S. ABDARAZAK MOUSSA ATILIM UNIVERSITY 2025

SECURITY AWARENESS OF SMARTPHONE USERS: A DESCRIPTIVE STUDY

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

SALAH ABDARAZAK MOUSSA

A MASTER OF SCIENCE THESIS
IN
THE DEPARTMENT OF INFORMATION TECHNOLOGY

JUNE 2025

SECURITY AWARENESS OF SMARTPHONE USERS: A DESCRIPTIVE STUDY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

SALAH ABDARAZAK MOUSSA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION TECHNOLOGY

JUNE 2025

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

Assoc. Prof. Dr. Gökhan TUNÇ
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Information Technology, Atılım University.

Assoc. Prof. Dr. Sacip TOKER
Head of Department

This is to certify that we have read the thesis SECURITY AWARENESS OF SMARTPHONE USERS: A DESCRIPTIVE STUDY submitted by SALAH ABDARAZAK MOUSSA and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Murat KOYUNCU
Supervisor

Examining Committee Members:

Assoc. Prof. Dr. Tolga PUSATLI
Dept. of Management Inf. Syst., Çankaya University

Prof. Dr. Murat KOYUNCU
Information Systems Engeneering, Atılım University

Asst. Prof. Dr. Kerem AY
Information Systems Engeneering, Atılım University

Date: *24.06.2025*

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: SALAH ABDARAZAK MOUSSA

Signature:

ABSTRACT

SECURITY AWARENESS OF SMARTPHONE USERS: A DESCRIPTIVE STUDY

Abdarazak Moussa, Salah
M.S., Information Technology
Supervisor: Prof. Dr. Murat KOYUNCU
June 2025, 73 pages

This thesis examines the critical issue of smartphone security awareness in an age where mobile devices have become indispensable in everyday life. With the extensive amount of personal data stored on smartphones, these devices are not only tools of convenience but also potential targets for cyberattacks. Their ubiquity, combined with sensitive applications and information, makes them vulnerable to various threats, from hacking to physical loss. Consequently, ensuring the security of smartphones has become increasingly vital. Users should increase their awareness of digital threats such as phishing and malicious apps and adopt measures such as strong lock screen settings and secure backup routines.

This study aims to evaluate the security awareness levels of smartphone users through a survey method, focusing on their understanding of common risks, adoption of protective measures, and perceived susceptibility to cyberattacks. A diverse sample of 145 participants, primarily aged 18–30, provided insights into their security behaviors.

Findings indicate that while users often employ basic measures such as locking their devices, more advanced practices like regular data backups, encryption, and vigilance against phishing attempts are frequently overlooked. Furthermore, the study reveals a strong emphasis on physical security, such as preventing unauthorized device access, over soft security measures like protecting online accounts and personal data. This research sheds light on significant gaps in smartphone security practices and underscores the importance of user education in addressing these deficiencies. By

providing actionable insights and practical recommendations, the study contributes to the broader field of cybersecurity and supports the development of more effective awareness campaigns and tools for enhancing smartphone security.

Keywords:

Security awareness in smartphones, user behavior, data protection, cybersecurity threats, quantitative research.

ÖZ

AKILLI TELEFON KULLANICILARININ GÜVENLİK FARKINDALIĞI: BELİRTİMSEL BİR ÇALIŞMA

Abdarazak Moussa, Salah
Y.L., Bilgi Teknolojileri
Tez Yöneticisi : Prof. Dr. Murat KOYUNCU
Haziran 2025, 73 sayfa

Bu tez, mobil cihazların günlük hayatta vazgeçilmez hale geldiği bir çağda akıllı telefon güvenliği farkındalığının kritik sorununu incelemektedir. Akıllı telefonlarda depolanan kapsamlı miktarda kişisel veriyle, bu cihazlar yalnızca kolaylık sağlayan araçlar değil, aynı zamanda siber saldırılar için potansiyel hedeflerdir. Her yerde bulunmaları, hassas uygulamalar ve bilgilerle birleştiğinde, onları bilgisayar korsanlığından fiziksel kayba kadar çeşitli tehditlere karşı savunmasız hale getirir. Sonuç olarak, akıllı telefonların güvenliğini sağlamak giderek daha hayati hale gelmiştir. Kullanıcılar, kimlik avı ve kötü amaçlı uygulamalar gibi dijital tehditler konusunda farkındalıklarını artırmalı ve güçlü kilit ekranı ayarları ve güvenli yedekleme rutinleri gibi önlemler benimsemelidir.

Bu çalışma, akıllı telefon kullanıcılarının güvenlik farkındalık düzeylerini, yaygın riskleri anlamalarına, koruyucu önlemleri benimsemelerine ve siber saldırılara karşı algılanan duyarlılıklarına odaklanarak bir anket yöntemi aracılığıyla değerlendirmeyi amaçlamaktadır. Çoğunlukla 18-30 yaş aralığındaki 145 katılımcıdan oluşan çeşitli bir örneklem, güvenlik davranışları hakkında içgörüler sağlamıştır.

