Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 8 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i08.51959

PAPER

Securing the Mobile Future: An Extensive Analysis of the Threat Landscape from Mobile Devices User Perspectives

Mahmoud Aljamal[1,2], Ayoub Alsarhan[2], Mohammad Aljaidi[3](✉), Ala Mughaid[2,4], Wafa' Q. Al-Jamal[5], Abdullah Ewayed Twairesh[6]

[1]Department of Cybersecurity, Irbid National University, Irbid, Jordan

[2]Department of Information Technology, Faculty of Prince Al-Hussien bin Abdullah for IT, The Hashemite University, Zarqa, Jordan

[3]Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa, Jordan

[4]Department of Computer Science, Gulf University of Science and Technology, Mubarak Al-Abdullah, Kuwait

[5]Faculty of Science and Technology (FST), University Sains Islam Malaysia (USIM), Nilai, Malaysia

[6]Department of Finance and Insurance, College of Business Administration, Northern Border University, Arar, Saudi Arabia

mjaidi@zu.edu.jo

ABSTRACT

Mobile devices are becoming increasingly popular in the modern era, posing a significant threat to the security of organizations. As a result, mobile devices have become more and more vulnerable to cyberattacks. The current study aims to assess the threat landscape of mobile devices from the perspectives of users, highlighting the importance of user-centered perspectives in designing solutions to mobile security threats. A total of 47 participants of different demographic profiles were recruited as respondents, and the primary data were collected through an online questionnaire. The study concludes with a discussion of the findings' implications for research and practice in mobile security. The paper outlines the current state of the art in mobile device security, including vulnerability to security threats, privacy risks, trust in security measures, awareness of potential threats, and satisfaction with the security provided by mobile operating systems. The results demonstrated that users are unaware of data protection and mobile device security, which have a substantial impact on an organization's performance. However, this study lays a foundational perspective for future advancements in security audits, aiming to enhance cybersecurity practices in an increasingly mobile-centric corporate landscape.

KEYWORDS

mobile security, perspective of the smartphone user, threat landscape, risk mitigation

1 INTRODUCTION

In modern society, mobile devices have grown into everyday tools that allow people to access digital services and information anytime, anywhere. The mobile revolution has resulted in the widespread adoption of mobile applications for everyday tasks. The mobile developer and user communities are growing rapidly. Users view mobile devices as personal tools that store sensitive personal information while also aiding daily tasks. However, the extensive use of mobile devices has been linked to a rise in mobile security threats, including malware, phishing, and data breaches [1]. As the use of mobile devices becomes an even more prominent element

Aljamal, M., Alsarhan, A., Aljaidi, M., Mughaid, A., Al-Jamal, W.Q., Twairesh, A.E. (2025). Securing the Mobile Future: An Extensive Analysis of the Threat Landscape from Mobile Devices User Perspectives. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(8), pp. 140–158. https://doi.org/10.3991/ijim.v19i08.51959

Article submitted 2024-08-30. Revision uploaded 2025-01-21. Final acceptance 2025-01-21.

of daily life, it is crucial to discern the threat landscape they encounter. Studying the threat landscape is vital for developing security measures that protect user privacy and personal information. Several studies have explored different aspects of mobile device security, focusing on device technical vulnerabilities and the efficiency of security measures [2], [3]. However, the threat landscape must be viewed from the consumers' perspective since user behavior, attitudes, and perceptions are critical determinants of security solutions' success [4].

Despite growing interest in mobile security threats, current research indicates that many users do not know about the various security threats and the risks they pose [5], [6]. In addition to a lack of knowledge, users often engage in poor behavior, such as keeping their systems up-to-date or clicking on links, allowing them to compromise their devices [7]. Previous studies have proposed several solutions to the problem of mobile security. These approaches include implementing games and messages to personalize user security messages to encourage users to do what is safe [8], [9]. However, many of the recommended solutions lack awareness of user perception and their needs. Thus, these solutions are widely considered irrelevant or antagonistic to users [10]. Ultimately, these solutions have no effect.

To ensure that mobile security policies are relevant and realistic, incorporating the interests and requirements of all stakeholders, including users, is necessary. This consideration will encourage the developers of these applications to provide solutions that will enhance mobile security based on the users' requirements [11].

In the broader field of mobile security, there is a pressing need to explore the interplay between user behavior, awareness, and technology. As mobile devices become increasingly integrated into all aspects of daily life, understanding the human element in cybersecurity becomes critical. Traditional security measures often focus on technological solutions, such as encryption, authentication protocols, and antivirus software, ignoring the role users' play in the security ecosystem [12]. A holistic approach that includes psychological, sociological, and educational perspectives is essential to comprehensively address the security challenges posed by mobile technology. This approach would not only aim to fortify devices against attacks but also empower users to act as informed participants in their security.

The rapidly changing landscape of mobile technology evolution and security threats sophistication makes research in this field incredibly adaptive and challenging. The solutions sufficient to ensure security today will not be enough to protect users tomorrow. Therefore, development and research in this area should be comprehensive, taking into account the diversity of users and their respective contexts. The modern approach to mobile security should not be universal; therefore, a one-size-fits-all solution would not be able to cover the spectrum of threats and security needs of all companies and end users [13]. To succeed in improving security systems, researchers should consider the diversity of user behaviors, including socio-economic and cultural factors. Thus, the development of effective mobile security solutions will require a combination of technology and user-oriented research, including IT solution implementation and user education and regulation.

1.1 Contribution

- Conducted a novel qualitative study to investigate the threat landscape of mobile devices from the users' perspective.
- Explored how users perceive and mitigate mobile security threats and identified their unique needs and perspectives.

- Generated insights into the challenges and concerns of mobile users and their perceptions of the effectiveness of existing security measures.
- Provided valuable information for developing more effective and user-centered mobile security solutions that promote a culture of secure behavior.
- Our study is broad in scope and can be applied to improve the performance of a wide range of real-world applications, including healthcare. The accuracy of health information shared via mobile phone is critical for receiving appropriate instructions for patients. Our research may expand to address privacy concerns.

The structure of this paper is designed as follows: Section 2 shows the related works part. Section 3 shows the procedure of the proposed study. Section 4 shows the results and discussion. The conclusion and future work direction are given in Section 5.

2 LITERATURE REVIEW

Today's mobile devices are becoming more and more convenient. Users can access a range of services, such as e-banking, e-mail, and multimedia, from anywhere at any time using PDAs, computers, and mobile phones. The scheme proposed in [14] delves into balancing data privacy and utility, examining stakeholder roles in data privacy, and employing qualitative analysis to underscore user-centered approaches for privacy in visualization. It maps out advances in visualization for privacy, highlighting user perception's role in mobile security solutions. The study, acknowledging its reliance on self-reported data and potential biases, points to the need for broader, more inclusive research methodologies. This study is crucial to improving user-focused mobile security measures.

