Kastamonu Education Journal, 2025, Vol. 33, No:3, 535-546
doi: 10.24106/kefdergi.1748618

| Research Article / Araştırma Makalesi |

Investigation of University Students' Smartphone Security Measures Behaviors

Üniversite Öğrencilerinin Akıllı Telefon Güvenlik Önlemleri Davranışlarının İncelenmesi

Vildan ATEŞ[1]

Keywords

1. Smartphone
2. Security
3. Security measure behaviours
4. University students

Anahtar Kelimeler

1.Akıllı telefon
2.Güvenlik
3. Güvenlik önlemi davranışları
4.Üniversite öğrencileri

Received/Başvuru Tarihi
10.12.2024

Accepted / Kabul Tarihi
25.07.2025

Abstract

Purpose: This study aims to investigate the security measure behaviours of the 18-24 age group, which constitutes the majority of smartphone users, while using smartphones. In this study, in contrast to other studies, security measures and behaviours were examined through three approaches: protection by smartphone settings and add-on utilities, protection by avoiding harmful behaviours and applications, and protection by preventive behaviours and applications.

Design/Methodology/Approach: This research employs a quantitative methodology. One of the survey models used was the descriptive survey model. The data for this study were collected from 320 university students enrolled at four state universities in Ankara (Ankara University, Ankara Yıldırım Beyazıt University, Gazi University, and Middle East Technical University) during the fall term of the 2024-2025 academic year. The data collection tool for this study is a questionnaire comprising three sections. The questionnaire includes questions to collect demographic information and items for 17 smartphone security behaviours, presented in three categories. IBM SPSS 30.0 was used for data analysis. Data analysis obtained in this study, frequency, and percentage (%) from descriptive statistics were used.

Findings: The study’s findings indicate that the Android operating system is the most dominant among smartphone users. The study revealed that users don’t set their smartphones to remote data wipe in case of loss or theft, and that wireless connection areas are turned on when not in use. It was observed that users retain their usernames and passwords on their smartphones. Furthermore, the respondents indicated that they don’t utilize antivirus or security software on their phones and create backup copies of their data. It was noted that users don’t review license agreements or security messages when installing or using a new application. Conversely, users employ encryption and screen locks to safeguard the data on their devices. Users refrain from installing illegal or unauthorized software on their smartphones and don’t download attachments from unknown email addresses using their smartphones.

Highlights: Users need training and support on how to protect their smartphones with preventive behaviours and applications. They also need to be informed about phone settings and add-on utilities. On the other hand, users have appropriate security behaviours to protect their smartphones by avoiding harmful behaviours and applications.

Öz

Çalışmanın amacı: Bu çalışmanın amacı akıllı telefon kullanıcılarının önemli yüzdesini oluşturan 18-24 yaş grubunun akıllı telefon kullanırken gösterdikleri güvenlik önlemleri davranışlarını ortaya çıkarmaktır. Bu çalışmada diğer çalışmalardan farklı olarak güvenlik önlemleri davranışları akıllı telefon ayarları ve eklenti yardımcı programları ile koruma, zararlı davranış ve uygulamalardan kaçınarak koruma ve önleyici davranış ve uygulamalar ile koruma olmak üzere üç yaklaşımla incelenmiştir.

Materyal ve Yöntem: Bu araştırmanın yöntemi nicel araştırmadır. Tarama modellerinden biri olan betimsel tarama modeli kullanılmıştır. Araştırmanın verileri Ankara’daki dört devlet üniversitesinde (Ankara Üniversitesi, Ankara Yıldırım Beyazıt Üniversitesi, Gazi Üniversitesi ve Orta Doğu Teknik Üniversitesi) 2024-2025 öğretim yılı güz döneminde öğrenim gören 320 üniversite öğrencisinden toplanmıştır. Bu çalışmanın veri toplama aracı üç bölümden oluşan ankettir. Ankette demografik bilgileri toplamaya yönelik sorular ile üç yaklaşım ile düzenlenmiş 17 akıllı telefon güvenlik davranışı için maddeler bulunmaktadır. Verilerin analizi için IBM SPSS 30.0 programı kullanılmıştır. Bu çalışmada elde edilen verilerin analizinde betimsel istatistiklerden sıklık (frekans) ve yüzde (%) kullanılmıştır.

Bulgular: Bu çalışma sonucunda Android’in, kullanıcıların akıllı telefonlarında kullandıkları en popüler işletim sistemi olduğu görülmüştür. Çalışmada kullanıcıların akıllı telefonunlarının kaybolması veya çalınması durumunda uzaktan veri silme işlemine ayarlı olmadığı ve kullanmadıkları zamanlarda kablosuz bağlantı alanlarının açık olduğu görülmüştür. Kullanıcılar akıllı telefonlarında kullanıcı adlarını ve şifrelerini akıllı telefonlarında saklamaktadır. Ayrıca antivirüs ya da güvenlik yazılımları telefonlarında yüklü olmayıp telefonlarının yedek kopyasını da almadıklarını belirtmişlerdir. Kullanıcıların akıllı telefonlarına yeni bir uygulama yüklerken veya kullanırken lisans sözleşmelerini ve güvenlik mesajlarını okumadıkları da görülmüştür. Diğer taraftan kullanıcılar telefonlarındaki verileri korumak için şifreleme ve ekran kilidi kullanmaktadırlar. Kullanıcılar akıllı telefonlarına yasadışı veya izinsiz yazılım yüklememekte ve akıllı telefonları ile bilinmeyen e-postalardaki ekleri de indirmemektedirler.

