مجلة جامعة فزان العلمية
Fezzan University scientific Journal
journal@fezzanu.edu.ly

Smartphone Users' Information Security Practices in Libya A Study of Sebha University Students

* Rabia Masoud [1] and Alsanossi Ahmed[2] and Taher Brideh [3]and Maher Alghali[4]
[1] Electrical and Electronic Eng. Dept., Engg, Faculty, Wadi Alshatti University, Brack, Libya
[2] Computer Science Dept., Faculty of Sciences. Wadi Alshatti University, Brack, Libya
[3] Network Dept, Information Technology Faculty, Sebha University, Sebha, Libya
[4] Management Dep, Economics and Accounting Sciences Faculty, Fezzan University, Libya

Abstract
In today's digital age, smartphones have clearly become indispensable tools. With such a large number of people using smartphones unknowingly, the security risk increases significantly. therefore, this study aims to understand the behavior of students at Sebha University in Libya in relation to information security when using smartphones. A quantitative survey approach used to examine students' strategies to avoid various security threats. A total of 280 students took part in the study, and the collected data was analyzed using appropriate statistical techniques. Based on the study results, Sebha University students are relatively safe when it comes to carrying out disaster recovery, avoiding harmful behavior and using helpful telephone settings and add-on utilities. In addition, this study shows that not all students behave safely when using different safety features in the same way, and that there are some differences depending on age and gender. It is recommended that the university focus on instructing and advising students on best practices for using smartphones.
Keywords: Smartphones, Information Security, Security Risk, Libya.

Introduction

In this digital age, smartphones are considered a very helpful means of communication. By using various types of mobile applications, smartphones offer a wide range of computing capabilities and connectivity options that go beyond the mere ability to make and receive calls and texts. Smartphones are now a necessary part of everyone's life and have even led to addiction in many cases [1]. Smartphones can be used for phone calls, but they also have many other connectivity features and are always online, so users can always access the latest information. In addition, they can instantly send random information to almost anyone. The processing power of smartphones today is the same as that of standard PCs ten years ago, and they're small enough to fit in any pocket.

The adaptable design of smartphones allows developers and designers to create new creative applications. This allows users of contemporary smartphones to access a vast array of applications for a variety of uses. The Google Play Store and the Apple App Store, which offer around 2 million and 2.3 million apps, respectively, in the first quarter of August 2024, provide pertinent statistics [2]. The total number of app downloads reached 25.6 billion mobile apps in 2024, which clearly reflects trends in smartphone usage [3]. As far as computer history is concerned, the market shares of smartphones exceeded those of desktops in 2024. In November 2024, mobile phones, desktops, and tablets accounted for 62.87%, 35.3% and 1.84% of the market share [4].

Most applications are free to download and use, but some cost money and must be paid for before being installed on a smartphone. This has helped smartphones gain popularity, and using these

*Corresponding author: als.ahmed@wau.edu.ly Received in 9 October 2025 – revised form 8 November 2025 Accepted 28 January 2026 - Publication date 23 February 2026

apps has had a big impact on how people behave when they use them [5]. While there are many benefits to using a smartphone, it also poses many security risks [6] . The extensive use of network systems and the rapid development of information technology have meant that people are more reliant on the Internet. It has become an essential part of everyday life and has had an impact on social interactions, education, public services, payments, and entertainment [7]. Data and information security needs to be ensured, as smartphones rely on the Internet to carry out most of their activities. Patterns such as passwords, code passwords, PIN passwords, and Face Unlock can be used for smartphone authentication [8] However, these authentication techniques aren't very secure as guesswork and brute force attacks can evade them.

Students today use smartphone applications for a range of academic tasks, such as accessing social media, email, online banking, and shopping [9] [10]. The rapid increase in smartphone usage has made it extremely difficult for researchers and information security professionals to provide information security [11] [12]. Furthermore, the security of the entire smartphone network is significantly affected by the information security practices of each individual user.