Bulgular, kullanıcıların cihazlarını kilitlemek gibi temel önlemleri sıklıkla kullanırken, düzenli veri yedeklemeleri, şifreleme ve kimlik avı girişimlerine karşı dikkatli olma gibi daha gelişmiş uygulamaların sıklıkla göz ardı edildiğini göstermektedir. Ayrıca, çalışma, çevrimiçi hesapları ve kişisel verileri korumak gibi yumuşak güvenlik önlemlerine kıyasla yetkisiz cihaz erişimini engelleme gibi fiziksel güvenliğe güçlü

bir vurgu yapıldığını ortaya koymaktadır. Bu araştırma, akıllı telefon güvenliği uygulamalarındaki önemli boşluklara ışık tutmakta ve bu eksiklikleri gidermede kullanıcı eğitiminin önemini vurgulamaktadır. Eyleme dönüştürülebilir içgörüler ve pratik öneriler sunarak, çalışma daha geniş siber güvenlik alanına katkıda bulunmakta ve akıllı telefon güvenliğini artırmak için daha etkili farkındalık kampanyaları ve araçlarının geliştirilmesini desteklemektedir.

Anahtar Sözcükler:
Akıllı telefonlarda güvenlik farkındalığı, kullanıcı davranışı, veri koruması, siber güvenlik tehditleri, nicel araştırma.

To Familly

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to everyone who supported me throughout this journey. First and foremost, I extend my sincere appreciation to my supervisor, Prof. Dr. Murat Koyuncu, for his invaluable guidance, encouragement, and patience during the completion of this work. My gratitude also goes to all the dedicated staff at Atılım University, whose assistance made this experience both enriching and fulfilling.

I am deeply thankful to my family, whose unwavering support and belief in me have been the foundation of my success. Their encouragement gave me the strength to persevere and achieve my goal of completing my postgraduate studies.

Additionally, I am profoundly grateful to the Center for Electronic Systems and Programming, the National Agency for Scientific Research, and the Ministry of Higher Education for providing me with the opportunity to study in Turkey. Without their support, this accomplishment would not have been possible.

Lastly, I would like to express my deepest gratitude to my beloved country, Djibouti, for its belief in my potential and its commitment to the pursuit of knowledge. It is my sincerest hope that I can contribute to the progress and prosperity of my homeland in the future.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

NFC	Near Field Communication
GPS	Global Positioning System

CHAPTER 1

INTRODUCTION

Mobile devices, including smartphones and tablets, are compact, handheld computing tools equipped with touchscreen interfaces, digital buttons, and built-in communication features such as Bluetooth, near-field communication (NFC), cellular networks, and Wi-Fi. These devices typically include cameras, GPS capabilities, and support for both third-party and proprietary applications. Despite their limited processing power and memory, mobile devices are optimized for lightweight, low-scale applications known as mobile apps.

Their portability, light weight, and multifunctional design have contributed to their widespread adoption. Modern mobile devices enable users to perform daily tasks remotely—such as checking emails, online banking, shopping, participating in video conferences, and making voice calls—without the need for a traditional computer or physical workspace. As a result, smartphones have become indispensable tools in both personal and professional settings, enhancing communication, streamlining business processes, and boosting productivity.

However, the increasing reliance on smartphones has raised significant concerns regarding digital security and user behavior. With the rapid expansion of smartphone usage, understanding patterns of compulsive use and the growing risks associated with poor security practices has become essential [1]. As the number of smartphone users rises dramatically, information security experts face mounting challenges in protecting users' digital assets [2]. Smartphones often store sensitive personal data, making them attractive targets for theft and cyberattacks [3].

Recent research has emphasized the critical role of security awareness among smartphone users. For instance, highlighted the prevalence of risky behaviors in response to phishing attempts, while demonstrated how targeted education programs can significantly improve users' cybersecurity practices [4]. Despite a growing body of literature, current data remains limited in several key respects. First, given the fast-paced evolution of technology and user behavior, ongoing research is required to identify and respond to emerging security challenges. Moreover, most existing studies focus on general computer security rather than smartphone-specific behavior [5]. Research tends to be confined to institutional environments—such as universities—and frequently overlooks users' prior cybersecurity knowledge or experiences [6]. Consequently, a substantial knowledge gap remains regarding smartphone users' real-world security practices.

This thesis addresses that gap by investigating users' awareness, behaviors, and attitudes toward smartphone security. Specifically, the study explores practices related to device locking, backup routines, data protection, and responses to common threats. The following five research questions guide the investigation:

RQ1: What is the level of security awareness among smartphone users?
RQ2: Do owners of smartphones select the proper lock (screen) settings for their devices?
RQ3: Do smartphone users (beyond locking their devices) adhere to best practices for data security?
RQ4: How aware are users of the importance of routine data backup, and how capable are they of recovering data in case of loss?
RQ5: Do users prioritize hard security (device access control) over soft security (data privacy and protection)?

The study focuses on participants who completed most of the survey questions. It mainly aims at:

- **Understanding User Behavior:** The research provides detailed insights into the security awareness and practices of smartphone users, particularly among young adults and university students. These findings may inform targeted cybersecurity awareness campaigns for specific demographic groups.

- **Identifying Security Gaps:** By analyzing users' practices—such as lock settings, frequency backup, and exposure to data breaches—the study identifies key weaknesses. For example, despite widespread use of fingerprint authentication, many users fail to regularly update lock settings, revealing a need for improved security recommendations.

- **Highlighting Risks of Public Wi-Fi Use:** While some users take precautions like VPNs, others still engage in risky behaviors such as connecting to unsecured networks. These findings emphasize the importance of increasing public awareness regarding mobile security in open spaces.

- **Evaluating Backup Practices:** The thesis highlights inconsistent backup behaviors among users, with many neglecting to back up data regularly. This reinforces the need for educational interventions promoting frequent and secure data backups.