Önemli Vurgular: Kullanıcıların önleyici davranış ve uygulamalar ile akıllı telefonlarını nasıl koruyacakları konusunda eğitim ve desteğe ihtiyaçları olduğu görülmüştür. Aynı şekilde telefon ayarları ve eklenti yardımcı programları hakkında da bilgilendirilmeleri gerekmektedir. Diğer taraftan kullanıcılar zararlı davranış ve uygulamalardan kaçınarak akıllı telefonlarını korumaya yönelik güvenlik davranışları uygun biçimdedir.

[1] **Corresponded Author**, Ankara Yıldırım Beyazıt University Business School Department of Management Information Systems , Ankara Yıldırım Beyazıt University , Ankara, Türkiye; https://orcid.org/0000-0002-8855-8556

Citation/Alıntı: Ateş, V. (2025). Investigation of University Students' Smartphone Security Measures Behaviors, *Kastamonu Education Journal,33* (3), 535-546. doi: 10.24106/kefdergi.1748618

INTRODUCTION

Mobile technologies have led to the emergence of a new type of device, the programable mobile phone or smartphone. The smartphone is a radical device that has features that are not traditionally associated with phones, such as an operating system, web browsing, and the ability to run software applications and integrates a computer that can simplify any task with just a few clicks. Moreover, smartphones combine an integrated computer and a mixture of other features that make them exceptionally capable, such as web browsing and operating systems.

Users are increasingly storing personal information, such as transactions on e-commerce, finance, and social media platforms, on smartphones. Attackers have primarily focused on mobile applications over the past decade (Alkindi, Sarrab, and Alzeidi, 2021). The first mobile malware, Cabir, was discovered in the Symbian mobile operating system in 2004. Since then, there has been a steady increase in the amount of malware in the mobile market (Goni et al., 2021).

Since 2008, the smartphone industry has been steadily growing and expanding in terms of market size, number of models, and vendors. By the end of 2023, nearly 70% of the world's population was smartphone users (Laricchia, 2024). In the top 10 more developed countries, about three-quarters of the population own a smartphone, and globally, nearly 90% of mobile phones are smartphones. The unprecedented growth in demand for the smartphone market over the past decade has paved the way for increased use of smartphones for personal and official communication, gaming, and online shopping. Additionally, approximately 92.3% of internet users access the internet using a mobile phone (Howarth, 2024). There are over 7.2 billion smartphones worldwide, and it is expected to grow in the future. The smartphone market also grows significantly, by 7.8%, in the first quarter of 2024 (Howarth, 2024). In Turkey, the number of smartphone users has also been increasing, exceeding 80 million as of 2023, and is expected to reach approximately 88 million by 2028 (Dierks, 2023).

Smartphones have become an indispensable part of modern life. Users can program any customized application to suit their needs and share these applications online. Therefore, smartphones and related applications have become the most popular keywords in mobile technology. The mobility, portability, and increasing smartphone capabilities have significantly contributed to the increasing popularity of multipurpose devices. As smartphones begin to replace personal computers due to their advanced features and ease of use, most users' sensitive data, including emails, photos, and videos, are now stored and processed on smartphones. For example, during the COVID-19 pandemic, smartphones and other mobile devices were routinely used for data storage and interactions, including in healthcare (Farshidfar & Hamedani, 2020; Ganesh et al., 2020; Sansom-Daly & Bradford, 2020) and telehealth services (Chin, Jones & Little, 2021).

While cyberattacks have traditionally been primarily targeted at computers and servers, smartphones have increasingly become the target of cybercriminals who seek to steal personal or corporate data. The increase in the functionality and adoption of smartphones has made these devices attractive targets for cybercriminals. The device and the vast amount of information contained constitute a valuable target for attack (Parker et al., 2015). The increase in remote work, especially during the COVID-19 pandemic, the use of smartphones to access company systems and software, and the growth in mobile commerce have led to a significant increase in threats. These activities using smartphones have allowed cybercriminals to gain access to smart devices (Wasserman, 2022). Considering the rapidly increasing storage capacity of devices and the ability to store more personal data (such as photos and videos), the threat of data theft is also increasing (Allam, Flowerday & Flowerday, 2014). In addition, targeted theft of data stored on or shared online through smartphones is a concern (Chin, Jones & Little, 2021; Das & Khan, 2016). Therefore, smartphone users must implement security measures to protect against threats from potential criminals or user negligence (Parker et al., 2015).

Malware and data leakage are the most prominent threats faced by smartphone users. However, it has been observed that smartphone users have a habit of ignoring the security messages they receive (Mylonas, Kastania & Gritzalis, 2013). This is a security vulnerability that jeopardizes smartphone security. Additionally, users rarely consider privacy and security when downloading new applications and do not adequately protect themselves by implementing smartphone protection mechanisms (Ophoff & Robinson, 2014). This is true even for younger, tech-savvy generations who have early access to mobile devices. Studies on students have revealed that they do not pay significant attention to smartphone protection mechanisms (Park & Drevin, 2016).

The fundamental issue is that users are unaware that smartphones require the same security and protection as computers (Lawton, 2008). This primarily increases security concerns and reveals the need to understand whether smartphone users are aware of security issues related to smartphone use. In other words, understanding user behaviour related to information security in smartphone usage has become increasingly critical. Additionally, to establish an effective and secure mobile ecosystem, it is necessary to understand user behaviour related to smartphone security and privacy This study aims to investigate the security measures behaviour of university students aged 18-24 in using smartphones.

The research question for this study is as follows:

1) What are the smartphone security measure behaviours of university students?

This study reveals the security measures behaviours of the 18-24 age group, which constitutes the largest percentage of smartphone owners. In addition, this study examines security measures behaviours through three different approaches, which is different from other studies. This study is expected to make valuable contributions to the Turkish literature by revealing the basic security behaviours of smartphone users. Furthermore, the study is important because it will assess the awareness level of young people regarding smartphone security and identify areas that need to be focused on.

