalık

Citation: S. S. Kaleli, “Measuring Digital Data Security Awareness: The Case of Higher Education Institution”, *Journal of Studies in Advanced Technologies*, vol. 2, no. 2, pp. 108-119, Dec 2024, doi: 10.63063/jsat.1591281

1. Introduction

Digital data security has a vital importance in today's rapidly changing and digitalised world with new technologies. The proliferation of the Internet and digital technologies has brought with it the need to protect the security of personal and corporate data. With information security breaches increasing and cyber-attacks becoming more sophisticated, digital data security awareness has become an ever more important issue for people. The scope of digital security includes understanding online threats, knowing how to defend against them and actively using these defences across all devices. Protecting users' digital data starts with the creation of strong passwords and continues with the use of both free and paid security tools [1]. Digital information security is of great importance at both organisational and individual level. Because, loss of information or unauthorised access can have serious consequences such as financial losses, reputational damage and legal sanctions. Especially the protection of personal data is a critical issue in terms of privacy and security of individuals. For this reason, digital information security has become an increasingly important and widespread area today [2].

Digital data security covers a set of practices that protect the data in the digital environment against threats such as unauthorised access, modification or deletion. These applications ensure the protection of information by aiming to ensure the confidentiality, integrity and accessibility of data. There are 3 basic needs for the security of digital data. Confidentiality: It means protecting sensitive and private information and preventing its dissemination. Integrity: ensures that data remains complete in its original form. Accessibility: refers to the ability to access the system immediately when authorised users need it. In order to ensure security within the framework of these 3 basic requirements, it is very important that individuals or organisations take measures to prevent attacks such as authentication and encryption, access control, antivirus software, strong passwords [3].

For this purpose, the aim of the study is to determine the level of awareness of administrative staff, academic staff and students at Ardahan University on digital data security and to offer solutions to increase and improve this awareness. The main objectives of the study are to evaluate current digital data security practices and risks and to understand the digital data security perceptions and behaviours of different user groups (administrative staff, academic staff, students).

2. Conceptual Framework

Today, the expression "digital technologies" usually refers to devices with internet connection, but it actually covers all electronic tools, systems and resources that produce, store or process data. At this point, it is important to pay attention to the distinction between the concepts of "digitalization" and "digitalization", which are often confused in Turkish. Digitalization is the process of transferring analog or physical information (printed documents, images, sound recordings, etc.) to a digital environment, that is, converting them into bits or bytes. While the conversion of all information and documents of an institution to a digital format is called "digitalization", "digitalization" is a broader concept. When the evolution of digital technologies is examined, it is seen that the process, which starts with the transfer of tangible materials to a digital environment in the first stage, progresses over time towards the digitalization of processes and ultimately the deep interaction of people with the digital world [4]. In fact, the factors that form the basic structure of digitalization are technological and organizational processes. These processes include activities such as collecting, storing, processing, analyzing and securing data. Therefore, digital data refers to the data processed and evaluated through these processes. In other words, digital data can be defined as data produced and processed through digital technologies. These data can be obtained from various sources and used in different ways. For example, digital data obtained about students and teachers can be used to monitor, evaluate and improve learning processes [5].

In people's daily lives, social and business life includes physical environments as well as cyberspace (digital world) where we connect to people and software through internet connections. Today, the internet has become an inseparable part of our daily lives and behaviors. Using this area, where personal data is also shared, requires a certain level of awareness and skill. In this direction, it is critical for users to gradually improve their daily behaviors and to address unconscious behaviors and habits in terms of data security [6]. This includes both building knowledge, attitudes and behaviors that are in line with users' needs and expectations, and eliminating knowledge, attitudes and behaviors that stem from incomplete or incorrect perceptions of risky situations. In short, people must be conscious of data security, develop the necessary skills and constantly evaluate and improve their online behaviors, especially in order to exist safely and effectively in cyberspace.

The main purpose of data security is to protect valuable and sensitive personal data such as e-mail and bank information. Valuable data, including educational information, financial data, and confidential information such as sensitive information on phone numbers collected, stored and managed by different institutions or organizations are a gold mine for hackers. Within the scope of data security, the processes and technologies used to protect data play a critical role in the best protection of personal data. In today's digital world, the protection of personal data has become one of the most important priorities for both individuals and institutions. Collected and stored data is a valuable asset [7].