- **Raising Awareness of Cyber Threats:** The study also reveals that although most participants have not fallen victim to phishing attacks, a minority have underlined ongoing vulnerabilities. The findings support the necessity of continuous education on recognizing and responding to cybersecurity threats. This study contributes to raising awareness among users about the determination of cybersecurity threats, such as phishing attacks. Data relating to the fact that a large majority of participants have never fallen victim to phishing attacks show good self-protective behavior; however, the small percentage that has fallen into such situations underlines ongoing vulnerabilities. This is a contribution to emphasize the need for continuous education on how to recognize and react in the event of cybersecurity threats.

The study is organized as follows: in Chapter 2, we first provide a summary of relevant literature. The survey approach is then described in Chapter 3, along with sample considerations. Chapter 4 gives the findings of the descriptive statistics. The limits of the investigation are covered in Chapter 5. In addition to the conclusion, the last chapter includes an examination and discussion of the findings.

CHAPTER 2

SUMMARY OF RELEVANT LITERATURE

2.1 Introduction to Smartphone Security Awareness

In the contemporary digital landscape, smartphones have transcended their original function as mere communication devices, evolving into indispensable personal and professional tools. These ubiquitous devices now serve as central repositories for an extensive array of sensitive personal, financial, and proprietary information, ranging from intimate photographs and contact lists to banking applications and confidential work documents. This pervasive integration of smartphones into daily life underscores a critical imperative: the need for a robust understanding of and proactive engagement with smartphone security measures among users. The proliferation of mobile devices, coupled with the increasing sophistication of cyber threats, has rendered smartphone security awareness a paramount concern in the broader field of cybersecurity [7] [22].

The inherent portability and constant connectivity of smartphones, while offering unparalleled convenience, simultaneously expose users to a myriad of vulnerabilities. A compromise of these devices can precipitate severe consequences, including but not limited to privacy violations, identity theft, financial fraud, and the unauthorized disclosure of sensitive data [3], [22]. Consequently, safeguarding these miniature computing powerhouses has become an increasingly vital aspect of personal and organizational digital hygiene. This chapter aims to provide a comprehensive and in-depth review of the existing academic literature pertaining to smartphone security awareness, user behavior, prevalent threats, and the efficacy of various protective measures. It seeks to synthesize current scholarly discourse, identify critical research gaps, and establish a robust theoretical foundation for the empirical analysis presented in subsequent chapters.

2.2 The Evolving Landscape of Smartphone Threats

The cyber threat landscape targeting smartphones is dynamic and continuously evolving, characterized by an increasing volume and sophistication of attacks. While traditional threats such as malware and viruses persist, new vectors and more advanced social engineering techniques have emerged, exploiting both technological vulnerabilities and human factors [22]. Early research highlighted general concerns regarding data theft and physical loss [3], but more recent analyses demonstrate a shift towards highly targeted and deceptive attacks.

One of the most pervasive and insidious threats to smartphone users remains phishing, which encompasses a broad range of deceptive tactics designed to trick individuals into divulging sensitive information or performing actions that compromise their security [10], [21]. Phishing attacks, including email-based phishing, SMS-based phishing (smishing), and voice-based phishing (vishing), have seen exponential growth in recent years. For instance, reports indicate a significant surge in phishing attempts, with millions of attacks blocked annually and a notable increase in smishing incidents, reflecting attackers' diversification beyond traditional email vectors [21]. The effectiveness of these attacks is often directly correlated with users' lack of cybersecurity knowledge and their inability to discern legitimate communications from malicious ones [11], [15].

Beyond phishing, mobile malware continues to pose a significant risk. This includes various forms such as Trojan horses, spyware, ransomware, and botnets, which can infiltrate devices through malicious applications downloaded from unofficial stores, deceptive links, or compromised websites [22], [23]. Ransomware, in particular, has become a grave concern, as it can encrypt user data and demand payment for its release, often bypassing conventional security software [27]. Other threats include software vulnerabilities, Denial of Service (DoS) attacks, sniffing, spoofing, and physical attacks, all of which can compromise the device, its data, applications, or network connectivity [22]. The sheer volume of cyberattacks on mobile devices, reaching tens of millions annually, underscores the critical need for heightened user awareness and robust protective measures [22].

2.3 User Awareness Versus Security Behavior: The Awareness-Practice Gap

A recurring and significant theme in the literature is the discernible gap between users' theoretical understanding of cybersecurity threats and their actual security practices. While many smartphone users may possess a general awareness of digital risks, their day-to-day behaviors often fall short of recommended security standards, creating a critical vulnerability [8], [9]. This "awareness-practice gap" is a complex phenomenon influenced by various psychological, cognitive, and practical factors.

Research indicates that users frequently neglect to implement even fundamental safety measures, such as consistently enabling screen locks or regularly updating their devices [8], [23]. For example, despite the clear benefits of timely updates in patching security vulnerabilities, a significant portion of users may delay or skip installing OS updates due to perceived lack of time or concerns about compatibility issues [24]. This highlights a trade-off users often make between security and convenience, where the immediate perceived benefit of bypassing a security measure outweighs the abstract or distant threat of a cyberattack [20].