With user permission, Location Services enables applications and websites (including maps, webcams, weather, and other apps) to access information from cellular, Wi-Fi2, GPS3, and Bluetooth4 networks in order to determine your precise location. In [15], this study delves into privacy protection within mobile cloud computing, specifically for location-aware services. Through an extensive review, techniques such as K-Anonymity and private information retrieval are analyzed to safeguard user location data against unauthorized access. The article highlights the trade-off between privacy and service efficiency, noting the need for advanced solutions that ensure user privacy without compromising service quality. While pointing out the limitations in the scope of the reviewed literature, the paper contributes significantly to understanding privacy challenges in mobile cloud services, providing a foundation for future privacy-preserving strategies in location-based services. This information is crucial for my research on developing strategies to protect user privacy in mobile services.

Mobile OS systems' sandboxing features improve security. An application's access to the system and other apps, including potentially dangerous code and viruses, is restricted via application sandboxing. Giving each application a unique ID and running it as a separate process is known as sandboxing. It is less likely that malicious damage will occur when the program is isolated from other applications. The authors of [16] discuss Android's ascent in the mobile industry, highlighting its challenge to iPhone dominance by offering consumer choice through multiple vendors and an open-source platform. Android's rapid market share growth is attributed to its extensive app ecosystem, fueled by an open model that contrasts with Apple's curated App Store. The platform's approach to security and privacy, giving users control over app permissions, is noted alongside the potential for malicious applications. The introduction of Google's App Inventor, aimed at broadening app development,

underscores Android's influence on mobile computing's future, despite ongoing challenges around app quality and user privacy.

Using an online survey of 212 fitness tracker users, the study [17] investigates their awareness and behavior towards the security and privacy of their data. The methodology encompassed an array of survey questions focusing on users' confidence in understanding what data is collected and how it's used, their attitudes towards potential privacy threats, and their actual data protection practices. The findings revealed a gap in users' confidence in the utilization of their data compared to what is collected. Although users acknowledged the plausibility of privacy threats, they underestimated the likelihood of such occurrences, leading to minimal protective action toward their data. The research underscored users' differential comfort levels in sharing various data types with different entities, indicating a nuanced perspective toward data privacy. This study calls for enhanced user education on data use and sharing implications, advocating for more granular control over data-sharing preferences to bolster user privacy in the digital era. This insight directly supports the need to develop privacy-preserving strategies in mobile services, aligning with my research focus on enhancing user-centered mobile security solutions.

In a systematic exploration of machine learning (ML) methods for Android mobile malware detection, [18] examines the efficacy of various ML techniques in identifying malicious applications. The review meticulously assesses 106 articles, delineating the strengths, weaknesses, and avenues for improvement across ML-based detection strategies. The analysis spans static, dynamic, and hybrid analysis methods, revealing a comprehensive landscape of current methodologies and their applications in safeguarding Android environments. Key findings underscore the critical role of ML in evolving a classifier from training examples, thereby bypassing the need for explicit signature definitions in malware detection. This adaptability is particularly vital given Android's dominant market share and the consequent attractiveness to cyber threats. The study highlights the ongoing need for innovative ML approaches that can address emerging malware tactics, underscoring the importance of continuous research in this area to fortify mobile security frameworks.

In the context of increasing mobile device vulnerabilities, a comprehensive examination reveals both emerging threats and established countermeasures within mobile security [19]. The research, through an extensive literature review and a survey that involved over 167 mobile application users, uncovers a high level of awareness among users about both threats and their mitigations. Despite recognizing risks associated with physical access and social engineering, a significant portion of participants actively utilize built-in security mechanisms to combat the adverse effects of malware and social engineering scams. This study not only enriches the theoretical discourse by mapping prevalent security concerns and best practices but also offers practical insights at the individual and corporate levels. It emphasizes the criticality of understanding user intentions and technology adoption behaviors to improve the security of mobile applications.

Some businesses decide to allow or require employees to use their personal cell phones for work-related activities. BYOD policies can range from requiring employees to carry their own laptop or PC to permitting them to use remote tools on their personal devices. In [20], authors address the complexities of mobile device security within organizations, particularly under, and this study emphasizes the critical role of Information System (IS) audits in evaluating and enhancing mobile security postures. Recognizing the challenges posed by the integration of personal devices into corporate networks, the research outlines the multiple risks and vulnerabilities inherent to mobile devices and their implications for organizational information security. Through a detailed literature review, the paper elucidates the diverse aspects of mobile

device threats, from insecure connections and applications to user awareness and privacy dilemmas, thereby underpinning the need for a holistic security assessment framework. The feasibility of IS audits as a strategic tool in this context is explored, highlighting their potential to offer comprehensive insights into the effectiveness of existing security measures, policy compliance, and the overall management of mobile devices within organizational information systems. This work lays a foundational perspective for future advancements in mobile device audits, aiming to enhance cybersecurity practices in an increasingly mobile-centric corporate landscape.

Authors in [8] investigate the impact of a gamified information security education system (ISES) on enhancing users' information security awareness and their intentions to adopt protective behaviors; this study integrates affordance theory and means-end chain theory into a comprehensive model. Analyzing data from 220 valid responses through partial least-squares structural equation modeling, findings illustrate that gamified ISES significantly increases information security awareness through emotional and cognitive pathways. Contrary to expectations, while information security awareness directly influences users' intention to engage in security-protective behaviors, elements like physical presence and security knowledge growth do not have a significant impact. Furthermore, the study uncovers the crucial role of curiosity types in modulating the effects of gamified ISES features on user engagement and knowledge acquisition. This study not only underscores the effectiveness of gamification in security education but also offers insight to educators and designers on optimizing gamified systems to foster user engagement and information security behaviors. Future inquiries might delve into the effects of education level and other demographic variables on the efficacy of gamified security education.

In [9], authors delve into the impact of active versus passive phishing warnings in web browsers, revealing a stark contrast in their effectiveness. Through a simulated spear phishing attack, it was discovered that an overwhelming 97% of participants clicked on phishing links. However, the presence of active browser warnings significantly improved user response, with 79% adhering to these warnings, underscoring their potential in safeguarding users. The study emphasizes the inefficacy of passive warnings, with only a single participant heeding them. Using the Communication Human Information Processing Model (C-HIP) for analysis, the research proposes that effective warnings must interrupt the user's current task, clearly, present action options, ensure safety by default, avoid habituation, and visually alter the appearance of phishing sites to reduce their perceived legitimacy. The findings suggest a high susceptibility to phishing among users, yet also highlight the significant protective benefits of well-designed browser warnings, with Firefox's active warnings being particularly effective in securing user compliance. The usefulness of Android-based learning resources in enhancing students' proficiency with electrical measuring devices in the context of the Fourth Industrial Revolution was investigated in [21]. Assessing students' readiness for mobile learning from a cybersecurity perspective was the aim of [22]. The usefulness of Android-based learning resources in enhancing students' proficiency with electrical measuring devices in the context of the Fourth Industrial Revolution was investigated in [23]. The 4D model was used in this study's research and development (R&D) methodology.