Protecting data from corruption and unauthorized access prevents individuals from having their data stolen and used without their knowledge and consent. This requires creating defense mechanisms against threats that may come from both inside and outside. Data security is an essential element to ensure the privacy and security of individuals. Systems that allow people to store and share data on the internet are called cloud storage [8]. Cloud storage has advantages such as unlimited data storage and the creation of secure and useful storage areas. Data security is a critical issue for individuals and institutions in the digital age. Confidentiality, integrity, accessibility and secure management of data form the cornerstones of a reliable and effective information system. In this context, it is possible to summarize the basic principles of data security as follows [8], [9], [10].

- Data Confidentiality: It refers to the protection of data against unauthorized access. It is essential that the information received by the data recipient is completely consistent with the information sent by the sender. In other words, only authorized persons have access to data. For example, employees who are interested in personal bank accounts should have access, but no one else should have access. When data is accessed by others, data confidentiality is violated, and this situation is irreversible.

- Data Integrity: It refers to the reliability of data; that is, data cannot be arbitrarily changed or altered by others. For example, when shopping online, someone should not be able to change the products in your cart without your permission. Lack of data integrity can lead to serious security problems.

- Data Accessibility: It emphasizes that data can be accessed normally at any time. Users have the right to access, download or modify data in the cloud whenever they need.

- Complete Data Deletion: When users stop using cloud storage, they can completely delete the data they transferred to the cloud server and verify that the data is completely destroyed, rather than being tricked by malicious cloud service providers.

- Privacy Protection: While users are getting used to the convenience of cloud storage, cloud storage providers are stealing privacy information such as personal identity, location, and sensitive data for the organization. Privacy security mechanisms are used to ensure that this data remains private from snoops and malicious employees of cloud service providers.

In conclusion, since data security is a multidimensional concept, all the principles mentioned above should be considered together to manage data securely and effectively. The application of these principles allows individuals and institutions to exist and operate safely in the digital world. The importance of digital data brings with it various risks. Cyber attacks, data breaches, malware, hardware failures and even natural disasters can damage or prevent access to digital data. Such incidents can lead to financial losses, identity theft and reputation damage for individuals, as well as serious consequences for institutions such as financial losses, loss of reputation and even bankruptcy. In order to avoid much worse consequences, people need to gain awareness of digital data security [11].

The main purpose of data security awareness is to raise awareness among people of all levels and social backgrounds about various critical issues that arise from insufficient attention to the management of their own data and the data of others. Therefore, Data security awareness undertakes the task of teaching users the correct use of information technologies and making them aware of this issue, providing tools to prevent and reduce the unintentional disclosure of sensitive data.

Cybercriminals are constantly developing new methods to exploit weaknesses in data security infrastructure. While organizations implement advanced security measures such as firewalls, encryption, and real-time monitoring, it is crucial to take proactive steps to further protect against data breaches and threats. In this regard, some practical and effective strategies that can be used to minimize data risks and strengthen data protection can be summarized as follows;

1. First, data breaches should be limited. Data breaches often start with weak passwords. Unsolicited personal requests via email, phone or text should not be responded to.

2. Create strong and unique passwords. Passwords should be changed regularly to reduce the possibility of data breaches.

3. It is important to enable multi-factor authentication. Multi-factor authentication acts as a double defense system for data. This significantly reduces the possibility of unauthorized access.

4. Beware of phishing attacks. Phishing is a leading tactic, especially in data breaches. Beware of emails or messages from unknown senders and avoid clicking on unverified links.

5. Software and systems need to be updated regularly. Operating systems, applications and antivirus software should be updated to fix new security vulnerabilities and minimize data breaches.

By implementing the above strategies, data security can be strengthened and become more resilient to cyber-attacks. Data security awareness plays an important role in implementing and implementing these strategies

3. Literature Review

The concept of digital data security has become one of the very important building blocks of today's information management by significantly affecting various sectors such as education, health, banking and public services due to the widespread use of computers, tablets and mobile devices. At the same time, it is equally important for individuals to be aware and conscious about the protection of information and data stored in digital environment. In one of the studies conducted for this purpose [12], examined the relationship between digital data security awareness and digital literacy. The research was conducted with the participation of 265 students and the relationship between the two concepts was presented in detail. According to the study, it was found that students' digital literacy levels were medium and digital data security awareness levels were high. In addition, a significant positive relationship was found between digital literacy and digital data security awareness. As a result of the study, adding digital literacy and data security courses to the curriculum is among the recommendations to raise awareness.