Furthermore, the overconfidence bias can exacerbate this gap. Some users may overestimate their ability to identify and mitigate threats, leading to a false sense of security and a reduced likelihood of adopting proactive measures [27]. Conversely, an excessive fear of technology can also hinder the adoption of beneficial security practices, as users might avoid downloading necessary applications or engaging with security features due to apprehension [27]. This complex interplay of awareness, perception of risk, and behavioral intent necessitates a nuanced approach to understanding and improving smartphone security practices.

2.4 Specific Threat Vectors: Phishing and Malware

Phishing and malware represent two of the most prevalent and damaging threat vectors targeting smartphone users, demanding focused attention within literature. As discussed, phishing attacks continue to evolve, with attackers leveraging sophisticated social engineering tactics across various communication channels [21]. The effectiveness of these attacks is often predicated on human susceptibility rather than purely technical vulnerabilities. Users' ability to recognize the subtle cues of a phishing attempt, such as suspicious sender addresses, urgent language, or unusual requests for personal information, is paramount to prevention [15]. Despite widespread awareness campaigns, many individuals still fall victim, underscoring the need for more engaging and tailored cybersecurity education programs that go beyond mere information dissemination to foster critical thinking and behavioral change [11].

Mobile malware, on the other hand, operates through various mechanisms to compromise device integrity and confidentiality. This includes applications embedded with malicious code, often distributed through unofficial app stores or disguised as legitimate software [22]. Once installed, malware can perform a range of nefarious activities, from stealing personal data (e.g., contacts, messages, financial information) to tracking location, displaying aggressive advertisements, or even locking the device for ransom [23], [27]. The constant emergence of new malware families, such as various forms of spyware and Trojans, necessitates continuous vigilance and the adoption of protective applications like virus scanners [23]. The challenge lies not only in developing robust technical defenses but also in educating users about the risks associated with downloading unverified applications and interacting with suspicious content, thereby reinforcing the critical role of user behavior in preventing malware infections.

2.5 The Role of Built-in Security Features and User Adoption

Modern smartphones are equipped with a plethora of built-in and third-party security features designed to protect user data and device integrity. These include, but are not limited to, biometric authentication (fingerprint, face recognition), strong password/PIN options, device encryption, remote wipe capabilities, and application permission controls [10], [16]. However, the mere existence of these features does not guarantee their effective utilization. A significant body of research suggests that many users either lack awareness of these tools, do not fully understand how to engage with them effectively, or choose not to activate them due to perceived inconvenience [13], [8].

For instance, while biometric authentication methods are widely favored for their convenience and perceived security [16], users may still neglect to set strong PINs or regularly update their lock settings, creating a potential loophole [8]. Similarly, device encryption, often enabled by default on newer smartphones, may not be fully understood or verified by users [23]. The decision to adopt or bypass security features is often influenced by a trade-off between perceived security benefits and usability [20]. Users tend to favor options that require minimal effort, such as automated backups or biometric locks, which, while offering some protection, can lead to a false sense of security if not complemented by other robust practices [16]. This highlights that technological safeguards alone are insufficient without active user participation and a comprehensive understanding of how these features contribute to overall security posture.

2.6 Demographic and Psychographic Influences on Security Practices

The literature consistently highlights that demographic and psychographic factors significantly influence smartphone security awareness and behavior. Variables such as age, gender, education level, technological familiarity, and even cultural background can shape an individual's perception of risk, adoption of security measures, and susceptibility to cyber threats [11], [17] [25].

Age, for example, presents a nuanced picture. While younger users (e.g., those aged 18-30) often demonstrate greater familiarity with digital technologies and a higher awareness of emerging threats, they may also exhibit more risky behaviors, such as a greater propensity to click on suspicious links or interact with unknown attachments [12], [27]. This could be attributed to overconfidence or a tendency to prioritize convenience over security. Conversely, older users, though potentially less informed about the latest digital threats, may adopt more cautious behaviors by default, such as avoiding public Wi-Fi or being more hesitant to download new applications [12], [24]. However, some studies suggest that education and awareness alone may not always translate directly into improved security behaviors across all age groups [24].

Gender also plays a role, with some studies indicating differences in specific security practices. For instance, research has shown variations in operating system preferences (e.g., iOS vs. Android) and the adoption of certain security features like face recognition or the frequency of backing up data [26]. While some findings suggest that females might exhibit slightly higher pro-security behaviors in certain contexts, other studies report no significant gender-based differences in general security concerns or practices [26], [17]. These discrepancies underscore the need for further research to understand the specific nuances of gender influence on smartphone security.

Education level and digital literacy are also crucial determinants. Higher levels of education and digital proficiency are generally associated with greater security awareness and a better understanding of complex security concepts [10]. However, as noted earlier, knowledge does not always translate directly into consistent secure behavior, highlighting the importance of bridging the awareness-practice gap through targeted interventions [24]. Psychographic factors, such as an individual's perceived risk, trust in technology, and willingness to engage with security measures, further complicate this dynamic, emphasizing the need for personalized approaches to security education [20], [24].

2.7 Educational Interventions and Awareness Campaigns

Given the persistent awareness-practice gap and the evolving threat landscape, educational interventions and awareness campaigns are widely recognized as critical components in enhancing smartphone security. Literature consistently advocates for tailored security awareness training programs that account for different levels of technological literacy, user experiences, and demographic characteristics [14], [11]. Generic, one-size-fits-all approaches often prove ineffective in fostering lasting behavioral change.