The aforementioned list of papers shows that research on mobile device security considers a variety of aspects of smartphone use despite the publications' thorough coverage of a wide range of topics, the studies carried out to yet have not addressed the complexities and combinations of various issues, such as the technological, security, practical, economic, and sociological aspects of smartphone use. Especially, these papers neglect users' awareness of data protection and mobile device security. The literature suggests that mobile security is a critical issue that poses significant

risks to both individuals and organizations. To address this issue, it is important to develop user-centered mobile security solutions that take into account users' unique needs and perspectives. The current study aims to contribute to this goal by investigating the threat landscape of mobile devices from the perspective of users.

3 METHODOLOGY

As the work is aimed at exploring the users, the methodology section is crucial for the study since it is closely tied to the credibility and reliability of the entire project. The qualitative methodology aims to collect a nuanced perspective of mobile device users regarding the threat landscapes they are subjected to. Phenomenology is the most effective strategy that can be used to explore detailed and rich phenomena due to the complex and detailed nature of a user's interaction with mobile security threats. The methodology also necessitated the use of purposive sampling to include users with diverse experiences and views, which helped give a representative dimension to the responses. By better matching the sample to the goals and objectives of the research, purposive sampling increases the accuracy of the research and the reliability of the data and conclusions. The data collected through an online questionnaire included both Likert scale and open-ended questions to gather quantitative data and qualitative data, respectively. Pilot testing was conducted to evaluate the questions' clarity and simplicity. This work employed SPSS to analyze complex data sets to identify trends and relationships that can guide and provide a user-centered perspective on mobile security policies. The section defines the research design, selection of participants, data collection instruments, and the procedures of the analysis, all aimed at investigating the mobile threat landscape from the perspective of the users.

3.1 Participants

For this study, a total of 47 participants were recruited using a purpose-sampling technique aimed at capturing a diverse array of demographics, including age, gender, occupation, and level of education, to ensure a representative sample that would provide a broad understanding of the user's perspectives on mobile device usage. The consistency in the data, as shown in Table 1, reveals that all participants actively engage with mobile devices daily without any missing responses, demonstrating a uniformly high level of mobile technology adoption among the surveyed population. This uniformity underscores the integral role mobile devices play in the daily lives of the participants.

Table 1. Demographic and mobile device usage statistics

Statistics				
		Please Select Your Age	Please Select Gender	How Often Do You Use a Mobile Device?
N	**Valid**	47	47	47
	Missing	0	0	0

Drawing from the age distribution in Table 2, the majority of the study's participants fall within the 18–24 age range, accounting for 61.7% of the total, followed by the 25–34 age range with 34%. Only a small fraction, 4.3%, is represented by

individuals aged 35–44. This distribution highlights a predominantly younger demographic in the sample, suggesting that younger users are more engaged in mobile device usage, which could reflect their attitudes and behaviors towards mobile security. It also raises questions about how security perceptions could vary between different age groups, a factor that could influence the development of targeted security measures and educational initiatives. Figure 1 presents the statistics distribution of the age groups participating in the survey.

Table 2. Age distribution of survey participants

Question: Please Select Your Age					
	Age Range	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18–24	29	61.7	61.7	61.7
	25–34	16	34	34	95.7
	35–44	2	4.3	4.3	100
	Total	47	100	100	

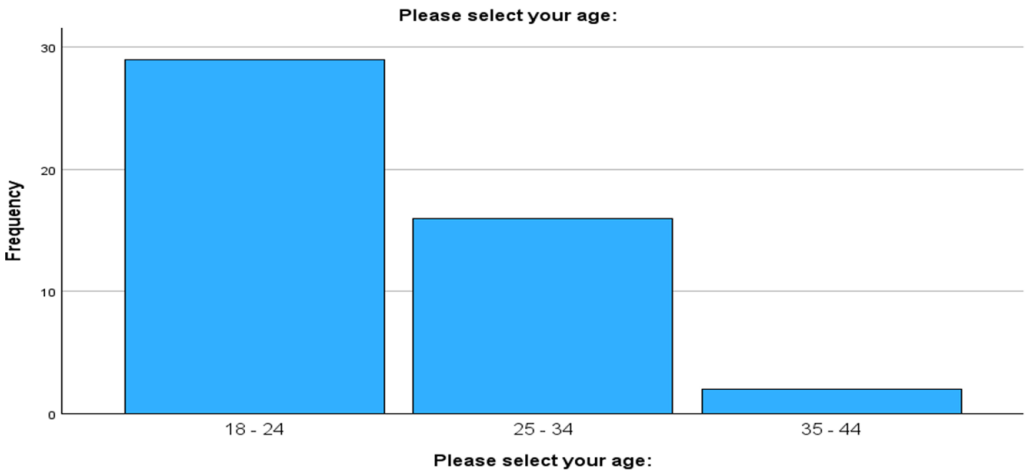

Fig. 1. Statistics of the age groups participating in the survey

The gender distribution in Table 3 reflects the composition of the study's sample, with a healthy representation of both male (63.8%) and female (36.2%) participants as shown in Figure 2. This balance provides a broad perspective on user attitudes towards mobile security threats. It's a positive indication that the study captures varied gender-related insights, which can enhance the understanding of different security perceptions and behaviors in the context of mobile device usage.

Table 3. Gender distribution of survey participants

Question: Please Select Your Gender					
	Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	30	63.8	63.8	63.8
	Female	17	36.2	36.2	100
	Total	47	100	100	163.8

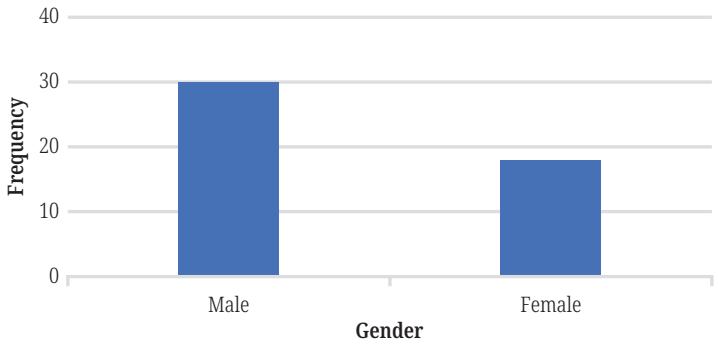

Fig. 2. Statistics of the gender of the respondents in the survey

The mobile device usage frequency in Table 4 presents a unanimous trend with all 47 participants reporting daily use of their mobile devices Figure 3 represents that visually. This homogeneity suggests a high level of mobile technology integration into the participants' daily lives, which could imply a uniform exposure to mobile security threats and highlight the relevance of fostering robust security measures tailored to frequent usage patterns.