Recent data on mobile malware threats suggests that the volume of new malware has increased dramatically, as has its sophistication and complexity. It is common knowledge that smartphone users frequently ignore security warnings [13]. The vulnerability in smartphones disrupts the security trust model. In addition, it was found that consumers rarely consider privacy and security when installing new apps and often do not adequately protect themselves by configuring security features on their smartphones [14]. This is also supported by younger, technology-savvy generations who came into contact with mobile devices at a young age. Research on students revealed that they paid little attention to the security features of smartphones [15].

Kaspersky Security Network reports that 7 million attacks on mobile software were foiled by adware, malware, and unwanted software in the second quarter of 2024[16]. RiskTool software was the most common threat to mobile devices, accounting for 41% of all threats found. A total of 367,418 malicious install packages have been detected, including 13,013 mobile banking Trojans and 1,392 mobile ransomware Trojans. As 7,697,975 attacks were detected, the number of mobile device attacks with adware, malware, or malicious software fell compared to the first quarter of 2024, but increased compared to the same period last year.[16]

Crucially, the application program interface (API) of smartphones was the basis for the development of numerous malware, viruses and Trojans. Most of these programs, including reputable programs like Facebook, Gmail, and others, appear to be safe software. They collect user information, such as geolocation, using a smartphone's GPS service without the user's consent [17] [18] [19] . This study focuses on the information security behavior of smartphones to determine whether students refrain from risky smartphone use and to examine how differences in students' smartphone use affect their information security behavior.

Literature Review

Smartphones are used for phone calls, photos, emails, social media status updates, web browsing, banking transactions, and many other activities. In addition to unintentional disclosure of personal data, this type of diverse smartphone use can also expose users to the risk of illegal blackmail attempts to get out of their plight [20, 21]. Another worrying feature is their tendency to download third-party apps without doing thorough research [22]. Third parties may be able to access users' personal information if smartphones are lost or stolen, which represents another security risk [23] [24]. It is well known that adopting appropriate security technologies is essential to protect smartphone users' information [25] [26], [27]. However, user data cannot be fully protected by security technology alone [28] [29]. In addition, it is common knowledge that the security features of smartphones are directly affected by the information security practices of individual users. [30] [31] [32].

McGill [33] claims that users are much more likely to actively protect their home computer or laptop than their tablet or smartphone, and many people are still reluctant to perform crucial tasks like financial transactions on their mobile devices, This pattern of use is evolving as more and

more young people become familiar with them. Mobile devices have greater vulnerabilities than a home computer. Even though smartphones are typically thought of as personal devices, the "Bring Your Own Device" (BYOD) concept allows them to be used for task organization. [34] [35]. As a result, smartphone security is becoming critical.

Smartphone users who engage in risky behavior are more vulnerable to mobile threats and the associated harmful effects [36]. Understanding the user behavior of smartphones is therefore becoming increasingly important for information security (IS) in general, as it depends heavily on how each user behaves [23] [29]. Although many studies have explored the technical aspects of mobile threats and strategies to combat them [37] [38] [39] [40] , there is little behavioral analysis research on smartphones. As a result, researchers [41] [33] have found that more behavioral IS studies focused on mobile devices are needed to better understand user behavior in this environment. Although users find speed and ease of use attractive, there are several risks associated with these benefits.

Numerous studies, including one by [42], have revealed the risks of mobile phones, owing to insufficient knowledge of their security and privacy, they found that only 36% of respondents said they were responsible for keeping their smartphones secure. The majority of people are unlikely to take precautionary measures against potential threats as they believe that third parties are responsible for keeping smartphones safe. As reported by Mylonas and his colleagues [22], users often rely on the app repository but ignore or neglect security features that are either missing or inactive.

The concept of security awareness consists of two parts: educating people about information security issues and inspiring them to behave in accordance with the importance of the information they handle on a daily basis for their work [43]. Markelj [44] claims that users' level of online security depends on their awareness of threats and their ability to respond appropriately. Users should be better informed about risks and appropriate training on cyber-security should be provided. From the research above, it's clear that understanding smartphone security threats and solutions is critical, we need to inform users what factors they need to consider in this situation. Harris [45] explores the factors influencing consumers prior to the installation of mobile applications and concludes that consumers place safety as a top priority when evaluating risks. The desire to install apps increases when trust increases due to lower risk perception. The European Network and Information Security Agency (ENISA) points out “lack of user awareness” as a vulnerability for smartphones and warns against installing apps unless the source is reliable and known [46] [47]. The lack of awareness of the dangers of installing apps from unreliable sources is one of the weaknesses [48]. According to [48] “Being aware of the developers of the applications and their repositories” should be the first consideration for smartphone users. In order to use the installed applications, a user must agree to provide the application with the private information it requests or allow the application to access multiple mobile information systems.