This study is organized into five sections. The first section introduces the research topic, providing essential background information and highlighting its significance, and research question. The second section offers a comprehensive literature review, summarizing key studies and identifying gaps this research aims to address. The third section details the research methodology, participants, data collection tool, and process employed. The fourth section presents the findings of the study. Finally, the fifth section concludes the study with a summary of the key insights and offers recommendations for future research and practical applications.

LITERATURE REVIEW

Smartphones have recently become a significant target for cybercriminals due to the large amount of sensitive data and user credentials stored on such devices (Knapova et al., 2021). Users can also apply various security behaviors to protect themselves from cyber threats. While smartphone companies offer various security tools such as encryption, firewalls, antivirus, and malware prevention that can lower the risk of security breaches in smartphone networks, multiple studies have shown that smartphone users do not adopt these Technologies (Egan et al., 2012; Lazou & Weir, 2011). Furthermore, an insecure smartphone device not only jeopardizes the security of personal data but can also put the company's information assets at risk. Therefore, employees using personal smartphones at work pose a greater risk to the company's information security (Egan et al., 2012).

A study by Androulidakis and Kandus (2011) that investigated mobile phone students' security awareness in Budapest showed that only 12.3% of users used antivirus software, and only 24.5% of students had a password on their phones. Similar results were also presented in a study by Ophoff (2014). Among the participants, 97% used security software on their computers, whereas only 27% used security software on their smartphones. The results also demonstrated that only half of the users who believed security software was necessary had it installed on their devices.

A study conducted in China also highlighted that security information is often ignored during the downloading and use of applications in smartphone usage, auxiliary programs are inappropriately enabled, and appropriate disaster recovery plans are lacking on smartphones, indicating serious concerns about information security (Zhang, Li, & Deng, 2017). Another study reported a lack of awareness among smartphone users about the security and privacy risks associated with downloaded smartphone applications. Most participants assumed controlled application marketplaces (e.g., Google Play) were secure. In addition, more than 65% of participants engaged in risky behavior by allowing free applications to access their data (Mylonas, Kastania, & Gritzalis, 2013). A related study revealed that although the majority of users had configured appropriate screen lock settings to prevent unauthorized physical access to their smartphones, they largely neglected other critical security practices, such as utilizing virtual private networks (VPNs) when accessing public Wi-Fi networks or disabling unused features on their devices (Breitinger, Tully-Doyle, & Hassenfeldt, 2020). A study conducted in India also examined the usage patterns of smartphone users and investigated whether general security concerns existed among such users. The most notable finding was that, despite possessing knowledge about various security threats, participants seldom implemented protective measures for their devices. Additionally, they appeared to lack awareness of technical security mechanisms such as data encryption and remote wipe functionalities (Shah & Agarwal, 2020). Another study in India reported a deep understanding of users' awareness regarding smartphone security. However, users are concerned about data stored on their smartphones because they believe smartphones are not as secure as computers. In addition, users reported installing pirated software on their smartphones rather than purchasing applications from official app stores (Bagga et al., 2017). A study conducted in Greece by Stylios et al. (2016) also demonstrated that although many smartphone users implemented some security measures, most users ignored security and privacy risks.

A study conducted in Turkey on this topic was conducted by Koyuncu and Pusatlı in 2019. This study investigated the awareness levels of smartphone users regarding different security parameters and compared the awareness levels of user groups categorized by demographic data (Koyuncu & Pusatlı, 2019). Another study examined university students' mobile application security awareness (Talan et al., 2015). In a more recent study, Erdoğan and Coşar (2024) investigated the cybersecurity awareness of teachers when installing a mobile application. The research results revealed that the awareness level of teachers regarding security vulnerabilities in mobile applications was 79.7% (Erdoğan & Coşar, 2024). In conclusion, studies reporting different results have been conducted in this area.

A review of the literature shows that recent research has largely focused on computer and cybersecurity threats (Abdullahi et al., 2022; Basholli, Mezini & Basholli, 2023; Dolan & Widayanti, 2022, Kaur & Ramkumar, 2022; Nadeem et al., 2023; Prakash, Anoop & Asharaf, 2022; Taherdoost, 2022). These studies have addressed technical topics such as blockchain, cloud computing, artificial intelligence, and machine learning. On the other hand, while increasing a user's knowledge can improve their compliance with security practices, educators need a complete understanding of users' current behaviours, misconceptions, and general attitudes toward smartphone security. In this study, the security measures behaviours of university students aged 18-24 in using smartphones will be examined under three approaches.

METHOD

This section presents the study's research method, participants, data collection tool, and data collection process.

Research Method

This study employed a quantitative research methodology. This study is descriptive research, and its model is a survey. The descriptive survey model was selected for two primary reasons. First, it enables collecting many participants, which is a significant advantage. Second, it allows for analyzing individuals' views and attitudes toward a phenomenon or event, along with the description of the phenomenon or event itself. In other words, this model provides the ability to explore different aspects of a topic and understand complex issues.

Participants

The study group for this research comprises university students aged 18-24. There are two reasons for selecting this age group. First, they are enthusiastic about and easily adopt smartphone technologies (Fidan, 2019; Jones & Chin, 2015). The second reason is that users in this age group comprise the largest percentage (48%) of smartphone owners (Pew Research Center, 2022). When selecting university students who will participate in the research, the convenience and criterion sampling methods, which are non-random sampling methods, were used. Convenience sampling was preferred because it provides access to participants who can contribute to the research quickly and easily. Criterion sampling was also used to ensure that participants who met the criteria for the study were selected. Criteria for this research are that the participants must be university students between 18 and 24 years old and have been using a smartphone for at least 1 year. The study's data was collected from 320 university students enrolled at four state universities in Ankara (Ankara University, Ankara Yıldırım Beyazıt University, Gazi University, and Middle East Technical University) during the fall semester of the 2024-2025 academic year.