Table 4. Mobile device usage frequency of survey participants

Question: How Often Do You Use a Mobile Device?					
	Frequency	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daily	47	100	100	100

3.2 Data collection

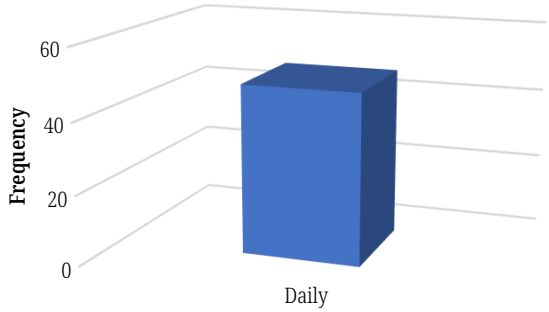

Fig. 3. Statistics on participants' weekly phone usage based on a questionnaire

The data for this study was collected through a dedicated online questionnaire that addressed a range of topics essential for comprehending the mobile security threat from the users' perspective. At first, demographic data were collected to fit the following findings into the framework of age, gender, occupation, and education. The following sections addressed the experience of using mobile devices and the frequency of such interactions to provide a baseline understanding of the experience of every respondent. Then, they were supplemented by inquiries into perceived and real threats and their psychological dimension, which allowed measuring both subjective and objective aspects of mobile security. In addition to behaviors and beliefs, the questionnaire aimed to evaluate the education of people tested on mobile

threats and protective measures to contrast this information with actual practices. Finally, the survey assessed user awareness about the performance of existing measures and the improvement proposals to close with the open-ended question for additional information. This multifaceted approach provided comprehensive data collection, which is vital to establish a detailed view of the mobile threat and the user experience thereof.

3.3 Likert scale

A Likert scale was employed in this study to quantitatively measure the participants' attitudes and perceptions over different constructs directly or indirectly influencing mobile device security. The scale utilized a five-level rating system, a well-recognized approach to adopting survey research for studying opinions and behaviors. It was chosen due to the need to balance the number of options to allow the capture of response variance and not to confuse the participants with too many categories. The points ranged from 1 for disagreement or concern to 5 for agreement or concern. The granularity of ratings allowed the capture of nuances in participants' perceptions of each statement, expressing from strong disagreement to strong agreement or from very low to very high concern levels. The scale implementation contributed to better data quality through clarity of question interpretation and response. Moreover, it offered a standardized method for analyzing user perception as a subjective measure, creating a basis for objective statistical analysis. The Likert scale converted qualitative judgments into quantifiable data, aiding in identifying patterns and interrelations between mobile security aspects, including risk perception, protective measure trust, and the perception of security practice efficiency.

3.4 Data analysis

To dissect the collected dataset, the study leveraged SPSS for its advanced statistical analysis tools. The initial phase of analysis involved the calculation of descriptive statistics, providing an overarching view of the data's structure. Frequencies (f_i) mapped out the number of occurrences for each response, while the arithmetic mean ($\bar{x}$) and standard deviation (s) quantified the central tendency and dispersion, respectively. The arithmetic mean is given by equation (1):

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{1}$$

Where x_i is the value of the ith response and N is the total number of responses, and the standard deviation is given by equation (2):

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2} \tag{2}$$

The exploration deepened with cross-tabulations to construct contingency tables that allowed for the visual digestion of the relationship between categorical variables

such as demographic segments and security concerns. To statistically validate these relationships, the chi-square (X^2) test was applied equation (3):

$$X^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{3}$$

Where O_i denotes the observed frequency, and E_i is the expected frequency under the null hypothesis of independence. This test's p-value was used to discern the presence of statistically significant associations across the different strata of data. These methodological choices provided a robust foundation for identifying key insights and substantiating the study's subsequent conclusions regarding users' security perceptions and behaviors in the mobile domain.

3.5 Ethical considerations

The research fully adhered to an ethical framework. All participants were informed about the purpose of the study, their rights for unwilling participation, and assured confidentiality and anonymity of the gathered information. The prior informed consent for participation in the questionnaire study was provided by all participants. All gathered data will be stored on a protected computer, which only this writer has access.

3.6 Validity and reliability

Several steps were followed to protect the quality of the results. The questionnaire structure was rooted in a relevant review of the literature and with the help of validated scales. Before the data collection, pilot testing was completed to evaluate the clarity and simplicity of the questions. Additionally, multi-coder reliability was assured through the independent coding of a sample of the data by three researchers to support the aligning of subjective data interpretations.

4 RESULTS AND DISCUSSION

Table 5 presents descriptive statistics regarding the perceptions and concerns related to mobile device security among the participants. The study aimed to assess various aspects of mobile device security, including vulnerability to security threats, privacy risks, trust in security measures, awareness of potential threats, and satisfaction with the security provided by mobile operating systems. The data is based on responses from a sample of 47 individuals. The statistics reported include the minimum and maximum values, the mean, and the standard deviation for each item. These statistics provide valuable insights into the participants' perceptions and concerns regarding mobile device security, shedding light on their attitudes and awareness of potential risks in the ever-evolving threat landscape.

Table 5. Descriptive statistics of participants' security perceptions

Statement	N	Min.	Max.	Mean	Std. Deviation
Mobile devices are vulnerable to security threats.	47	1	5	3.57	0.878
I am concerned about the security of my data on mobile devices.	47	1	5	3.45	1.138
I think mobile devices are at risk of malwareor virus attacks.	47	1	5	3.96	0.806
I feel my privacy is at risk when using mobile devices.	47	1	5	3.32	1.105
I trust the security measures in place on mobile devices.	47	1	5	3.32	0.911
I believe that mobile device manufacturers prioritize user security.	47	1	5	3.36	0.965
I am aware of potential threats associated with mobile devices.	47	1	5	3.72	0.852
I feel confident in my ability to protect my mobile device from security threats.	47	1	5	3.38	1.012
I think mobile users should take more precautions to secure their devices.	47	1	5	4.17	0.789
I feel the threat landscape for mobile devices is evolving rapidly.	47	1	5	3.96	0.859
I am aware of the best practices for securing mobile devices.	47	1	5	3.51	1.061
I am satisfied with the level of security provided by mobile operating systems.	47	1	5	3.36	0.819
Valid N (listwise)	47				