Similarly, Watson and Zheng [49] examine users' awareness of mobile security recommendations and find that non-technicians often ignore or are unaware of numerous important security options. Therefore, they recommend creating plans to raise awareness of mobile security solutions and promote the use of mobile security solutions. Hackers often target smartphones based on the data they store. It is therefore important that smartphone users take precautionary measures, such as implementing security controls to protect against threats and being aware of threats and vulnerabilities [13, 50].

Android users were surveyed by Alani [51], with a focus on permission settings, malware/adware leaks, and privacy, the finding showed that security breaches, such as rooted devices, had an impact on Android users' privacy awareness. Bieringer [14] created a survey to find out how younger generations (born between 1984 and 2012) are affected by the awareness, decisions, and education of users regarding the cybersecurity of their smartphones. the finding showed that

although the sample was familiar with physical smartphone access, other security measures (such as using a VPN when using public WiFi) were completely ignored.

The authors Bitton [52] provide a hierarchical taxonomy on security awareness developed specifically for mobile device users. It sets a series of measurable standards and categorizes them according to various technological specializations and psychological elements. In this study, smartphone users' awareness of various security-related factors is compared based on their age, education, and level of cybersecurity knowledge. Computer users who behave differently from traditional computer users have paid little attention to smartphone security [52]. In addition, the majority of research is concerned with awareness of smartphone in a specific context, such as in a university with staff and/or students [53].

In contrast to technical security measures, information security generally barely takes human factors into account. Because technology alone cannot provide comprehensive security solutions, and security cannot be complete if human factors are not considered, it is important to study them. Knowledgeable users may be more likely to follow security best practices [54] [55]. To develop effective materials to raise awareness of security, trainers and instructors must have a comprehensive understanding of users' existing behaviors, knowledge, misconceptions, and attitudes regarding smartphone security. Therefore, the aims of this study to investigate how smartphone users behave when using their devices in terms of information security. The aim is to find out how they perceive information security, how they feel about it and how they behave when using smartphones. It is imperative that we take into account the latest information from users. Accordingly, the authors believe that this study provides the literature with valuable information to understand the current level of smartphone awareness users from various demographic perspectives and to develop strategies to increase it.

Methodology

The quantitative method used in this study. This design provides an overview of university students' cybersecurity awareness and allows data to be collected at a specific point in time. The questionnaire used to collect data on students' knowledge, attitudes, and behavior in the area of cybersecurity. The target group were university students from various academic fields. 280 students have already taken part in this survey and the sample will be selected from Sebha University students. Descriptive statistics were used to analyze the data using IBM SPSS software. Use the chi-square test to examine the data at a confidence level of a = 0.05. According to the hypothesis, it is assumed that the variable is significantly contiguous when $p>0.05$ or when the t-statistic is 1.96.

Results and Discussion

Respondents' academic and demographic information, including their gender, age group, and faculty/institution affiliation, is shown in Table 1. According to the demographics of the participants, both male and female smartphone users are involved in a balanced way. 70.7% of the participants are between 18 and 24 years old. Most participants came from the faculties of IT and Sciences. However, the study can once again be considered representative as it included representatives from all areas of the university, including smaller institutes.