Data Collection Tool

The data collection tool used in this study was a questionnaire consisting of three sections. The first section provides information about the purpose, importance, and details of the questionnaire to the participants. The second section includes five questions to collect participants' demographic information (gender, age, grade, university, faculty) and two questions to determine their smartphone operating system and the duration of their internet use. The third section contains items related to 17 smartphone security behaviors (Harris, Patten & Regan, 2013). The necessary permissions were obtained by emailing the researchers regarding the questionnaire items' usage. The draft questionnaire was submitted to the opinions of three experts, and the English-Turkish translations were checked. Then, the Turkish comprehensibility of the questionnaire items was sent to a field expert, and feedback from the experts was applied to finalize the questionnaire items. The pilot questionnaire test was conducted with five university students. Because of these processes, a final version of the questionnaire was created. The questionnaire contains 24 questions.

The questionnaire items were organized according to three approaches proposed by Jones and Heinrichs (2012). These approaches include protection through smartphone settings and auxiliary applications, avoidance of harmful behaviors and applications, and protection through preventive behaviors and applications. Participants were asked to select the most appropriate option (always, often, sometimes, rarely, and never) for each behavior. These three approaches and the recommended security behaviors for smartphones are summarized in Table 1.

Table 1. Approaches and recommended security behaviours for smartphones

Approach	Code	Security Behaviours
Protection with phone settings and add-on utilities	PP1	My smartphone is set up for remote data wipes in case of loss or theft.
	PP2	I use encryption to protect data on my smartphone.
	PP3	The Bluetooth on my smartphone is turned on when not in use.
	PP4	I use a screen lock on my smartphone.
	PP5	My smartphone’s wireless connection (Wi-Fi) is turned on when not in use.
Avoiding of harmful behaviours and applications	AH1	I install illegal or unauthorized software on my smartphone.
	AH2	I install software from trusted sources on my smartphone.
	AH3	I connect my smartphone to an unsecured free wireless network (Wi-Fi).
	AH4	I avoid clicking on unknown links on my smartphone.
	AH5	I download attachments from unknown emails on my smartphone.
Protection through preventive behaviours and applications	PB1	I promptly install software updates on my smartphone.
	PB2	I store my usernames and passwords on my smartphone.
	PB3	I always read license agreements when installing a new application on my smartphone.
	PB4	I always read security messages when installing or using an application on my smartphone.
	PB5	I create backup copies of the data on my smartphone.
	PB6	I have antivirus protection installed on my smartphone.
	PB7	I have firewall software installed to protect my smartphone.

As shown in Table 1, a total of 17 recommended security behaviors are categorized under three smartphone usage approaches. These behaviors are widely recognized as fundamental practices for mitigating potential information security risks faced by smartphone users.

Data Collection

Before data collection, approval was obtained from the Ankara Yıldırım Beyazıt University’s Social and Humanities Ethics Committee (dated November 22, 2023, and numbered 09-216) confirming that the study was ethically appropriate. Participants were provided with two options for participation: digital or in print format. The digital version of the data collection tool was prepared using Google Forms. 320 students participated in the study, 194 completed the digital version, and 126 preferred the printed format. The researcher conducted data collection between September 22 and October 23, 2024.

Data Analysis

The IBM SPSS Statistics 30.0 software was used for data analysis. Descriptive analysis was used to analyze data. Descriptive analysis summarizes data clearly and concisely, enabling researchers to understand the dataset’s patterns, trends, and distributions and gain insights. Descriptive analysis was preferred because the dataset provides basic information about the variables and describes the distribution of each variable related to smartphone users’ behaviors (Worgotter, 2011). Data analysis obtained in this study, frequency, and percentage values (%) were used, indicating how often the data occurred.

FINDINGS

This section comprises two subsections. The first subsection presents the participants’ demographic information, including gender, age, grade, university, and faculty, along with findings related to smartphone operating systems and daily smartphone usage times. The second subsection presents the descriptive analyses of the data collected on the 17 smartphone security behaviours of the participants.

Demographic Information About the Participants

Participants’ demographic information regarding age, university, faculty, and grade is presented in Table 2.

Table 2. Participants demographic information

Age	Frequency	%	Faculty	Frequency	%
18-20	131	41	Business	207	64
21-23	144	45	Education	105	33
24-26	45	14	Arts	8	3

University	Frequency	%	Study year	Frequency	%
Ankara	92	29	First-year	38	12
Ankara Yıldırım Beyazıt	115	36	Second-year	66	21
Gazi	105	32	Third-year	81	25
Middle East Technical	8	3	Fourth-year	135	42

A review of the participants' gender data revealed that 214 participants were female and 106 were male. When Table 2 is analyzed, it is also seen that most participants (86%) are between 18 and 23 years old. When the university distribution of the participants is examined, there are almost equal proportions of participants from the three state universities, while only 8 participants are from METU. In the same direction, most participants (64%) were business administration faculty students, and the remaining participants (33%) were education faculty students. Additionally, an analysis of the participants' study years revealed that most of them (67%) were in their third or fourth year of study. The participants were asked about the operating system that they used on their smartphones. Android was the most popular operating system (OS) (181 participants, 58%) used on the participants' smartphones. The second most used operating system was Apple iOS, with 131 participants (41%). It was observed that only two participants utilized disparate operating systems. One participant reported using Windows Mobile, while the other participant used Harmony. The final question asked the participants in this section concerned their daily smartphone usage. The responses to this question are presented in Table 3.