Recent advancements in cybersecurity education emphasize the integration of interactive and engaging methodologies. Gamification, for instance, has shown promise in improving users' cybersecurity practices by making learning more immersive and enjoyable [11]. Similarly, mobile learning approaches are gaining traction, offering flexible, accessible, and cost-effective ways to deliver cybersecurity awareness programs directly to smartphone users, thereby improving "cyber hygiene" [18], [19]. These approaches acknowledge that traditional classroom-based instruction or passive awareness campaigns often fall short in engaging students and ensuring long-term retention of critical cyber hygiene practices.

Effective awareness programs should not only inform users about threats but also empower them with practical skills and the motivation to apply security measures consistently. This includes emphasizing the importance of regular data backups, recognizing the signs of phishing attacks, understanding the implications of app permissions, and promoting timely software updates [18], [21]. Furthermore, campaigns should address the psychological factors that influence user behavior, such as overconfidence or the prioritization of convenience, by presenting security as an integral and manageable aspect of digital life rather than an onerous burden [20]. Ongoing research is crucial to develop and evaluate such interventions, ensuring their adaptability to emerging threats and evolving user behaviors, ultimately fostering a more security-conscious user base.

2.8 Challenges and Future Directions in Smartphone Security Awareness

Despite significant advancements in both technical security measures and user awareness initiatives, several challenges persist in ensuring comprehensive smartphone security. One primary challenge lies in the rapid pace of technological innovation and the continuous emergence of new threat vectors. As smartphones become more integrated with other smart devices and the Internet of Things (IoT), the attack surface expands, requiring users to adapt to increasingly complex security paradigms [22]. Maintaining up-to-date awareness and adapting behaviors to these new threats is a continuous uphill battle for the average user.

Another significant challenge is the inherent tension between security and usability. Users often prioritize convenience, leading them to bypass or underutilize robust security features if they perceive them as cumbersome or disruptive to their daily routines [20], [16]. Designing security mechanisms that are both highly effective and seamlessly integrated into the user experience remains a critical area for future development. This requires a collaborative effort between security researchers, device manufacturers, and application developers to create intuitive and user-friendly security defaults and prompts that encourage secure behaviors without imposing an undue burden.

Furthermore, the global and diverse nature of smartphone usage introduces cultural and socioeconomic complexities. As highlighted by Mugisha et al. [24], users in developing countries, for instance, may face different barriers to adopting security practices, such as data charges associated with updates or limited access to reliable internet connectivity. This necessitates localized and culturally sensitive awareness campaigns that address specific regional challenges and resource constraints.

Future research directions should therefore focus on several key areas. Firstly, there is a need for longitudinal studies that track changes in user behavior and awareness over time, providing insights into the long-term effectiveness of security interventions. Secondly, research should delve deeper into the psychological underpinnings of insecure behaviors, exploring cognitive biases, risk perception, and decision-making processes in the context of mobile security. Thirdly, the development and rigorous evaluation of personalized security awareness programs, leveraging artificial intelligence and adaptive learning techniques, could offer more effective ways to deliver targeted education. Finally, promoting a "security-by-design" philosophy among developers and manufacturers, where security is an inherent part of product development rather than an afterthought, will be crucial in building a more resilient smartphone ecosystem [18].

2.9 Summary

In summary, the literature unequivocally underscores the critical importance of smartphone security awareness in an increasingly interconnected and threat-laden digital environment. While technical safeguards continue to advance, user behavior consistently emerges as the most significant vulnerability. The awareness-practice gap, where knowledge does not consistently translate into secure actions, remains a central challenge, exacerbated by the dynamic nature of cyber threats like phishing and malware. Demographic and psychographic factors further complicate this landscape, necessitating tailored educational approaches.

This chapter has synthesized key findings from recent academic studies, highlighting the pervasive nature of mobile security threats, the complexities of user engagement with security features, and the nuanced influences of individual characteristics on security practices. It reinforces the consensus that effective educational interventions are paramount to empowering users with the knowledge, skills, and motivation to navigate the digital world securely. By addressing the identified gaps and embracing innovative approaches to security education and design, the collective aim is to cultivate a more security-conscious user base, thereby fortifying the overall resilience of the smartphone ecosystem against ever-present cyber risks. The empirical analysis presented in the subsequent chapters will build upon this comprehensive literature review, offering specific insights into the security awareness levels and practices of smartphone users within the context of this ongoing global challenge.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter delineates the methodological framework employed to investigate the security awareness levels of smartphone users. It provides a comprehensive exposition of research design, participant selection, instrumentation, data collection procedures, and statistical analysis techniques. The aim is to establish a robust and transparent foundation for the empirical findings presented in subsequent chapters, ensuring the study's rigor, reliability, and validity. The choices made in this methodological approach are directly informed by the study's overarching objective: to descriptively analyze the security awareness levels of smartphone users and identify key behavioral patterns and vulnerabilities.

3.2 Research Design

This study adopted a quantitative research design, primarily utilizing a descriptive and cross-sectional survey approach. This design was selected as the most appropriate method to achieve the research objectives, particularly given the exploratory nature of assessing current security awareness levels and practices among a defined population of smartphone users. A quantitative approach was chosen to enable the systematic collection of numerical data, allowing for statistical analysis to identify patterns, relationships, and differences within the dataset.

The descriptive component of the research design aims to accurately portray the characteristics of the population concerning smartphone security awareness and practices. This involves summarizing the collected data through frequencies, percentages, and central tendencies, providing a snapshot of the current state of affairs.