The research results are based on the three approaches: avoiding harmful behaviors and practices, using telephone settings and add-on utilities, and preventive behaviors and practices, as presented in Table 2

Table 1. Academic and demographic information of the students

Item	Response	Frequency	(%)
Gender	Male	134	47.8
	Female	146	52.2
Age	18- 22	198	70.7
	23-27	74	26.4
	28-32	6	2.1
	Above 32	2	0.7
Faculties/Institutions	Arts	29	10.35

	Sciences	68	24.3
	IT	74	26.4
	Engineering	37	13.3
	Pharmacy	13	4.65
	Commerce and Political Science	41	14.65
	Law	18	6.4

- In terms of avoiding harmful behavior and practices, Table 2 shows that around 7.5% of respondents occasionally share their passwords. 22.5% of respondents said they occasionally clicked on the link in emails, text messages, social media posts, etc. while playing or using the app, or that they came from an unknown source. Respondents are more vulnerable to malware and phishing attacks when they click on dubious links. Approximately 43.21% of respondents said they occasionally connect to unprotected Wi-Fi networks, making them vulnerable to data breaches. Malware infections are primarily caused by applications that have been installed from unreliable sources. The security and legitimacy of such an application cannot be guaranteed. Around 23.21 percent of respondents occasionally download apps from untrustworthy sources, leaving them vulnerable to malware infections. 48.57 percent of respondents upload location-based information to social networks, exposing them to numerous threats including identity theft, data breaches, and cyberstalking. It is impossible to guarantee the legitimacy and security of such an application. Of those surveyed, 23.21% occasionally download apps from unreliable sources, leaving them vulnerable to malware infections. And 48.57% of respondents post location-based data on social media, exposing them to various risks including cyberstalking, identity theft, and data breaches. The analysis concludes that respondents are more vulnerable to malware, phishing, Individual users are at risk of privacy and security issues with location-based updates.
- Regarding the using of add-on utilities and phone settings. According to the survey, 90% of respondents used the screen lock, 38% turned on automatic updates, 62% turned off Bluetooth, and 10% turned off GPS when it wasn't being used. However, the low percentage of users who can perform encryption 8.92% indicates that respondents are either unaware of privacy or are unable to protect data on the phone.
- Finally, as regards preventive practices and behaviors, the analysis in Table 2 shows that a larger percentage of respondents do not follow preventive practices and behaviors, such as 46.78% don't change their password or PIN frequently, 94.28% read end-user agreements, 75.71% create unique passwords for apps, and 76.78% sign out of social networks and email services. The risk of losing sensitive data due to malware infections or data loss without backups increases if preventive cybersecurity security measures and practices are not implemented.

Table 2. Recommended cybersecurity behaviors and practices for smartphone

Avoiding harmful behaviors and practices			
Behaviors	Always	Sometimes	Never
Sharing of PIN/password/pattern information	21 7.5%	46 16.4%	213 76.07%
Clicking on the link in an email, SMS, social networks, etc. from an unknown source or while playing games or using apps	63 22.5%	91 32.5%	126 45%
Downloading apps from untrusted third-party websites	87 31.07%	69 24.64%	124 44.28%

Connecting to free unsecured Wi-Fi networks	121 43.21%	92 32.85%	67 23.92%
Downloading attachments from unknown emails	56 23.21%	91 32.5%	133 47.5%
Uploading location-based information on social networking sites	136 48.57%	85 30.35%	59 21.07%
Use of phone settings and add-on utilities			
Behaviors	Always	Sometimes	Never
Enable auto-update	109 38.92%	143 51.07%	28 1%
Enable screen lock	254 90.7%	23 8.21%	3 1.07%
Enable encryption	25 8.92%	31 11.07%	224 80%
Disable GPS when not required	29 10.35%	53 18.92%	198 70.71%
Disable Bluetooth when not required	176 62.85%	69 24.64%	35 12.5%
Enable remote tracking of device	154 55%	87 31.07	39 13.92%
Enable remote locking of the device	136 48.57%	91 32.5%	47 16.78
Preventive behaviors and practices			
Behaviors	Always	Sometimes	Never
Frequently changing PIN/password/pattern information	53 18.92%	96 34.28%	131 46.78
Scanning phones using anti-virus/ anti-malware regularly	24 8.57%	79 28.21%	177 63.21%
Regular update of apps	122 43.57%	98 35%	60 21.42%
Regular backup of data	86 30.71%	109 38.92%	85 30.35%
Uninstalling/deleting apps which are not used	37 13.21%	116 42.42%	127 45.35
Logging off of services such as email and Facebook	23 8.21%	42 15%	215 76.78%
Setting a different password for apps	17 6.07%	51 18.21%	212 75.71%
Checking permissions while installing apps	9 3.21%	26 9.28%	245 87.5%
Reading the end-user agreement	5 1.78%	11 3.92%	264 94.28%

To identify the relationship between different demographic factors and the cybersecurity behavior and practices of smartphone users, the researchers used the chi-square test. Age and gender are the demographic variables considered in this study.