Table 3. Daily smartphone usage

Duration (hour)	Frequency	%
0-1	3	1
1-2	10	3
2-3	41	13
3-4	82	26
4-5	80	25
5-6	67	21
More than 6	37	11
Toplam	320	100

Table 3 illustrates that 162 participants (51%) used their smartphones for between 3 and 5 hours per day, and 104 participants (32%) engaged for more than five hours daily.

Findings on Participants' Smartphone Security Behaviours

In this subsection, the security behavior questions related to smartphone security are grouped and presented according to the three approaches (protection through smartphone settings and add-on utilities, avoidance of harmful behaviours and applications, and protection through preventive behaviours and applications). The frequency and percentage values obtained for each security behavior are also provided.

The first approach is to protect smartphones through phone settings and add-on utilities and includes five security behaviours. Table 4 presents these five security behaviours and the frequency and percentage values of the participant responses to each behavior.

Table 4. Frequency and percentage values of participants' security behaviours with phone settings and add-on utilities

Security Behaviour	Never	Rarely	Sometimes	Often	Always
My smartphone is set up for remote data wipes in case of loss or theft.	**145** **%45**	**54** **%17**	36 %11	26 %8	59 %19
I use encryption to protect data on my smartphone.	10 %3	16 %5	26 %8	71 %22	**196** **%62**
The Bluetooth on my smartphone is turned on when not in use.	**120** **%38**	69 %21	38 %12	44 %14	49 %15
I use a screen lock on my smartphone.	10 %3	3 %1	14 %4	32 %10	**261** **%82**
My smartphone's wireless connection (Wi-Fi) is turned on when not in use.	60 %19	50 %16	52 %16	**71** **%22**	**87** **%27**

Table 4 reveals that 62% of participants didn't enable remote data wipes in the event of smartphone loss or theft. On the other hand, another security behavior with the same percentage was that the participants used encryption to protect the data on their smartphones. The majority of respondents (82%) also use a screen lock. When not in use, 38% of the participants had their Bluetooth turned off on their smartphones, while 49% of participants often or always had their wireless connection turned on.

The second approach involves protecting smartphones by avoiding harmful behaviours and applications. In this approach, the participants were asked about five security behaviours. Their responses are presented in Table 5.

Table 5. Frequency and percentage values of participants' security behaviours by avoiding harmful behaviours and applications

Security Behaviour	Never	Rarely	Sometimes	Often	Always
I install illegal or unauthorized software on my smartphone.	**219** **%68**	48 %15	29 %9	16 %5	8 %3
I install software from trusted sources on my smartphone.	35 %11	19 %6	39 %12	**126** **%39**	**101** **%32**
I connect my smartphone to unsecured free wireless networks (Wi-Fi).	**104** **%33**	**69** **%22**	80 %25	42 %13	25 %7
I avoid clicking on unknown links on my smartphone.	5 %2	21 %7	31 %10	**89** **%27**	**174** **%54**
I download attachments from unknown emails on my smartphone.	**172** **%54**	70 %22	34 %10	15 %5	29 %9

As shown in Table 5, most participants (68%) did not install illegal or unauthorized software on their smartphones. Consistent with this finding, most participants (71%) installed software from trusted sources. It was observed that 55% of the participants never or rarely connected to unsecured wireless networks, whereas 25% sometimes did. In contrast, 20% of them frequently connect or always. Table 5 shows that most participants (81%) often or always avoid clicking on unknown links. Similarly, half of the participants stated that they didn't download attachments from unknown emails using their smartphones.

Table 6. Frequency and percentage values of participants' security behaviours with preventive behaviours and applications

Security Behaviour	Never	Rarely	Sometimes	Often	Always
I promptly install software updates on my smartphone.	11 %3	39 %12	101 %32	**98** **%31**	**71** **%22**
I store my usernames and passwords on my smartphone.	45 %14	52 %16	79 %25	**74** **%23**	**70** **%22**
I always read license agreements when installing a new application on my smartphone.	**123** **%38**	**89** **%28**	66 %21	25 %8	17 %5
I always read security messages when installing or using an application on my smartphone.	**55** **%18**	**81** **%25**	81 %25	61 %19	42 %13
I create backup copies of the data on my smartphone.	24 %7	61 %19	101 %32	81 %25	**53** **%17**
I have antivirus protection installed on my smartphone.	**87** **%27**	**61** **%19**	56 %18	49 %15	67 %21
I have firewall software installed to protect my smartphone.	**83** **%26**	**71** **%22**	53 %17	51 %16	62 %19

In this section, the initial security behavior is the on-time installation of software updates. 32% of participants indicated that they occasionally install software updates on time, whereas 53% of participants stated that they frequently or consistently install software updates on their smartphones on time. Furthermore, 45% of the participants stored their usernames and passwords on their smartphones. The remaining two security behaviors pertain to the antivirus and security software installed on the respondents' smartphones. It was noted that 46% of participants didn't have an antivirus program installed on their smartphones. In a similar proportion, 48% of participants indicated that they didn't install firewall software on their smartphones. As shown in Table 6, only 21% of participants had antivirus software installed, while 19% had firewall software installed. Additionally, only 17% of participants regularly created backup copies of the data on their smartphones.

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

This study presents the security measures observed in the smartphone usage behaviors of Turkish university students aged 18 to 24. In contrast to existing studies, this study classified 17 security behaviours under three approaches to examine.