In another study [13], examined the digital parenting, digital literacy and digital data security awareness levels of preschool teachers and parents. "Digital Parenting Attitude Scale", "Digital Literacy Scale" and "Digital Data Security Awareness Scale" were used as data collection tools in the study. As a result of the study, it was found that preschool teachers had higher levels of digital literacy and digital data security awareness than parents, and there was a statistically significant difference between digital literacy and digital data security awareness. In another study where a significant relationship was found between digital data security and parental guidance scores [14], adapt the "Parental Guidance of Young Children's Internet Use Scale" developed by Nikken and Jansz into Turkish and to examine parental guidance according to some variables. As a result of the study, it is stated that a valid and reliable scale that is sufficient in terms of content to determine the level of parental guidance of young children's internet use contributes to the Turkish literature. In addition, it was determined that the parental guidance levels of young children's internet use differed according to age, education and internet use experience levels with the scale created as a result of the scale adaptation study.

In another study examining digital data security awareness [15], conducted a survey on pharmacy students. First, explanatory factor analysis was performed on the obtained data, then the effects of some variables on digital data security awareness were investigated with t-test and variance analysis. It was determined that digital data security awareness was higher in those who had an antivirus program on their smartphones. In addition, it was determined that the average of the students' responses to the statements in the scale was around three, and it was concluded that students' awareness on this issue should be improved. In another study [16], conducted a study on security awareness and behavior of young people (digital natives). The study found that although users are less concerned about security when using laptops, even security-savvy users are more likely to compromise on security when it comes to usability.

Aiming to measure the information security awareness level of digital wallet users in Indonesia [17], a survey was conducted with 156 participants consisting of digital wallet users. The level of information security awareness was calculated using the analytical hierarchy method. As a result of the study, it was seen that the participants' information security awareness level was generally good (80.78%). However, it was determined that the scores remained at an average level in some focus areas. This situation is thought to be one of the reasons why information security violations against digital wallet users are still common. [18], it analyzed how public officials understand the need for information security in Romanian public administration. The study is based on a survey conducted in three institutions in Romanian public administration. The aim of the survey is to identify vulnerabilities in specific areas such as accessibility management in user interface design, password management, cybersecurity incident prevention, cybersecurity incident response capacity, personal data protection, data backup and recovery, and personal assessment. The study presents conceptual solutions for ensuring information security and states that these solutions are based on the analysis of international documents.

4. Method

This study aims to determine the digital data security awareness (DDSA) of academic, administrative staff and students at Ardahan University. The research universe consists of 7411 people, including 6680 students, 372 academic staff and 359 administrative staff. Curry's (1984) sample size determination rule was used when determining the research sample. According to this method; 100% sample for sample sizes ranging from 10 to 100, 10% sample for sample sizes ranging from 101 to 1000, 5% sample for sample sizes ranging from 1001 to 5000 and 3% sample for sample sizes ranging from 5001 to 10000 is recommended [19]. Based on this method, a survey was conducted online with 324 students and staff at Ardahan University using the convenience sampling method.

The findings obtained within the scope of the research will be evaluated at a significance level of 5% at a 95% confidence interval, and the Jamovi 2.4 program was used for the analyses. Normality analysis was performed before starting the data analysis. In addition to descriptive statistics, confirmatory factor analysis, internal consistency reliability (Cronbach's Alpha, Composite Reliability-CR) and Convergent validity (AVE) were used in the analysis of the data. Whether the digital data security awareness of the participants differed according to gender was determined with the t-test; whether it varies according to age, education level, duty, daily internet and computer usage was tested with One-way analysis of variance (Anova).

The digital data security awareness scale developed by Yılmaz et al. [20], was used in the study. The scale consists of 32 statements and a single dimension. The reliability of the scale, which was rated with a 5-point Likert-type rating (1- Strongly disagree, 2- Disagree, 3- Undecided, 4- Agree, 5- Strongly agree), was found to be high by the researcher (Cronbach’s Alpha 0.90).