4.1 Statistical overview of participant responses

The analytical results for mobile device security were tabulated to encapsulate the varied dimensions of participants' responses. Each entry in the first column corresponds to a different statement concerning mobile device security, ranging from perceived vulnerability to trust in protective measures. The second column, denoted as "N," records the count of valid responses received for each item, with the total number of respondents being 47. The columns labelled "Minimum" and "Maximum" display the range of responses, anchored between 1 and 5, which indicate the least and most severe levels of concern or agreement, respectively. The "Mean" column provides an arithmetic average for the responses to each statement, elucidating the overall tendency among participants' perceptions; for instance, the statement concerning the vulnerability of mobile devices to security threats has an average score of 3.57. Finally, the "Std. Deviation" column quantifies the spread of responses around the mean, offering insights into the consensus among the participants; a lower standard deviation points to a tight clustering of opinions, whereas a higher value denotes a wider range of viewpoints.

4.2 Correlation coefficient or Pearson correlation coefficient

The Pearson correlation coefficient, denoted as r, serves as a pivotal statistical metric, capturing the strength and direction of a linear association between two quantitative variables. This coefficient is scaled between –1 and +1, where the extremities reflect the intensity of the correlation.

An r value of +1 signifies a perfect positive linear relationship, implying that an increase in one variable consistently corresponds with an increase in the other. Conversely, an r value of –1 denotes a perfect negative linear relationship, indicating that an increase in one variable is met with a proportional decrease in the other. An r value at the midpoint of 0 represents the absence of a linear correlation between the variables under investigation.

The absolute value of r, r, serves as an index of correlation strength; a value approaching 1 denotes a strong correlation, while a value near 0 suggests a weak or non-existent linear relationship. The computational formula for r is as follows:

$$r = \frac{\Sigma\left(\left(X_i - \bar{X}\right)\left(Y_i - \bar{Y}\right)\right)}{\sqrt{\Sigma\left(X_i - \bar{X}\right)^2}\sqrt{\Sigma\left(Y_i - \bar{Y}\right)^2}} \tag{4}$$

In this equation:

- X_i represents the observed value of the variable X for the i-th observation.
- $\bar{X}$ denotes the mean of the variable X.
- Y_i represents the observed value of the variable Y for the i-th observation.
- $\bar{Y}$ denotes the mean of the variable Y.
- Σ signifies the sum over all observations.
- Interpreting the equation, the numerator encapsulates the covariance of X and Y, which measures the joint variability of the variables. The denominator is a normalization factor that scales this covariance by the product of the standard deviations of X and Y, thus yielding a dimensionless coefficient. Upon computing this equation, the resultant r value delineates the degree of linear correlation between X and Y, as per the established definition.

4.3 Interpreting the P-value in hypothesis testing

Turning to the environment of statistical analysis, the p-value is a key indicator that is used to evaluate how confident one can be in the results, especially the interpretation of the Pearson correlation coefficient: it is the probability of observing a correlation coefficient with an absolute value at least as large as achieved based on the collected sample data in the situation where the null hypothesis of no correlation in the population is true. Simply put, the p-value is important in the procedure of testing the hypothesis itself. A small p-value, which is usually less than the level of alpha, 0.05, provides strong grounds for rejecting the null hypothesis, indicating a statistical relationship that likely wasn't caused by chance. On the other hand, a high p-value suggests that it would be possible to observe the shown correlation due to the expected variability in random sampling. In the case of a high p-value, there aren't enough statistically justified reasons to reject the null hypothesis.

For the computation of the p-value associated with the Pearson coefficient, the following formula can be used:

$$p = 2 \times \left(1 - F\left(|r|, n-2\right)\right) \tag{5}$$

where,

- p is the p-value,
- F represents the cumulative F-distribution function, used in the case of variances,

- $|r|$ is the absolute value of the observed Pearson correlation coefficient,
- n "What is the size of the sample?" from which the coefficient was calculated.
- This formula indicates how the p-value can be calculated, based on the F-distribution, a common probability distribution. By using this, statisticians can find the p-value for their observed correlation coefficient, aiding in a rigorous evaluation of the evidence against the null hypothesis.

4.4 Correlation analysis

Table 6 offers a brief correlation analysis, illustrating how demographic factors relate to user perceptions of mobile security. It quantifies these relationships, providing insight into the varied influences on users' attitudes towards securing their mobile devices.

Table 6. Correlations between age, gender, and mobile device security perceptions