The finding showed that male respondents performed more effectively than female respondents, suggesting that they had understood and used safety procedures more comprehensively. Male participants behaved risky when updating apps, connecting to unprotected Wi-Fi networks, and downloading apps from unreliable third-party repositories. While female participants preferred PIN/password authentication, male respondents preferred biometric authentication. When verifying app permissions and reading the user agreement, male respondents fared better.

Younger students aged between 18 and 22 have grown up using technology, while those over 22 are trying to adopt it. Younger students are more aware of security checks and accept them better than the oldest. The oldest students preferred a PIN/password, while the younger students preferred a biometric authentication system.

In this study, risky behavior was observed among smartphone users under 22 years of age. Over 22 smartphone users have demonstrated secure practices when they connect to unprotected Wi-Fi networks, download attachments from unknown sources, share PINs and passwords, and download apps from dubious sources.

Respondents demonstrated that they did not adhere to suggested cybersecurity behaviors and practices. According to data analysis, some common security practices have been adopted, including locking the screen, automatically updating, and turning off GPS and Bluetooth when not in use. On the other hand, respondents were less aware of the technical security measures used, such as encryption, remote lock, and remote wipe. Respondents were vulnerable to malware and phishing attacks due to their harmful behavior and cybersecurity practices.

Respondents showed that they did not follow recommended cybersecurity practices and behaviors. Data analysis indicates that some standard security procedures have been implemented, such as locking the screen, enabling automatic updates, and turning off Bluetooth and GPS when not in use. However, respondents were less aware of technical security measures such as encryption, remote locking and remote wipe. Respondents' destructive behavior and cybersecurity practices made them vulnerable to malware and phishing attacks.

Limitation

The study recognizes a number of limitations which may affect the generalizability of its findings. The main limitations of this research are the following:

- Respondents' perceptions of their cybersecurity behavior and practices were measured against their actual behavior and practices.
- For time reasons, no other universities in Libya are included in the study except Sebha University, further study may be conducted to better understand the study by including students from other universities.

Conclusion

Despite the many new features offered by smartphones, the risk of data theft is increased when using a smartphone. Therefore, understanding the behavior of information security is important for developing solutions and raising awareness among users. Information security awareness can help smartphone users change their information-related behavior and thus reduce the risks associated with using smartphones. However, the finding of the study will provide some important information that will help improve knowledge of information security practices when using smartphones. This understanding could be useful for creating appropriate plans and regulations and introducing the necessary training to improve the information security of smartphones. This study will help raise awareness among students about information security and encourage authorities to implement appropriate strategies and policies to address information security risks when using smartphones. In this situation, the university can take targeted measures, including by offering lectures, seminars, workshops and advice, to make students aware of safety concerns.

References

[1] C. Y. Fook, S. Narasuman, N. Abdul Aziz, and C. J. A. J. o. U. E. Tau Han, "Smartphone usage among university students," vol. 7, no. 1, pp. 282-291, 2021.

[2] Statista. (2024, 10-11). *Number of apps available in leading app stores as of August 2024*. Available: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[3] Statista. (2024, 10-11). *Number of iOS and Google Play app downloads as of Q1 2024*. Available: https://www.statista.com/statistics/695094/quarterly-number-of-mobile-app-downloads-store/

[4] StatCounter. (2024, 2-12). *Desktop vs Mobile vs Tablet Market Share Worldwide*. Available: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide

[5] I. A. Zolkepli, S. N. S. Mukhiar, and C. J. J. o. m. c. Tan, "Mobile consumer behaviour on apps usage: The effects of perceived values, rating, and cost," vol. 27, no. 6, pp. 571-593, 2021.

[6] Q. J. T. Xiao and Informatics, "Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study," vol. 58, p. 101535, 2021.