The research was designed in line with the following questions?

1. What is the level of digital data security awareness of academic staff, administrative staff and students?
2. Do demographic variables (gender, age, educational status, etc.) make a difference on digital data security awareness?
3. Do the positions in the university (academic, administrative, student) make a difference on digital data security awareness?
4. Does daily computer usage time make a difference on digital data security awareness?
5. Does daily internet usage time make a difference on digital data security awareness?

4. Findings

As the first step of the scale analysis, the normal distribution of the data was checked with the Skewness and Kurtosis values. The skewness value being between -2 and +2 and the kurtosis being between -7 and +7 are considered acceptable limits for normal distribution [21].

Table 1. Digital Data Security Awareness

	$\bar{X}$-SS	**α**	**Skewness**	**Kurtosis**
DDSA	4.09±0.59	0.96	-0.988	2.88

When Table 1 is examined, it is seen that the digital data security awareness of the participants at Ardahan University is above 4 and in good condition. The Cronbach's Alpha coefficient of the data in the study was found to be 0.96. This value shows that the digital data security awareness scale is reliable. In addition to these results, it is seen that the data has a normal distribution.

Confirmatory factor analysis was applied to determine whether the original structure of the scale used in the research was confirmed by the data collected. The results are shown in Table 2.

Table 2. Result Measurement of Model Assessment.

Factor	**Item**	**Faktor Loading**	**Standart Error**	**t**	**p**	**AVE**	**CR**
DVSA	DVSA2	0.664	-	-	-	0.50	0.96
	DVSA3	0.628	0.083	12.57	***		
	DVSA4	0.622	0.086	10.44	***		
	DVSA7	0.602	0.093	10.13	***		
	DVSA8	0.704	0.092	11.66	***		
	DVSA9	0.684	0.099	11.36	***		
	DVSA10	0.687	0.097	11.42	***		
	DVSA11	0.667	0.089	11.12	***		
	DVSA12	0.561	0.101	9.49	***		
	DVSA13	0.791	0.090	12.90	***		
	DVSA14	0.753	0.087	12.37	***		
	DVSA15	0.818	0.086	13.28	***		
	DVSA16	0.724	0.094	11.96	***		
	DVSA17	0.731	0.092	12.06	***		
	DVSA18	0.792	0.088	12.92	***		
	DVSA19	0.680	0.096	11.30	***		
	DVSA22	0.707	0.093	11.70	***		
	DVSA23	0.738	0.100	12.15	***		
	DVSA24	0.765	0.082	12.54	***		
	DVSA25	0.737	0.090	12.15	***		
	DVSA26	0.735	0.089	12.11	***		
	DVSA27	0.748	0.092	12.30	***		
	DVSA28	0.771	0.090	12.62	***		
	DVSA30	0.726	0.091	11.98	***		
	DVSA31	0.578	0.100	9.76	***		
	DVSA32	0.643	0.099	10.76	***		

	χ2/DF	**CFI**	**NFI**	**TLI**	**GFI**	**AGFI**	**RMSEA**	**SRMR**
DVSA	2.04	0.94	0.90	0.94	0.97	0.97	0.05	0.04
Acceptable Fit*	≤ 3	≥ .90	≥ .90	≥ .90	≥ .90	≥ .85	≥ .08	≥ .08
Perfect Fit*	≤ 2	≥ .95	≥ .95	≥ .95	≥ .95	≥ .90	≥ .05	≥ .05

*[22]

When Table 2 is examined, items with factor loadings lower than 0.40 (1, 5, 6, 20, 21, 29) were removed from the scale. When the fit index values were examined after the items were removed, it was seen that the Chi-Square Fit Test (χ2/DF), Comparative Fit Index (CFI), Tucker-Lewis Fit Index (TLI), Goodness of Fit

Index (GFI) and Adjusted Goodness of Fit Index (AGFI) values were within the perfect fit limits, while the Root Mean Square Error of Approximation (RMSEA) and Standardized Root Mean Square Error of Approximation (SRMR) values were within acceptable limits. In addition to the examination of the structure obtained as a result of CFA, convergent and discriminant validity data were also examined. Accordingly, it is seen that the Average Variance Extracted (AVE) value is higher than 0.50 and the Composite Reliability (CR) value is higher than 0.70. All these results show that the model is compatible with the data, acceptable and reliable.