Correlations

		Please select your gender:	I am concerned about the security of my personal data on mobile devices.	I think mobile devices are at risk of malware or virus attacks.	I feel my privacy is at risk when using mobile devices.	I trust the security measures in place on mobile devices.	I believe that mobile device manufacturers prioritize user security.	I am aware of potential threats associated with mobile devices.	I feel confident in my ability to protect my mobile device from security threats.	I think mobile users should take more precautions to secure their devices.	I feel the threat landscape for mobile devices is evolving rapidly.	I am aware of the best practices for securing mobile devices.	I am satisfied with the level of security provided by mobile operating systems.
Please select your gender:	Pearson Correlation	1	.016	.096	-.098	-.021	-.053	-.068	-.200	.006	.038	-.155	-.008
	Sig. (2-tailed)		.916	.522	.511	.889	.722	.649	.179	.968	.801	.297	.957
	N	47	47	47	47	47	47	47	47	47	47	47	47
I am concerned about the security of my personal data on mobile devices.	Pearson Correlation	.016	1	.447**	.817**	.195	.008	.265	.131	.325*	.509**	.185	-.224
	Sig. (2-tailed)	.916		.002	<.001	.189	.957	.072	.379	.026	<.001	.213	.131
	N	47	47	47	47	47	47	47	47	47	47	47	47
I think mobile devices are at risk of malware or virus attacks.	Pearson Correlation	.096	.447**	1	.503**	.344*	.272	.615**	.340*	.524**	.562**	.280	.155
	Sig. (2-tailed)	.522	.002		<.001	.018	.065	<.001	.019	<.001	<.001	.057	.297
	N	47	47	47	47	47	47	47	47	47	47	47	47
I feel my privacy is at risk when using mobile devices.	Pearson Correlation	-.098	.817**	.503**	1	.177	.032	.327*	.277	.385**	.496**	.080	-.250
	Sig. (2-tailed)	.511	<.001	<.001		.233	.830	.025	.059	.008	<.001	.591	.090
	N	47	47	47	47	47	47	47	47	47	47	47	47
I trust the security measures in place on mobile devices.	Pearson Correlation	-.021	.195	.344*	.177	1	.583**	.312*	.501**	.346*	.157	.367*	.483**
	Sig. (2-tailed)	.889	.189	.018	.233		<.001	.033	<.001	.017	.293	.011	<.001
	N	47	47	47	47	47	47	47	47	47	47	47	47
I believe that mobile device manufacturers prioritize user security.	Pearson Correlation	-.053	.008	.272	.032	.583**	1	.309*	.389**	.403**	.071	.325*	.491**
	Sig. (2-tailed)	.722	.957	.065	.830	<.001		.034	.007	.005	.633	.026	<.001
	N	47	47	47	47	47	47	47	47	47	47	47	47
I am aware of potential threats associated with mobile devices.	Pearson Correlation	-.068	.265	.615**	.327*	.312*	.309*	1	.478**	.427**	.489**	.689**	.178
	Sig. (2-tailed)	.649	.072	<.001	.025	.033	.034		<.001	.003	<.001	<.001	.232
	N	47	47	47	47	47	47	47	47	47	47	47	47
I feel confident in my ability to protect my mobile device from security threats.	Pearson Correlation	-.200	.131	.340*	.277	.501**	.389**	.478**	1	.298*	.119	.462**	.459**
	Sig. (2-tailed)	.179	.379	.019	.059	<.001	.007	<.001		.042	.425	.001	.001
	N	47	47	47	47	47	47	47	47	47	47	47	47
I think mobile users should take more precautions to secure their devices.	Pearson Correlation	.006	.325*	.524**	.385**	.346*	.403**	.427**	.298*	1	.460**	.284	.205
	Sig. (2-tailed)	.968	.026	<.001	.008	.017	.005	.003	.042		.001	.053	.166
	N	47	47	47	47	47	47	47	47	47	47	47	47
I feel the threat landscape for mobile devices is evolving rapidly.	Pearson Correlation	.038	.509**	.562**	.496**	.157	.071	.489**	.119	.460**	1	.454**	.084
	Sig. (2-tailed)	.801	<.001	<.001	<.001	.293	.633	<.001	.425	.001		.001	.574
	N	47	47	47	47	47	47	47	47	47	47	47	47
I am aware of the best practices for securing mobile devices.	Pearson Correlation	-.155	.185	.280	.080	.367*	.325*	.689**	.462**	.284	.454**	1	.283
	Sig. (2-tailed)	.297	.213	.057	.591	.011	.026	<.001	.001	.053	.001		.054
	N	47	47	47	47	47	47	47	47	47	47	47	47
I am satisfied with the level of security provided by mobile operating systems.	Pearson Correlation	-.008	-.224	.155	-.250	.483**	.491**	.178	.459**	.205	.084	.283	1
	Sig. (2-tailed)	.957	.131	.297	.090	<.001	<.001	.232	.001	.166	.574	.054	
	N	47	47	47	47	47	47	47	47	47	47	47	47

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

To clarify the complex interactions between multiple factors and the perception of mobile device security, the paper performed a thorough correlation analysis. The logic behind this type of investigation was to measure the strength and direction of relationships between the following variables: gender, concern about personal data security, fear of malware or virus attack, and assessment of combatting capabilities. Using the Pearson correlation coefficient helped identify how various demographic and psychological characteristics explain the relations and differences in attitudes and actions of people concerning mobile security. These points summarize

the outcomes of this statistical analysis and uncover the nuances of users' views on digital protection.

1. **Gender and security perceptions:** Correlation coefficient between gender and all the security perception variables is very close to zero, ranging from –0.200 to 0.185. There seems to be a weak or no relationship between gender and security perceptions. Thus, gender does not seem to influence how people perceive mobile device security.
2. **Concern for personal data security:** The variable "I am concerned about the security of my data on mobile devices" does not have any significant correlations except a weak positive correlation with "I believe that mobile device manufacturers prioritize user security" at $r = 0.185$ with $p = 0.213$. It indicates that people who think that mobile device manufacturers prioritize user security are more likely to be concerned about the security of their data on mobile devices.
3. **Perception of malware or virus attacks:** The variable "I think mobile devices are at risk of malware or virus attacks" has many significant positive correlations:
   - $r = 0.447$ with $p < 0.001$ with "I am concerned about the security of my data on mobile devices"
   - $r = 0.344$ with $p = 0.018$ with "I trust the security measures in place on mobile devices"
   - $r = 0.503$ with $p < 0.001$ with "I feel my privacy is at risk when using mobile devices"

   Overall, people who think that there is a higher risk of malware and virus attacks on mobile devices are concerned with the security of personal data, are less likely to have trust in security measures and feel that their privacy is at a higher risk.
4. **Trust in security measures and manufacturer prioritization:** The variable "I trust the security measures in place on mobile devices" has a significant positive correlation with "I believe that mobile device manufacturers prioritize user security", $r = 0.583$, $p < 0.001$. This means that individuals who trust the security measures implemented on mobile devices are likely to believe that manufacturers prioritize user security.
5. **Awareness of threats and best practices:** "I am aware of potential threats associated with mobile devices" shows significant positive correlations with "I think mobile devices are at risk of malware or virus attacks", $r = 0.615$, $p < 0.001$ and "I am aware of the best practices for securing mobile devices", $r = 0.689$, $p < 0.001$. Individuals more knowledgeable about potential threats are also more likely to perceive the risk of malware or virus attacks and understand best practices for securing their devices.
6. **Confident in device protection interaction:** "I feel confident in my ability to protect my mobile device from security threats" crosswise significantly with "I trust the security measures in place on mobile devices", $r = 0.501$, $p < 0.001$ and "I am aware of the best practices for securing mobile devices", $r = 0.462$, $p = 0.001$. Therefore, individuals who feel confident about their device protection are more likely to trust security measures and are aware of the best practices.
7. **Perception of user precautions interaction:** "I think mobile users should take more precautions to secure their devices" shows a significant correlation with "I am aware of potential threats associated with mobile devices", $r = 0.427$, $p = 0.003$, and "I am aware of the best practices for securing mobile devices", $r = 0.460$, $p = 0.001$. This demonstrates that individuals who think that users should take more precautions are more likely to be aware of external threats and security best practices.