The results of this study indicate that Android is the most prevalent operating system among the participants in terms of smartphone use. In addition, the study revealed that users don't read license agreements when installing new applications on their smartphones and do not read security messages when installing or using an application. On the other hand, the open-source nature of the Android platform allows developers to modify software, creating innovative and new applications. Additionally, developers can quickly bring apps to market with the help of the platform's readily available tools and efficient review process. However, users should still act with caution and carefully assess the developer's background. Furthermore, they should perform a detailed review of the application to ensure appropriateness, adherence to software development standards, and the absence of malicious code. In addition, Android users have access to numerous markets with disparate levels of security, which can present significant security risks without comprehensive awareness and training. It is recommended that users download apps from official channels, such as the Apple App Store, Google Play, and Amazon App Store. Although applications on these marketplaces are not 100% secure, they undergo a degree of screening and are filtered. Users should examine the applications' permissions they use and exercise caution before granting access, particularly when it comes to high-risk permissions, such as accessibility services.

Another challenge with the Android platform is the large number of operators and vendors that do not adopt a consistent standard, which results in the continued availability of the operating system's older versions. On the other hand, 41% of respondents indicated that they use Apple's iOS. In contrast to the Android operating system, the Apple iOS is a closed operating system managed by Apple. Only one manufacturer produces devices for the platform, and there is no OS fragmentation (Mansfield-Devine, 2012). Updating these devices is straightforward and encouraged by Apple, which is one reason why the operating systems of Apple devices are more up-to-date than those of Android devices, providing a higher level of security. It is important to note that there has been an increase in the incidence of advanced persistent threats (APT), side-channel attacks, sensor-based attacks, and attacks launched through the Google Play Store (Muhammed et al., 2023).

In the initial approach, an investigation was conducted into the security behaviours exhibited by users to safeguard their smartphones, with a specific focus on the use of phone settings and additional utilities. Upon examination of these behaviors, we found that users employed encryption and screen locks to safeguard data stored on their smartphones. It can be concluded that they demonstrate a high level of awareness regarding these two behaviors. Another encouraging observation is that most users disable Bluetooth on their smartphones when they are not in use. It is also noteworthy that two behaviours were observed that could compromise the security of the devices. The wireless connections were left enabled when the devices were not in use, and remote data wiping was not employed in the event of a lost or stolen smartphone. To prevent unintended connections to unsecured public wireless networks, users are recommended to disable the auto-join function and to connect only to secure wireless networks. In addition, users should avoid financial transactions or accessing social network accounts on insecure networks via public wireless connections. In addition, the most effective way to protect credentials (passwords, credit card details, etc.) is to enter them only on a secure network. It is also recommended to enable a firewall on a user's smartphone. Although a firewall is not a prerequisite for a secure connection, its activation when a public wireless network is used provides a crucial layer of protection against cyber threats. If a device is lost or stolen, data-wiping software can be used to delete sensitive data from the device. This deletes all personal information and eliminates the risk of data access, thus helping to minimize the risk of data theft. However, users should assume that all smartphone data has been leaked and take appropriate reactive measures.

The second approach examined user security behaviors to protect smartphones by avoiding harmful behaviors and applications. It is found that users did not install illegal or unauthorized software on their smartphones. Instead, they install software from trusted sources. Similarly, it can be concluded that users never connect to unsecured wireless networks. They also avoid clicking on unknown links on their smartphones. Furthermore, the participants did not download attachments from unknown emails using their smartphones. It is recommended that smartphone users avoid connecting to free wireless networks whenever possible. Furthermore, once connected, it is crucial to avoid performing financial transactions without a virtual private network (VPN). The five security behaviours described in this approach were observed to be performed appropriately by the users. It was observed that all five security behaviours in this approach were performed appropriately by the users. It was determined that users have a positive attitude toward this approach regarding these security behaviours.

The third approach is users' security behaviors in protecting their smartphones through preventive behaviors and applications. Initially, it was observed that users install software updates for their smartphones on time. The operating system and crucial applications must be updated immediately as new updates become available for the smartphone. It is also noteworthy that installing the latest software version can fix most security issues. It has been observed that users do not read license agreements when installing a new application on their smartphones and do not read security messages when installing or using an application. Users neglect to read license agreements or messages during the app installation process and are unaware of the terms and conditions to which they agree. However, some applications can affect user privacy, request the installation of other apps, or even change a device's OS settings, and such actions must be performed legally. The results of a survey conducted by Kaspersky revealed that nearly half of the respondents may be at risk due to the applications installed on their mobile devices. This is because users are not sufficiently knowledgeable about cybersecurity to restrict the permissions granted to applications during installation. A total of 15% of respondents indicated that they never limited the capabilities of applications installed on their mobile devices. In addition, 17% of respondents reported that they granted permissions to applications when prompted and subsequently forgot to alter these permissions. Furthermore, 11% of respondents believed they could not modify these permissions. Without restrictions on application permissions, apps can access personal and private data on mobile devices, including contact information, photos, and location data (Kanali, 2016). Therefore, it is crucial to read the license agreement when installing software. The list of permissions requested by an application should be carefully reviewed, and installation should not proceed without checking and understanding what is accepted during installation.

Another behavior in this approach is that users store usernames and passwords on their smartphones. The main risk associated with storing usernames and passwords in notes is that unwanted parties can access this information. In general, writing down passwords anywhere, especially on a cell phone, can compromise the security and privacy of such accounts. Usernames and passwords are the keys to digital life. They protect personal and professional data, online accounts, and user identities. Therefore, it is advisable to use a password manager. A password manager is an application that securely stores and encrypts your passwords and automatically fills them in when you log in to a website or application.