4.1. Demographic Information

Demographic information of the 324 students, administrative staff and academic staff who participated in the research is given in Table 3 below.

Table 3. Respondent’s Demographic Profile

Characteristics		Frequency	Percentage
Gender	Male	192	59.3
	Woman	132	40.7
Age	18-25	225	69.4
	26-33	66	20.4
	34+	33	10.2
Education Status	Associate degree	169	52.2
	Licence	103	31.8
	Postgraduate	52	16.1
Occupation	Student	240	74.1
	Academic Staff	50	15.4
	Administrative Staff	34	10.5
Daily computer usage time	Less than 1 hour	172	53.1
	1-3 hours	86	26.5
	4-6 hours	45	13.9
	7 hours and over	21	6.5
Daily Internet Usage Time	Less than 1 hour	7	2.2
	1-3 hours	92	28.4
	4-6 hours	144	44.4
	7 hours and over	81	25.0
I have my own computer	Yes	152	46.9
	No	172	53.1
I have a tablet computer	Yes	59	18.2
	No	265	81.8
I have a smartphone	Yes	315	97.2
	No	9	2.8

Of the 324 participants who participated in the study, 59.3% were male and 40.7% were female. When the age distribution was examined, it was seen that 69.4% of the participants were between the ages of 18-25, 20.4% were between the ages of 26-33, and 10.2% were 34 years of age or older. In terms of educational background, more than half of the participants (52.2%) had an associate degree. 31.8% had a licence degree, 16.1% had a postgraduate degree. When the occupational distribution of the participants was examined, it was seen that students were in the majority with 74.1%. Academic personnel came in second with 15.4%, while the rate of administrative personnel was 10.5%. In terms of technology use, 53.1% of the participants used the computer less than 1 hour a day, 26.5% used it for 1-3 hours, 13.9% for 4-6 hours, and only 6.5% used it for 7 hours or more. The daily internet usage time is higher; 2.2% connect to the internet for less than 1 hour, 28.4% for 1-3 hours, 44.4% for 4-6 hours and 25% for 7 hours and more. Based on this data, it can be said that the majority of the participants in the study have an associate degree or undergraduate degree. It can also be said that computer and especially internet use is quite common and the time spent on the internet is also remarkable. In terms of device ownership, 46.9% of the participants had their own computer, 18.2% had a tablet computer and 97.2% had a smartphone. These data show that digital devices, especially smartphones, are widely used among users

4.2. Descriptive Statistics

Descriptive statistical results related to the data obtained in the study are given in Table 4. In Table 4, the answers given by the participants on the subjects that they consider themselves deficient or self-sufficient are given in order from the highest average to the lowest average.

Table 4. Descriptive Statistics

Item No	Terms	Mean	Std. Dev.
24	I am aware that devices can be password-protected to prevent unauthorised use.	4.29	0.722
2	I know the importance of using letters, numbers and special characters when creating a password.	4.28	0.812
8	I am careful to create passwords that others cannot guess.	4.23	0.769
28	I know that logging in with a single-use password on your mobile phone increases security.	4.22	0.795
14	I know the importance of a high character count when creating a password.	4.20	0.771
4	I realise that files can be password-protected to prevent unauthorised use.	4.20	0.775
8	I know that credential verification messages (password etc.) received by e-mail should not be trusted.	4.19	0.821
25	I am careful not to perform operations that require a password on devices that do not belong to me.	4.18	0.798
15	I realise that storing passwords on any medium is a security risk.	4.17	0.753
13	I know that security questions used for password reminder should be answered in a way that others cannot guess.	4.16	0.788
30	I know the importance of using the ‘secure logout’ link when logging out of a website.	4.15	0.807
3	I know the importance of using different passwords for different operations.	4.11	0.892
17	I know that the files being worked on should be backed up on more than one medium.	4.10	0.814
26	I pay attention to the security warnings of the operating system (Windows, Android, etc.).	4.09	0.792
22	I realise that passwords need to be changed periodically.	4.09	0.828
11	I know the importance of downloading programs from the manufacturer's own site.	4.06	0.802
27	I know the importance of using laptops with batteries in case of power failure.	4.06	0.819
10	I am careful to delete e-mails that I consider unsafe without opening them.	4.03	0.872
16	I know that data can be stored on the Internet using various applications (Google Drive, etc.).	4.02	0.838
7	I make sure that the operating system (Windows, Android, etc.) is up to date.	4.01	0.844
19	I pay attention to whether the internet address bar is misleading.	3.99	0.858
23	I make a point of marking as ‘spam/junk/junk’ any rubbish emails that I don't want to receive.	3.95	0.887
32	I am aware that unlicensed software can create security vulnerabilities.	3.94	0.892
9	I know that portable storage units should be scanned for viruses before using them.	3.94	0.890
12	I know the importance of using antivirus software.	3.91	0.925
31	I have knowledge about the security certificates used in websites.	3.80	0.913
	General average	**4.09**	**0.591**