4.5 Comparative with related works

Drawing upon a diverse array of studies exploring the evolving threat landscape in mobile device security, this paper embarks on a comprehensive examination of user perspectives, methodological approaches, and the multifaceted nature of privacy and security challenges. From [14]'s qualitative insights into data privacy visualization to [8]'s innovative exploration of gamified information security education systems, the literature underscores a pivotal shift towards user-centered security solutions. Notably, the findings reveal a significant disparity between users' awareness of threats and their practical engagement in protective behaviors, as highlighted in the studies by [17]. Furthermore, the integration of ML techniques in malware detection, as examined by [18], alongside the critical examination of Android's security ecosystem by [16], delineates the technological advancements and persistent challenges in safeguarding mobile environments. Our work builds upon this foundation by directly engaging with user perceptions, behaviors, and barriers towards mobile security, offering a fresh perspective that not only enhances our understanding of the threat landscape but also paves the way for developing more effective, user-centric security solutions. Table 7 represents a comparative analysis of the literature on the mobile device threat landscape.

Table 7. Comparative analysis of the literature on the mobile device threat landscape

Reference	Purpose of the Study	Methodology	Key Findings	Significance of the Findings	Your Evaluation
[14]	Investigates balancing data privacy and utility, emphasizing user centered approaches for privacy in visualization.	Qualitative analysis	Advances in visualization for privacy highlighting user perception's role in mobile security solutions.	Pivotal for enhancing user focused mobile security measures.	Essential groundwork, yet requires broader methodologies for inclusivity.
[15]	Explores privacy protection in mobile cloud computing for location aware services.	Extensive literature review	Techniques like K-Anonymity and private information retrieval safeguard user location data. Highlights the privacy service efficiency trade-off.	Contributes significantly to understanding privacy challenges in mobile cloud services, laying the groundwork for future strategies.	Provides a foundation but needs advanced solutions for balancing privacy and service quality.
[16]	Discusses Android's rise in the mobile industry and its challenge to iPhone's dominance.	Descriptive analysis	Android's rapid market share growth due to its open-source platform and extensive app ecosystem. Points to the potential for malicious applications.	Highlights Android's influence on mobile computing's future despite challenges around app quality and user privacy.	Insightful analysis of Android's market dynamics and security implications.
[17]	Investigates fitness tracker users' awareness and behavior towards security and privacy.	Online survey of 212 users	A gap in users' confidence regarding data utilization. Underestimation of privacy threats leads to minimal protective actions.	Calls for enhanced user education on data use and implications, advocating for more granular data sharing control.	Highlights the need for improved privacy preserving strategies in mobile services.

(Continued)

Table 7. Comparative analysis of the literature on the mobile device threat landscape *(Continued)*

Reference	Purpose of the Study	Methodology	Key Findings	Significance of the Findings	Your Evaluation
[18]	Systematic exploration of ML methods for Android mobile malware detection.	Review of 106 articles	ML techniques are critical in identifying malicious applications, bypassing the need for explicit signature definitions.	Emphasizes the importance of innovative ML approaches to address emerging malware tactics and fortify mobile security frameworks.	Underlines the critical role of ML in enhancing Android security, suggesting continuous research for improvement.
[19]	Examines mobile device vulnerabilities, emerging threats, and countermeasures.	Literature review and survey of 167 users	High user awareness of threats and mitigations, with active utilization of built-in security mechanisms against malware and scams.	Offers practical insights at individual and corporate levels, emphasizing understanding user intentions and technology adoption behaviors to improve mobile application security.	Provides valuable insights into user awareness and security practices, high lighting the need for comprehensive security strategies.
[20]	Addresses the complexities of mobile device security in organizations under BYOD policies.	Detailed literature review	Highlights the multifaceted risks and vulnerabilities of mobile devices, emphasizing the importance of IS audits for enhancing organizational mobile security postures.	Lays a foundational perspective for future advancements in mobile device audits, aiming to bolster cybersecurity practices in a mobile centric corporate landscape.	Offers a critical view on the necessity of holistic security assessments in organizations, especially under BYOD policies.
[8]	Investigates the impact of gamified ISES on users' information security awareness and protective behaviors.	Analysis of 220 valid responses	Gamified ISES boosts information security awareness via emotional and cognitive pathways. Curiosity types moderate the effects of gamified features on engagement and knowledge acquisition.	Demonstrates the effectiveness of gamification in security education and provides insights for optimizing gamified systems to foster user engagement and security behaviors.	Validates the potential of gamification in enhancing information security awareness and behaviors, suggesting areas for future research.
[9]	Delves into the effectiveness of active versus passive phishing warnings in web browsers.	Simulated spear phishing attacks	Active warnings significantly improved user response to phishing attempts, with 79% adhering to active warnings. Passive warnings were largely ineffective.	Highlights the significant protective benefits of well-designed browser warnings, suggesting improvements in web browser security measures.	Emphasizes the importance of effective warning systems in web browsers to combat phishing, advocating for active over passive warnings.
Our Work	Qualitative exploration into the mobile device threat landscape from the user's perspective.	Online questionnaire with 47 participants, utilizing the Likert scale	Significant gap in users' confidence in their understanding and management of mobile security threats. Risky behaviors persist despite awareness.	Urges a paradigm shift towards developing user centered mobile security solutions, fostering a secure mobile ecosystem that resonates with user perspectives.	Calls attention to the disconnect between user awareness and action, advocating for engaging users in the security solution development process.

5 CONCLUSION AND POTENTIAL FUTURE WORKS

This study explored gender's impact on perceptions of mobile device security, finding little influence. The study concludes by highlighting how crucial it is to raise

user awareness in order to improve mobile device security. Given the widespread use of mobile devices and the growing complexity of cyberattacks, it is critical that people and businesses continue to be watchful and proactive in putting strong security measures in place. However, previous research neglected the role of user awareness on mobile phone security. Furthermore, the study highlighted individuals' attitudes and emphasized that those who believe manufacturers prioritize user security express greater concern for personal data security. Perceiving higher risks of malware or virus attacks correlates with data security concerns, lower trust in security measures, and increased privacy risk perception. Greater awareness of potential threats links to perceiving attack risks and knowing best practices for device security.

In future research, it would be valuable to explore the potential impact of socio-cultural factors on perceptions and attitudes towards mobile device security. Examining how factors such as age, education level, and cultural background influence individuals' security perceptions can provide deeper insights into their security behaviors and concerns. Additionally, conducting longitudinal studies to track changes in perceptions and attitudes over time would be beneficial in understanding the evolving landscape of mobile device security and the impact of technological advancements. Furthermore, investigating the effectiveness of different security awareness and education programs in promoting secure behaviors among mobile device users could help develop targeted strategies for improving security practices. Lastly, exploring the relationship between mobile device security and other domains, such as cybersecurity hygiene or organizational security practices, can provide a more comprehensive understanding of the broader security landscape.

6 ACKNOWLEDGMENT

The authors extend their appreciation to the Hashemite University and Zarqa University for supporting this study.