Furthermore, a cross-sectional design was employed, meaning data were collected from a sample of individuals at a single point in time. This approach is efficient for gathering information from a large number of participants simultaneously and is well-suited for descriptive studies aiming to assess prevalence or current attitudes and behaviors. For the purpose of understanding the current landscape of smartphone security awareness, this design offers a practical and effective means of data acquisition.

3.3 Population and Sampling

The target population for this study comprised smartphone users, given the research's focus on their security awareness level. Within this broad demographic, a specific focus was placed on individuals within the 18 to 30 age group, as this demographic represents a significant proportion of active smartphone users, often exhibiting distinct usage patterns and levels of technological engagement. University students formed a substantial segment of the participant pool, reflecting their high reliance on smartphones for academic, social, and personal activities.

A convenience sampling method was utilized for participant recruitment. This non-probability sampling technique involved selecting participants who were readily accessible and willing to participate in the study. Recruitment efforts leveraged both online platforms (e.g., social media groups, SurveyMonkey distribution) and in-person interviews within accessible community and university networks. The convenience sampling approach was chosen due to practical constraints, including time, resources, and accessibility to a diverse pool of smartphone users.

While convenience sampling offers advantages in terms of feasibility and cost-effectiveness, it is acknowledged that this method may introduce sampling bias. The sample may not be fully representative of the entire global smartphone user population, potentially limiting the generalizability of the findings. To mitigate this limitation and enhance the diversity of the sample, efforts were made to include participants from various demographic backgrounds and nationalities, as evidenced by the representation from Turkey, Somalia, Sudan, Djibouti, and other nations. The final sample consisted of 145 individuals. While this sample size is adequate for statistical analysis, particularly for descriptive statistics and chi-square tests, it is important to interpret the inferential findings with an understanding of the sampling method's inherent limitations. Future research could explore probability sampling techniques to enhance generalizability.

The demographic composition of the sample, as detailed in Chapter 4, included a near-equal gender distribution (51% male, 49% female) and a range of educational levels from high school to master’s degrees, with university students comprising the majority (69%). This diversity, despite the convenience sampling approach, allowed for meaningful comparisons of security awareness and practices across different demographic subgroups, providing a richer understanding of the factors influencing smartphone security behavior.

3.4 Instrumentation

The primary data collection tool for this study was a structured questionnaire, meticulously designed to gather comprehensive information on smartphone users' security awareness, habits, and practices. The development of this instrument was guided by a thorough review of existing literature on cybersecurity, mobile security, and user behavior, as well as adherence to established cybersecurity standards and best practices. This approach ensured that the questionnaire items were relevant, comprehensive, and aligned with the study's research objectives.

The questionnaire comprised 55 items, categorized into several key sections to systematically capture various facets of smartphone security:

1. Demographic Details: This section collected essential background information about participants, including age range, gender, education level, nationality, and current country of residence. These variables served as independent variables for exploring their influence on security awareness and practices.

2. Usage Habits: Questions in this section explored participants' general smartphone usage patterns, such as their device's operating system, frequency of Bluetooth and GPS use, and general device handling habits (e.g., always in possession, sometimes left unattended).

3. Security Awareness: This section assessed participants' knowledge and understanding of fundamental cybersecurity concepts, their ability to recognize phishing attempts, and their familiarity with various built-in and third-party smartphone security tools.

4. Security Practices: This crucial section delved into participants' actual behaviors related to smartphone security. It included items on lock screen habits (e.g., type of lock, auto-lock duration, PIN complexity, update frequency), data backup routines (e.g., frequency, methods), encryption use, and behaviors when using public Wi-Fi networks.
5. Behavioral Metrics: This section captured participants' responses to critical security prompts and encounters, such as their likelihood of installing OS updates immediately, their experiences with phishing encounters, and their general information protection practices.

The questionnaire employed a combination of closed-ended questions, Likert scales, and multiple-choice items. Closed-ended questions (e.g., Yes/No) were used for straightforward factual inquiries. Likert scales (e.g., "Strongly Agree" to "Strongly Disagree," or "Very Confident" to "Not Confident") were instrumental in measuring attitudes, perceptions, and self-assessed levels of awareness and confidence. Multiple-choice questions allowed participants to select from a predefined set of options, ensuring consistency in responses and facilitating quantitative analysis. This mix of question types was chosen to ensure comprehensive data collection while minimizing response bias and enhancing the ease of completion for participants.

Validity and Reliability:

To ensure the quality and robustness of the questionnaire, measures for both validity and reliability were incorporated:

- Content Validity: The questionnaire items were developed based on a thorough review of relevant academic literature and established cybersecurity guidelines. This process aimed at ensuring that the survey comprehensively covered the key dimensions of smartphone security awareness and practices as defined by the research objectives. While not explicitly stated in the original outline, typically, expert review (e.g., by cybersecurity professionals or academics in the field) would be conducted to further validate the content's relevance and clarity.