Among the data used in the study, the data with the highest mean was "I know the importance of using letters, numbers and special characters when creating passwords" with a mean of 4.29+-0.72, while the data with the lowest mean was "I have information about security certificates used in websites" with a mean of 3.80+-0.91. In this case, it shows that users actually pay attention when creating passwords for information security, but they have insufficient knowledge about security certificates on websites. When Table 4 is examined, it can be said that digital data security awareness is generally at a medium to high level. The average scores range from 4.29 to 3.80. The highest average scores are seen in statements related to basic security measures such as "I am aware that devices can be passworded to prevent unauthorized use" and "I know the importance of using letters, numbers and special characters when creating passwords." This shows that the participants are aware of basic security practices. On the other hand, the average scores are lower in statements related to more technical issues such as "I am aware of the security certificates used on websites" and "I am aware that unlicensed software can create security vulnerabilities." This finding shows that the participants may need more information on these technical issues.

4.3. Test of Difference

The results of the independent samples t-test and ANOVA, conducted to determine whether participants' awareness of digital data security differs based on gender, age, education status, occupation, and daily computer and internet usage duration, are presented in Table 5.

Table 5. Comparison of DVSA according to Socio-demographic characteristics

Variables		**N**	**x̄**	**SS**	**Test Value**	**p**	**Tukey**
Gender	Male	192	4,07	0,55	1,88	0,410	
	Woman	132	4,12	0,65			
Age	18-25 (1)	225	4,03	0,62	5,71	**0,005***	**3>1**
	26-33 (2)	66	4,28	0,48			
	34+ (3)	33	4,12	0,51			
Education Status	Associate degree (1)	169	4,00	0,60	5,82	**0,004***	**3>2**
	Licence (2)	103	4,16	0,62			
	Postgraduate (3)	52	4,25	0,42			
Occupation	Student (1)	240	4,07	0,63	0,88	0,410	
	Academic Staff (2)	50	4,11	0,45			
	Administrative Staff (3)	34	4,19	0,48			
Daily computer usage time	Less than 1 hour (1)	172	3,98	0.61	7,22	**0,001***	**4,3,2>1**
	1-3 hours (2)	86	4,25	0.60			
	4-6 hours (3)	45	4,26	0.44			
	7 hours and over (4)	21	4,26	0.44			
Daily Internet Usage Time	Less than 1 hour (1)	7	4,22	0,63	2,07	0,095	
	1-3 hours (2)	92	4,08	0,57			
	4-6 hours (3)	144	4,01	0,60			
	7 hours and over (4)	81	4,23	0,59			

In order to compare the digital data security scale scores according to the sociodemographic characteristics of the participants, independent t-test was applied for the comparison of two independent groups and one-way analysis of variance was applied for the comparison of more than two independent groups. As a result of the analysis, it was determined that there was a statistically significant difference between the participants' age, job, daily computer usage time and digital data security awareness scale scores ($p<0.05$). Tukey test was performed to determine the group that made a difference, and it was determined that the digital data security awareness score of 34+ participants was higher than the participants aged 18-25. It was determined that administrative staff had a higher digital data security awareness score than students, and those with a daily computer usage time of more than 1-3 hours had a higher digital security awareness than those with less than 1 hour.