7 REFERENCES

[1] A. Alsarhan, I. Al-Aiash, D. Al-Fraihat, M. Aljaidi, and D. A. A. H. A. Laila, "Expert phishing detection system," in *2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT),* Bali, Indonesia, 2024, pp. 54–59. https://doi.org/10.1109/IAICT62357.2024.10617460

[2] O. Adeniyi, A. S. Sadiq, P. Pillai, M. Aljaidi, and O. Kaiwartya, "Securing mobile edge computing using hybrid deep learning method," *Computers*, vol. 13, no. 1, p. 25, 2024. https://doi.org/10.3390/computers13010025

[3] L. Bilge and T. Dumitra, "Before we knew it: An empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 2012, pp. 833–844. https://doi.org/10.1145/2382196.2382284

[4] R. Fadli *et al.*, "Effectiveness of mobile virtual laboratory based on project-based learning to build constructivism thinking," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 6, pp. 40–55, 2024. https://doi.org/10.3991/ijim.v18i06.47643

[5] A. D. Samala, D. Mhlanga, L. Bojić, N. J. Howard, and D. Pereira Coelho, "Blockchain technology in education: Opportunities, challenges, and beyond," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 1, pp. 20–42, 2024. https://doi.org/10.3991/ijim.v18i01.46307

[6] B. Jin, J. Kim, and L. M. Baumgartner, "Informal learning of older adults in using mobile devices: A review of the literature," *Adult Education Quarterly*, vol. 69, no. 2, pp. 120–141, 2019. https://doi.org/10.1177/0741713619834726

[7] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings 2002 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2002, pp. 273–284. https://doi.org/10.1109/SECPRI.2002.1004377

[8] M. Ashawa and S. Morris, "Analysis of mobile malware: A systematic review of evolution and infection strategies," *JISCR*, vol. 4, no. 2, pp. 103–131, 2021. https://doi.org/10.26735/KRVI8434

[9] H. Chen, Y. Zhang, S. Zhang, and T. Lyu, "Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention," *Education and Information Technologies*, vol. 28, no. 12, pp. 15915–15948, 2023. https://doi.org/10.1007/s10639-023-11771-z

[10] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: An empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008, pp. 1065–1074. https://doi.org/10.1145/1357054.1357219

[11] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121. https://doi.org/10.1109/SP.2015.14

[12] K. R. Choo, L. Rokach, and C. Bettini, "Mobile security and privacy: Advances, challenges and future research directions," *Pervasive and Mobile Computing*, vol. 32, pp. 1–2, 2016. https://doi.org/10.1016/j.pmcj.2016.10.003

[13] A. Pollini *et al.*, "Leveraging human factors in cybersecurity: An integrated methodological approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371–390, 2022. https://doi.org/10.1007/s10111-021-00683-y

[14] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446–471, 2013. https://doi.org/10.1109/SURV.2012.013012.00028

[15] K. Bhattacharjee, M. Chen, and A. Dasgupta, "Privacy-preserving data visualization: Reflections on the state of the art and research opportunities, *Computer Graphics Forum*, vol. 39, pp. 675–692, 2020. https://doi.org/10.1111/cgf.14032

[16] Z. A. Almusaylim and N. Jhanjhi, "Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing," *Wireless Personal Communications*, vol. 111, pp. 541–564, 2020. https://doi.org/10.1007/s11277-019-06872-3

[17] M. Butler, "Android: Changing the mobile landscape," *IEEE Pervasive Computing*, vol. 10, no. 1, pp. 4–7, 2010. https://doi.org/10.1109/MPRV.2011.1

[18] S. Gabriele and S. Chiasson, "Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12. https://doi.org/10.1145/3313831.3376651

[19] J. Senanayake, H. Kalutarage, and M. O. Al-Kadri, "Android mobile malware detection using machine learning: A systematic review," *Electronics*, vol. 10, no. 13, p. 1606, 2021. https://doi.org/10.3390/electronics10131606

[20] P. Weichbroth and L. Lysik, "Mobile security: Threats and best practices," *Mobile Information Systems*, vol. 2020, pp. 1–15, 2020. https://doi.org/10.1155/2020/8828078

[21] N. A. A. Othman, A. A. Norman, and M. L. M. Kiah, "Information system audit for mobile device security assessment," in *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malayasia, 2021, pp. 1–6. https://doi.org/10.1109/CRC50527.2021.9392468

[22] F. Eliza *et al.*, "Assessing student readiness for mobile learning from a cybersecurity perspective," *Online Journal of Communication and Media Technologies,* vol. 14, no. 4, p. e202452, 2024. https://doi.org/10.30935/ojcmt/15017

[23] R. Fadli, H. D. Surjono, R. C. Sari, Y. Hidayah, and F. Eliza, "Assessing cybersecurity awareness among vocational students in office administration," *International Journal of Safety and Security Engineering,* vol. 14, no. 4, pp. 1115–1123, 2024. https://doi.org/10.18280/ijsse.140410

8 AUTHORS

Mahmoud Aljamal is working at the Department of Cybersecurity, Irbid National University, Irbid, Jordan P.O. Box 2600 (E-mail: m.aljamal@inu.edu.jo). Also works for Department of Information Technology, Faculty of Prince Al-Hussien bin Abdullah for IT, The Hashemite University, Zarqa, Jordan (E-mail: mahmood.yj.98@gmail.com).

Ayoub Alsarhan received a Ph.D. degree in Computer Engineering in the field of cyber security and wireless network from the Concordia University, Canada. He is currently a Full Professor with the Information Technology Department, the Hashemite University, Zarqa, Jordan. His research interests include cybersecurity, network security, wireless networks, and cloud computing contributed to several journals and conference papers (E-mail: ayoubm@hu.edu.jo).

Mohammad Aljaidi received his B.Sc. in Computer Science from Zarqa University in 2014, M.Sc. in Computer Science from Zarqa University in 2017, and Ph.D. in Computer Science from Northumbria University. Currently, he is working as an Assistant Professor at Zarqa University (E-mail: mjaidi@zu.edu.jo).

Ala Mughaid works for both Department of Information Technology, Faculty of Prince Al-Hussien bin Abdullah for IT, The Hashemite University, Zarqa, Jordan (E-mail: ala.mughaid@hu.edu.jo), and also the Department of Computer Science, Gulf University of Science and Technology, Kuwait (E-mail: Mughaid.A@gust.edu.kw).

Wafa' Q. Al-Jamal is working at the Faculty of Science and Technology (FST), University Sains Islam Malaysia (USIM), Nilai, Malaysia (E-mail: wafa.aljamal11@gmail.com).

Abdullah Ewayed Twairesh is working for Department of Finance and Insurance, College of Business Administration, Northern Border University, Arar, Saudi Arabia (E-mail: abdullah.twairesh@nbu.edu.sa).