[7] R. Masoud, M. Alghali, T. Brideh, and A. Ahmed, "Cybersecurity Awareness among College Students in Libyan Universities last," المجلة العلمية لكلية التربية, vol. 4, no. 1, pp. 238-224, 2025.

[8] I. Chenchev, A. Aleksieva-Petrova, and M. Petrov, "Authentication mechanisms and classification: a literature survey," in *Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3*, 2021, pp. 1051-1070: Springer.

[9] Q. Zeerak, M. Imran, K. Azeez, T. H. Lokanathan, and I. M. Ismail, "The effects of smartphone addiction on academic performance among undergraduate medical students in Karnataka, India: A multi-centric study," *Cureus,* vol. 16, no. 6, 2024.

[10] F. J. A. J. o. E. T. Nami, "Educational smartphone apps for language learning in higher education: Students' choices and perceptions," vol. 36, no. 4, pp. 82-95, 2020.

[11] F. Eliza *et al.*, "Assessing student readiness for mobile learning from a cybersecurity perspective," *Online Journal of Communication Media Technologies,* vol. 14, no. 4, p. e202452, 2024.

[12] S. F. Verkijika, "Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret," *Computers Security Communication Networks,* vol. 77, pp. 860-870, 2018.

[13] P. Shah and A. Agarwal, "Cybersecurity behaviour of smartphone users in India: an empirical analysis," *Information Computer Security,* vol. 28, no. 2, pp. 293-318, 2020.

[14] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education," *Computers Security Communication Networks,* vol. 88, p. 101647, 2020.

[15] M. Park and L. Drevin, "An investigation into the security behaviour of tertiary students regarding mobile device security," 2016.

[16] Securelist. (2024, 2-12). *IT threat evolution in Q2 2024. Mobile statistics*. Available: https://securelist.com/it-threat-evolution-q2-2024-mobile-statistics/113678/

[17] A. K. Tyagi, "Spy in the crowd: How user's privacy is getting affected with the integration of internet of thing's devices," in *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*, 2019.

[18] M. Modaresnezhad and H. Nemati, "Participatory sensing or sensing of participation: awareness and privacy concerns with smart device applications," *International Journal of Technology Human Interaction,* vol. 16, no. 3, pp. 124-143, 2020.

[19] H. Lu, "Assessing and Mitigating Emerging Threats in the Mobile Software Supply Chain," Indiana University, 2025.

[20] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know your enemy: the risk of unauthorized access in smartphones by insiders," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 2013, pp. 271-280.

[21] A. J. A. C. A. J. o. C. Minnaar and Victimology, "Cybercriminals, cyber-extortion, online blackmailers and the growth of ransomware," vol. 32, no. 2, p. 105, 2019.

[22] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers Security Communication Networks,* vol. 34, pp. 47-66, 2013.

[23] X. J. Zhang, Z. Li, and H. J. T. E. L. Deng, "Information security behaviors of smartphone users in China: an empirical analysis," vol. 35, no. 6, pp. 1177-1190, 2017.

[24] P. Onumadu and H. Abroshan, "Near-field communication (nfc) cyber threats and mitigation solutions in payment transactions: A review," *J Sensors,* vol. 24, no. 23, p. 7423, 2024.

[25] S. F. Verkijika, "Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret," *Computers Security,* vol. 77, pp. 860-870, 2018.

[26] B.-Y. Ng, A. Kankanhalli, and Y. C. J. D. S. S. Xu, "Studying users' computer security behavior: A health belief perspective," vol. 46, no. 4, pp. 815-825, 2009.

[27] M. Esmaeili, *Assessment of users' information security behavior in smartphone networks*. Eastern Michigan University, 2014.

[28] S. Suryawanshi, "Securing the Modern Web: A Comprehensive Exploration of Web API Authentication and Future Trends," *Authorea Preprints,* 2025.

[29] S. Nowrin and D. Bawden, "Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh," *Information Learning Science,* vol. 119, no. 7/8, pp. 444-455, 2018.

[30] P. Holicza and E. Kadëna, "Smart and secure? Millennials on mobile devices," *Interdisciplinary Description of Complex Systems: INDECS,* vol. 16, no. 3-A, pp. 376-383, 2018.