- Pilot Testing: A pilot test was conducted with a small sample of 10 participants prior to the full survey deployment. The primary objectives of the pilot test were to:
  - Assess the clarity, comprehensibility, and unambiguousness of each questionnaire item.
  - Identify any potential ambiguities, confusing language, or technical jargon that might hinder participant understanding.
  - Evaluate the flow and logical sequence of the questions.
  - Determine the approximate time required for completion.
  - Based on feedback from the pilot test, minor refinements were made to the questionnaire to improve item clarity and overall instrument reliability, ensuring a smoother and more effective data collection process for the main study.
- Reliability Testing (Internal Consistency): The internal consistency of multi-item measures within the questionnaire was assessed using Cronbach's Alpha (α). This statistical measure evaluates the extent to which all items on a scale consistently measure the same underlying construct. A Cronbach's Alpha coefficient of 0.70 or higher is generally considered acceptable in social science research, indicating good internal consistency. This analysis was performed post-data collection as part of the statistical methods, ensuring that the scales used to measure constructs like "security awareness" or "security practices" were reliable.

The complete questionnaire is provided in Appendix, offering full transparency regarding the instrument used in this study.

3.5 Data Collection Procedures

The data collection process was meticulously planned and executed to ensure both efficiency and ethical compliance. A multi-modal approach was adopted, combining online distribution with in-person interviews to maximize reach and accommodate diverse participant preferences.

Online Distribution: The primary method of data collection was through an online survey platform, SurveyMonkey. This platform was chosen for its user-friendly interface, robust data management capabilities, and ability to ensure participant anonymity. Survey links were disseminated through various digital channels, including:

- Social Media Platforms: Links were shared on relevant social media groups and networks, targeting communities interested in technology, cybersecurity, or general university student groups. This allowed for broad dissemination and self-selection by interested individuals.
- University Networks: Collaboration with university departments and student organizations facilitated the distribution of the survey link to a concentrated population of students and faculty, ensuring a strong representation from the academic community.
- Community Outreach: Where appropriate, links were shared with broader online communities and forums related to technology and consumer behavior.

In-person Interviews: To complement the online data collection and reach participants who might not be active on online platforms or prefer direct interaction, a limited number of in-person interviews were conducted. These interviews followed the exact same structured questionnaire to maintain consistency in data collection. The interviewer ensured a standardized administration process, reading questions clearly and recording responses accurately. This dual approach helped to capture a more diverse range of perspectives and potentially reduce biases associated with solely online surveys.

Participation Process:

- Informed Consent: Prior to commencing the survey, all participants, whether online or in-person, were presented with a clear and concise informed consent statement. This statement outlined the purpose of the study, the voluntary nature of their participation, the estimated time required (10–15 minutes), and assurances regarding data confidentiality and anonymity. Participants were required to indicate their consent before proceeding with the questionnaire.

- Anonymity and Confidentiality: Strict measures were implemented to ensure the anonymity and confidentiality of participant responses. For online surveys, no personally identifiable information was collected. For in-person interviews, responses were recorded in a manner that prevented direct linkage to individuals. All collected data were stored securely on password-protected systems, accessible only to the primary researcher, thereby safeguarding participant privacy.
- Data Collection Period: The full survey was deployed over a four-week period. This duration was deemed sufficient to gather a substantial number of responses while minimizing the impact of any external events that might influence participant attitudes or behaviors during a prolonged collection phase.

The combination of online and in-person methods, coupled with rigorous ethical protocols, aimed to ensure a comprehensive and responsible data collection process for this study.

3.6 Data Analysis

The collected quantitative data were meticulously analyzed using IBM SPSS Statistics, Version 24. This statistical software package was selected for its robust capabilities in handling large datasets and performing a wide array of statistical analyses, aligning perfectly with the study's quantitative research design. The data analysis process involved descriptive statistical techniques to address the research questions comprehensively.

Descriptive Analysis:

Descriptive statistics were employed to summarize and describe the basic features of the data collected from the 145 participants. This initial phase of analysis provided a clear overview of the sample's characteristics and the general patterns observed in smartphone security awareness and practices. Specific descriptive measures included:

- **Frequencies and Percentages:** Used to illustrate the distribution of categorical variables, such as demographic characteristics (e.g., age, gender, nationality, education level) and responses to multiple-choice questions (e.g., types of lock settings used, backup methods).

- **Mean Scores and Standard Deviations:** Applied to continuous or Likert-scale data (e.g., self-rated security awareness, hours of Bluetooth/GPS enabled) to indicate central tendency and variability.

By systematically applying these statistical methods, the study aimed to provide a rigorous and evidence-based analysis of smartphone users' security awareness and practices, contributing valuable insights to the field of cybersecurity.

3.7 Variables and Measurement

This study involved the identification and measurement of several key variables, categorized as either independent or dependent, to address the research questions.

Independent Variables: These variables were presumed to influence or explain variations in the dependent variables. They primarily comprise demographic characteristics and general smartphone usage patterns:

- Demographic Traits:
  - Age Range: Categorized (e.g., 18–23, 24–30, etc.), measured to investigate generational differences in security awareness and practices.
  - Gender: Categorized (Male, Female, Other), examined for potential gender-based variations in security behavior.
  - Education Level: Categorized (e.g., High school graduate, University student, Master student, etc.), explored to understand the impact of formal education on security awareness.
  - Nationality/Residence: Categorical, providing context for the sample's diversity.
- Behavioral Factors/Usage Habits:
  - Operating System (OS): Categorical (iOS, Android, Other), to assess if OS choice correlates with security practices.

- Public Wi-Fi Usage: Categorical (e.g., "Yes, always," "Yes, with encryption," "No"), to gauge risk-taking behavior.
- Bluetooth/GPS Usage: Measured in hours per day, to assess continuous exposure to potential vulnerabilities.
- Default Browser Settings Modification: Binary (Yes/No), indicating proactive security configuration.