The other two security behaviours in this section were associated with the antivirus and security software installed on the participants' smartphones. Almost half of the users did not install antivirus or firewall software on their smartphones. Harris, Patten, and Regan (2013) also highlighted in their study of university students that only 27% of users had antivirus software installed on their smartphones. Android operating systems are more susceptible to malware infections. One antivirus company estimates that over 4% of Android devices are infected with malware (Troung et al., 2014). Kaspersky reported a consistent increase in the number of attacks on mobile devices in 2023, reaching almost 33.8 million attacks, representing a 50% increase compared to the previous year's figures (Kaspersky, 2024). A further study was conducted in the United States with 2337 participants, the findings of which indicated that 70% of smartphone owners believed their devices to be secure from hackers, malware, and other forms of cybercrime (InfoSecurity, 2012). Despite the robust security measures inherent to mobile operating systems such as Android and iOS, these platforms remain susceptible to potential threats. Antivirus applications provide an additional layer of protection against malware, phishing attacks, and other cyber threats that have the potential to compromise personal data, privacy, and device performance. Moreover, as the prevalence of mobile devices continues to grow, so too does the number of individuals targeted by hackers. Anti-virus applications can scan for suspicious activity, block malicious websites, and assist users in locating lost or stolen phones. The installation of security software provides users with a valuable layer of protection, thereby enhancing the overall security and stability of their mobile experience. In addition, previous studies have revealed that most users do not create backup copies of data stored on their smartphones. As smartphones are becoming as powerful as computers, it is critical to apply the same security principles to computer-related devices. Therefore, users aged 18-24 should be more aware of smartphone device security. In addition, malware has become the most significant threat to smartphones. Therefore, a device must be up-to-date and protected against malware attacks.

The results of this study are important for businesses because these students may have already joined the workforce with their smartphones or will do so shortly. As these devices will connect to corporate networks, companies must consider them as part of their network. Security awareness and training should cover mobile devices such as smartphones, PCs, and other security threats to the organization. In addition, smartphones have increased so rapidly that many people do not know how to properly secure such devices, as evidenced by the university students who participated in this study. One solution to this problem is for businesses to create smartphone security awareness and training and provide it to all new and existing employees at least annually. Such training would inform users about free or inexpensive antivirus, firewall, and data-wiping software. Users will also be informed about malware and third-party marketplaces. Although smartphone security awareness and training are only one part of maximizing information security, it has become too important to ignore.

It should be noted that the study was conducted with a limited sample size, comprising students from only three state universities. This may be considered a potential limitation of the study. A further limitation is that the study focuses on only 17 security behaviors at the basic level. In future studies, researchers could consider conducting interviews with different age groups. In addition, the number of safety behaviors could be increased. Studies can be carried out with private university students in private universities to make comparisons with the results of this study.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, author-ship, and/or publication of this article.

Statements of publication ethics

I hereby declare that the study has not unethical issues and that research and publication ethics have been observed carefully.

Author contributions

V.A. conceived the research idea by reviewing the literature and developing the research question, collected the data. V.A. analyzed the data organized the manuscript and wrote the final manuscript.

Ethics Committee Approval Information

The study’s approval was obtained from the Social and Humanities Ethics Committee of Ankara Yıldırım Beyazıt University (dated November 22, 2023, and numbered 09-216) confirming that the study was ethically appropriate.

REFERENCES

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56-65.

Androulidakis, I., & Kandus, G. (2011). Mobile phone brand categorization vs. users' security practices. *Engineering, Technology & Applied Science Research*, *1*(2), 30-35.

Alkindi, Z.R., Sarrab, M. and Alzeidi, N. (2021). User privacy and data flow control for android apps: a systematic literature review. *Journal of Cyber Security and Mobility*, *10*, 261-304. https://doi.org/10.13052/jcsm2245-1439.1019.

Bagga, T., Sodhi, J., Shukla, B., & Qazi, M. (2017). Smartphone security behaviour of the Indian smartphone user. *Man In India*, *97*(24), 333-344.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security*, *88*, 101647.

Chin, A., Jones, B., & Little, P. (2021). A comparative analysis of smartphone security behaviours and practices. *International Journal of Education and Development using Information and Communication Technology*, *17*(3), 57-80.

Das, A., & Khan, H. U. (2016). Security behaviours of smartphone users. *Information & Computer Security*, *24*(1), 116-134.

Dierks, Z. (2023). Forecast of the smartphone user penetration rate in Turkey 2018-2024. https://www.statista.com/statistics/568281/predicted-smartphone-user-penetration-rate-in-turkey/#:~:text=Smartphone%20usage%20in%20Turkey,million%20smartphone%20users%20in%20Turkey, Erişim Tarihi: 07.11.2024.

Egan, G., Haley, K., Mckinney, D., Millington, T., Mulcahy, J., Parsons, T., … Hittel, S. (2012). *Internet security threat report*. Technical Report. April.

ENISA: European Union Agency for Network and Information Security (2010). Smartphone security: information security risks, opportunities and recommendations for users. http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport, Erişim Tarihi: 10.11.2024.

Erdoğan, E., & Coşar, M. (2024). Akıllı telefon uygulamalarının kullanıcı bazlı siber güvenlik farkındalığı. *Journal of Management Theory and Practices Research, 5*(1), 15-33.

Farshidfar, N., & Hamedani, S. (2020). The potential role of smartphone-based microfluidic systems for rapid detection of COVID-19 using saliva specimen. *Molecular Diagnosis & Therapy*, *24*(4), 371-373.

FCC: Federal Communications Commission (2015). FCC Smartphone security checker. https://www.fcc.gov/smartphone-security, Erişim Tarihi: 15.11.2024.

Fidan, M. (2019), Development of a scale for university students Facebook use purposes and an examination in terms of their Facebook use profiles. *International Journal of Education and Development using Information and Communication Technology, 15*(4), 132-150.