When the age variable is examined, it is seen that the digital data security awareness of the participants aged 34 and above is higher than the participants aged 18-25 ($p<0.005$). This situation can be associated with the increase in experience and knowledge as age progresses. In terms of the education status variable, it was determined that the participants with postgraduate degrees have a higher awareness level than the participants with associate degrees ($p<0.010$). This finding shows that the development of knowledge and skills with the increase in the level of education also positively affects the digital data security awareness. It was observed that as the daily computer use time increases, the digital data security awareness also increases ($p<0.001$).

The participants who use the computer for 7 hours and more have a higher awareness level than those who use the computer for less than 1 hour. This result can be interpreted as the intensity of computer use increases the familiarity with the risks and security measures in the digital environment. In general, it was seen that variables such as age, education status and daily computer use time significantly affect the digital data security awareness level. Therefore, it can be said that customized training and awareness programs should be developed according to the needs of different groups.

5. Conclusion

According to the data obtained, age, position and computer usage time are seen as effective factors on digital security awareness. It is concluded that the digital security awareness of young people between the ages of 18-25 is lower than other age groups. This situation can be explained by the fact that young people trust technology much more and their digital literacy skills are less developed than other age groups. Similar results are observed in other studies [14], [16]. Academic and administrative staff were found to have higher digital security awareness than students. Since academic and administrative staff interact much more with digital data due to the nature of their work, they bear more responsibility for data security. The study also concluded that as the duration of computer use increases, the level of digital data security awareness also increases. Similar results are observed in other studies [20]. The higher digital security awareness of users whose computer time is more than 1-3 hours can be interpreted as more intensive computer use may expose users to security risks more and therefore encourage them to learn more about security measures. One of the important findings of the study is that increasing the level of education also increases the level of digital data security awareness. Göldağ [12] and Ng [23], also obtained similar results regarding education levels in their study. This situation can be explained by the fact that individuals' information access and evaluation skills improve with the increase in education level, and therefore they become more conscious about digital data security. In the study, the statement "I know the importance of using antivirus software" is one of the statements with the lowest average. Tarhan [15], in a study conducted with pharmacy students, it was found that students who had an antivirus program on their smartphones had higher awareness of digital data security. This finding can be interpreted as the use of security software increases digital data security awareness and makes people more sensitive to security measures.

In conclusion, in order for our university to successfully complete its digital transformation and create a secure digital environment, it is necessary to increase and improve the digital data security awareness of the personnel. For this purpose, with the implementation of suggestions such as organising trainings for different user groups, including current threats and protection methods, and conducting information campaigns on various platforms (website, social media, newsletters, etc.) to raise awareness about digital data security, digital data security awareness at our university will increase significantly and a safer digital environment will be created.

Acknowledgements

There is no financial support.

Conflict of Interest Statement

There is no conflict of interest as there is only one author.

References

[1] PandaSecurity, "What is Digital Security?", PandaSecurity, 2024. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/what-is-digital-security/. [Accessed: Oct. 20, 2024].

[2] Novarge, "What is Digital Information Security?", Novarge, 2024. [Online]. Available: https://www.novarge.com.tr/blog/. [Accessed: Oct. 15, 2024].

[3] R. Hassan, W. Wahi, N. H. A. Ismail, and S. A. B. Awwad, "Data Security Awareness in Online Learning," International Journal of Advanced Computer Science and Applications, vol. 13, no. 4, pp. 276–282, 2022, doi: 10.14569/IJACSA.2022.0130432.

[4] M. A. Özerbaş, A. Mayrambeg Kizi, and B. N. Safi, "Kırgızistan'daki Üniversite Öğrencilerinin Dijital Veri Güvenliği Farkındalık Düzeyleri TT - Digital Data Security Awareness Levels of University Students in Kyrgyzstan," Türk Eğitim Bilimleri Dergisi, vol. 21, no. 1, pp. 383–401, 2023, [Online]. Available: https://doi.org/10.37217/tebd.1193412%0Ahttps://dergipark.org.tr/en/download/article-file/2726118

[5] N. Selwyn, “Data entry: towards the critical study of digital data and education,” Learning, Media and Technology, vol. 40, no. 1, pp. 64–82, 2015, doi: 10.1080/17439884.2014.921628.