[31] J. Iqbal, S. H. Soroya, and K. Mahmood, "Financial information security behavior in online banking," *Information Development,* vol. 40, no. 4, pp. 550-565, 2024.

[32] C. Candiwan and L. M. Rianda, "Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users," *International Journal of Safety Security Engineering,* vol. 14, no. 3, 2024.

[33] T. McGill and N. Thompson, "Old risks, new challenges: exploring differences in security between home computer and mobile device use," *Behaviour Information Technology,* vol. 36, no. 11, pp. 1111-1124, 2017.

[34] H. Lam, T. Beckman, M. Harcourt, and S. Shanmugam, "Bring Your Own Device (BYOD): Organizational Control and Justice Perspectives," *Employee Responsibilities Rights Journal,* pp. 1-19, 2024.

[35] P. Baillette, Y. Barlette, and A. J. I. J. o. I. M. Leclercq-Vandelannoitte, "Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users," vol. 43, pp. 76-84, 2018.

[36] A. M. Khalaf, A. A. Alubied, A. M. Khalaf, A. A. Rifaey, A. Alubied, and A. Rifaey, "The impact of social media on the mental health of adolescents and young adults: a systematic review," *Cureus,* vol. 15, no. 8, 2023.

[37] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad, "Cyber threats classifications and countermeasures in banking and financial sector," *IEEe Access,* vol. 11, pp. 125138-125158, 2023.

[38] A. Damaraju, "Mobile Cybersecurity Threats and Countermeasures: A Modern Approach," *International Journal of Advanced Engineering Technologies Innovations,* vol. 1, no. 3, pp. 17-34, 2021.

[39] J. Eppler and Y. Wang, "Towards improving the security of mobile systems using virtualization and isolation," in *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ)*, 2018, pp. 1-6: IEEE.

[40] B. A. Kumar and P. Mohite, "Usability of mobile learning applications: a systematic literature review," *Journal of Computers in Education,* vol. 5, pp. 1-17, 2018.

[41] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *computers security,* vol. 32, pp. 90-101, 2013.

[42] M. Koyuncu and T. Pusatli, "Security awareness level of smartphone users: An exploratory case study," *Mobile Information Systems,* vol. 2019, no. 1, p. 2786913, 2019.

[43] A. McIlwraith, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge, 2021.

[44] B. Markelj and I. Bernik, "Safe use of mobile devices arises from knowing the threats," *journal of information security applications,* vol. 20, pp. 84-89, 2015.

[45] M. A. Harris, R. Brookshire, and A. G. J. I. J. o. I. M. Chin, "Identifying factors influencing consumers' intent to install mobile applications," vol. 36, no. 3, pp. 441-450, 2016.

[46] G. Zamanis, "Security unawareness," Πανεπιστήμιο Πειραιώς, 2022.

[47] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," *European Network Information Security Agency,* vol. 710, no. 01, 2010.

[48] W. Jeon, J. Kim, Y. Lee, and D. Won, "A practical analysis of smartphone security," in *Symposium on Human Interface*, 2011, pp. 311-320: Springer.

[49] B. Watson and J. Zheng, "On the user awareness of mobile security recommendations," in *Proceedings of the SouthEast Conference*, 2017, pp. 120-127.

[50] F. Parker, J. Ophoff, J.-P. Van Belle, and R. Karia, "Security awareness and adoption of security controls by smartphone users," in *2015 Second international conference on information security and cyber forensics (InfoSec)*, 2015, pp. 99-104: IEEE.

[51] M. M. J. I. J. o. I. M. T. Alani, "Android users privacy awareness survey," vol. 11, no. 3, 2017.

[52] R. Bitton *et al.*, "Taxonomy of mobile users' security awareness," vol. 73, pp. 266-293, 2018.

[53] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos, and P. J. I. Kotzanikolaou, "Security awareness of the digital natives," vol. 8, no. 2, p. 42, 2017.

[54] A. G. Silva-Trujillo, M. J. González González, L. P. Rocha Pérez, and L. J. García Villalba, "Cybersecurity analysis of wearable devices: smartwatches passive attack," *Sensors,* vol. 23, no. 12, p. 5438, 2023.

[55] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers security,* vol. 106, p. 102267, 2021.