Ganesh, A., Sahu, P., Nair, S., & Chand, P. (2020). A smartphone-based e-consult in addiction medicine: An initiative in COVID lockdown. *Asian Journal of Psychiatry*, *51*, 102120.

Goni, I., Gumpy, J.M., Maigari, T.U. & Mohammad, M. (2020). Cybersecurity and cyber forensics: machine learning approach systematic review. *Semiconductor Science and Information Devices, 2,* 25-29. https://doi.org/10.30564/ssid.v2i2.2495.

Harris, M. A., Patten, K., & Regan, E. (2013). *The need for BYOD mobile device security awareness and training*. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, USA.

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, *21*(5), 381-400.

Howarth, J. (2024). How Many People Own Smartphones? (2024-2029). https://explodingtopics.com/blog/smartphone-stats, Erişim Tarihi: 10.11.2024.

InfoSecurity, 2012. Most users have not installed security software on their smartphones, survey finds. https://www.infosecurity-magazine.com/news/most-users-have-not-installed-security-software/, Erişim Tarihi: 15.11.2024.

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management*, *35*(5), 561-571.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53*, (2), 22-30.

Kanali, N. (2016). 63% of consumers globally don't license agreement when installing new apps on their devices. https://techtrendske.co.ke/2016/05/05/63-of-consumers-globally-dont-license-agreement-when-installing-new-apps-on-their-devices/, Erişim Tarihi: 20.11.2024.

Kaspersky. (2024). Attacks on mobile devices significantly increase in 2023. https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023, Erişim Tarihi: 20.11.2024.

Kim, H. (2017). Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. *Restorative Dentistry & Endodontics, 42*, 152-155.

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, 1-11.

Knapova, L., Kruzikova, A., Dedkova, L., & Smahel, D. (2021). Who Is smart with their smartphones? Determinants of smartphone security behaviour. *Cyberpsychology, Behaviour, and Social Networking, 24*(9), 584-592.

Laricchia, F. (2024). Smartphones - statistics & facts. https://www.statista.com/topics/840/smartphones/#topicOverview, Erişim Tarihi: 20.11.2024.

Lawton, G. (2008). Is it finally time to worry about mobile malware? *Computer, 41*(5):1214.

Lazou, A., & Weir, G. R. (2011). Perceived risk and sensitive data on mobile devices. *Cyberforensics: Issue and Perspectives*, 183–196.

Mansfield-Devine, S. (2012). Paranoid Android: just how insecure is the most popular mobile platform? *Network Security*, *2012*(9), 5-10.

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal Of Information Security And Applications*, *20*, 84-89.

Muhammad, Z., Anwar, Z., Javed, A. R., Saleem, B., Abbas, S., & Gadekallu, T. R. (2023). Smartphone security and privacy: a survey on apts, sensor-based attacks, side-channel attacks, Google Play attacks, and defenses. *Technologies*, *11*(3), 76.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

Ophoff, J., & Robinson, M. (2014, August). *Exploring end-user smartphone security awareness within a South African context*. In 2014 Information Security for South Africa, South Africa.

Park, M. J. (2016). *Mobile device security: Young people's awareness and perceptions* [Doctoral Dissertation Potchefstroom Campus of the North-West University South Africa]. Boloka, the open-access Institutional Repository. https://repository.nwu.ac.za/handle/10394/19863.

Park, M. & Drevin, L. (2016). An investigation into the security behaviour of tertiary students regarding mobile device security. CONF-IRM 2016 Proceedings, 63. https://aisel.aisnet.org/confirm2016/63

Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2015, November). *Security awareness and adoption of security controls by smartphone users*. In 2015 Second International Conference on information security and Cyber Forensics (InfoSec), Cape Town, South Africa.

Pew Research Center (2022). Internet, smartphone and social media use, https://www.pewresearch.org/global/2022/12/06/internet-smartphone-and-social-media-use-in-advanced-economies-2022/, Erişim Tarihi: 24.11.2024.

Sansom-Daly, U. M., & Bradford, N. (2020). Grappling with the "human" problem hiding behind the technology: Telehealth during and beyond COVID-19. *Psycho-Oncology, 29*(9), 1404.

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security*, *28*(2), 293-318.

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2016). *Users' attitudes on mobile devices: can users' practices protect their sensitive data?* 2016 Mediterranean Conference on Information Systems (MCIS), Cyrus, Greece.

Symantec (2015). Internet Security Threat Report. https://dig.watch/resource/symantec-2015-internet-security-threat-report, Erişim Tarihi: 20.11.2024.

Talan, T., Aktürk, C., Korkmaz, A., & Gülseçen, S. (2015). Üniversite öğrencilerinin akıllı telefon kullanımında güvenlik farkındalığı. *Istanbul Journal of Open and Distance Education*, *1*(2).

Truong, H. T. T., Lagerspetz, E., Nurmi, P., Oliner, A. J., Tarkoma, S., Asokan, N., & Bhattacharya, S. (2014, April). The company you keep: Mobile malware infection rates and inexpensive risk indicators. In Proceedings of the 23rd international conference on World wide web, 39-50. Seoul, Republic of Korea.

Wasserman, R. (2022). The Most Common Mobile Security Threats in 2022, https://www.pingidentity.com/en/resources/blog/post/common-mobile-security-threats.html#Common-Mobile-Security-Threats, Erişim Tarihi: 25.11.2024.

Worgotter, N. (2011). *Measurement model to assess market-driving ability in corporate entrepreneurship*.[Doctoral dissertation], University of Pretoria, Pretoria.

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviours of smartphone users in China: an empirical analysis. *The Electronic Library*, *35*(6), 1177-1190.