[6] G. Cascavilla, M. Conti, D. Frison, and A. Surian, “Data Security Awareness: metodi e strumenti per promuoverla nella scuola secondaria. Il caso del progetto Edu4Sec,” Media Education, vol. 8, pp. 276–284, 2017, doi: 10.14605/MED821709.

[7] A. Anil, V. K. Shukla, and V. P. Mishra, “Enhancing Data Security Using Digital Watermarking,” Proceedings of International Conference on Intelligent Engineering and Management, ICIEM 2020, pp. 364–369, 2020, doi: 10.1109/ICIEM48762.2020.9160090.

[8] P. Yang, N. Xiong, and J. Ren, “Data Security and Privacy Protection for Cloud Storage: A Survey,” IEEE Access, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[9] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead,” Journal of Network and Computer Applications, vol. 84, no. September 2016, pp. 38–54, 2017, doi: 10.1016/j.jnca.2017.02.001.

[10] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues,” IEEE Access, vol. 6, no. Idc, pp. 18209–18237, 2018, doi: 10.1109/ACCESS.2018.2820162.

[11] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, “I Think They’re Trying to Tell Me Something: Advice Sources and Selection for Digital Security,” Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, pp. 272–288, 2016, doi: 10.1109/SP.2016.24.

[12] B. Göldağ, “Investigation of the Relationship between Digital Literacy Levels and Digital Data Security Awareness Levels of University Students,” e-International Journal of Educational Research, vol. 12, no. 3, pp. 82–100, 2021, [Online]. Available: https://dergipark.org.tr/tr/doi/10.19160/e-ijer.950635

[13] E. Akman, Ö. İdil, and R. Çakır, “An Investigation into the Levels of Digital Parenting, Digital Literacy, and Digital Data Security Awareness among Parents and Teachers in Early Childhood Education,” Participatory Educational Research, vol. 10, no. 5, pp. 248–263, 2023, doi: 10.17275/per.23.85.10.5.

[14] A. Durak and H. Kaygin, “Parental mediation of young children’s internet use: Adaptation of parental mediation scale and review of parental mediation based on the demographic variables and digital data security awareness,” Education and Information Technologies, vol. 25, no. 3, pp. 2275–2296, 2020, doi: 10.1007/s10639-019-10079-1.

[15] N. Tarhan, “Digital Data Security Awareness: A Study with Pharmacy Students,” Fabad Journal of Pharmaceutical Sciences, vol. 47, no. 2, pp. 193–200, 2022, doi: 10.55262/fabadeczacilik.1134564.

[16] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos, and P. Kotzanikolaou, “Security awareness of the digital natives,” Information (Switzerland), vol. 8, no. 2, pp. 1–13, 2017, doi: 10.3390/info8020042.

[17] A. L. Fadhilah, Y. Ruldeviyani, R. Prakoso, and K. F. Arisya, “Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users,” IOP Conference Series: Materials Science and Engineering, vol. 1077, no. 1, p. 012003, 2021, doi: 10.1088/1757-899x/1077/1/012003.

[18] D. Banciu, M. Rădoi, and S. Belloiu, “Information security awareness in Romanian public administration: An exploratory case study,” Studies in Informatics and Control, vol. 29, no. 1, pp. 121–129, 2020, doi: 10.24846/v29i1y202012.

[19] A. Altunışık, R., Boz, H., Gegez, E., Koç, E., Sığrı, Ü., Yıldız, E., & Yüksel, “Sosyal bilimlerde araştırma yöntemleri: Yeni perspektifler,” Seçkin Yayıncılık, 2022.

[20] E. Yılmaz, Y. L. Şahin, and Y. Akbulut, “Development of the Digital Data Security Awareness Scale,” AJIT-e Online Academic Journal of Information Technology, pp. 23–40, 2015, doi: 10.5824/1309-1581.2015.4.002.x.

[21] R. B. Kline, “Principles and Practice of Structural Equation Modeling,” Guilford publications, 2023.

[22] K. Böke, “Sosyal Bilimlerde Araştırma,” Sosyal Bilimlerde Araştırma Yöntemleri, vol. 226, pp. 253–290, 2009.

[23] W. Ng, “Can we teach digital natives digital literacy?,” Computers and Education, vol. 59, no. 3, pp. 1065–1078, 2012, doi: 10.1016/j.compedu.2012.04.016.