Dependent Variables: These variables were the outcomes or phenomena being measured and explained by the independent variables. They directly addressed the core aspects of smartphone security awareness and practices:

- Users' Security Awareness: Self-rated (Likert scale: Very Low to Very High) and inferred from responses to questions about cybersecurity familiarity and recognition of threats (e.g., phishing). This directly addresses RQ1.
- Screen Lock Choices and Practices: Categorical (e.g., Fingerprint, PIN, Face, None) and interval (e.g., auto-lock duration, PIN complexity, frequency of updating lock settings). This directly addresses RQ2.
- Data Backup Frequency and Methods: Categorical (e.g., Never, Once a month, Cloud, External hard drive) and binary (regularly back up data). This addresses RQ4.
- Susceptibility to Phishing Attacks: Binary (Yes/No for falling victim) and Likert-scale (confidence in identifying phishing). This addresses aspects of RQ3 and RQ5.
- Adherence to Data Security Best Practices (beyond locking): Inferred from responses regarding storing sensitive information (e.g., SSN, wallet apps), use of protective applications (VPN, Virus Scanner), and device encryption status. This addresses RQ3 and RQ5.
- Prioritization of Hard vs. Soft Security: Inferred from comparative analysis of responses related to physical device security (lock settings, possession habits)

versus data privacy and online account protection (e.g., SSN entry, phishing vigilance, encryption). This directly addresses RQ5.

All variables were operationalized through the 55-item structured questionnaire, utilizing appropriate measurement scales (nominal, ordinal, ratio) to facilitate quantitative analysis. The specific questions corresponding to each variable are detailed in Appendix.

3.8 Ethical Considerations

The ethical conduct of this research was paramount throughout all stages of the study, from design to data analysis and reporting. Adherence to ethical guidelines ensured the protection of participants' rights, privacy, and well-being. The following key ethical considerations were rigorously observed:

- **Informed Consent:** Prior to any data collection, all participants were provided with a clear and comprehensive informed consent form. This form explicitly outlined the study's purpose, research objectives, the voluntary nature of participation, the estimated time commitment, and the procedures for data collection and storage. Participants were assured that they could withdraw from the study at any point without penalty. For online surveys, consent was obtained through an explicit agreement click-through before accessing the questionnaire. For in-person interviews, verbal consent was obtained and documented after the participant read and understood the consent form.
- **Anonymity and Confidentiality:** To safeguard participant privacy, strict measures were implemented to ensure anonymity and confidentiality. No personally identifiable information (such as names, email addresses, or specific IP addresses) was collected during the survey. Responses were recorded in an aggregated and de-identified manner. All collected data were stored securely on password-protected university servers, accessible only to the primary researcher. This approach minimized the risk of data breaches and ensured that individual responses could not be linked back to specific participants.
- **Data Security and Storage:** All raw data collected were encrypted and stored in a secure, restricted-access database. Access to the data was limited exclusively to

the research team for the purpose of analysis. Upon completion of the thesis and after a defined retention period, the data will be securely archived or permanently deleted in accordance with university policies and data protection regulations.

- Minimization of Harm: The study design aimed to minimize any potential discomfort or harm to participants. The questions were non-sensitive and did not delve into highly personal or distressing topics. The voluntary and anonymous nature of participation further ensured that individuals felt no pressure to disclose information they were uncomfortable sharing.

By diligently addressing these ethical considerations, the study upheld the highest standards of research integrity and participant protection.

3.9 Limitations of the Methodology

While this study employed a rigorous methodological approach to investigate smartphone security awareness, it is important to acknowledge several inherent limitations that may influence the interpretation and generalizability of the findings.

- Self-Reporting Bias: The primary data collection method relied on self-reported information through a questionnaire. This can introduce various forms of bias. Participants may:
    - Social Desirability Bias: Tend to provide responses that they perceive as socially acceptable or desirable, rather than their actual behaviors or knowledge, particularly concerning security practices they know they should follow.
    - Recall Bias: Have difficulty accurately recalling past behaviors or the precise frequency of certain actions (e.g., how often they update lock settings or experience unsolicited messages).
    - Overconfidence Bias: Overestimate their own security awareness or their ability to identify threats, leading to discrepancies between perceived and actual competence. These biases could potentially lead to an overestimation of security awareness and best practices among the study population. Future

research could incorporate observational methods or technical assessments (with appropriate ethical safeguards) to complement self-reported data and provide a more objective measure of security behaviors.

- Cross-Sectional Design: As a cross-sectional study, data were collected at a single point in time. This design inherently limits the ability to:
  - Establish Causality: While relationships and correlations between variables can be identified (e.g., between age and certain security practices), it is not possible to definitively determine cause-and-effect relationships. For instance, it cannot be concluded whether higher awareness causes better practices or if engaging in practices leads to higher awareness.
  - Track Changes Over Time: The study cannot capture how participants' security awareness or behaviors evolve in response to new threats, technological advancements, or educational interventions. Longitudinal studies would be necessary to observe such dynamic changes.
- Convenience Sampling: The use of convenience sampling, while practical, introduces limitations regarding the generalizability of the findings. The sample, primarily consisting of university students and individuals accessible through online and community networks, may not fully represent the broader population of smartphone users globally or even within specific regions. Factors such as socioeconomic status, digital literacy levels outside academic environments, or cultural nuances not captured in the diverse but still convenience-based sample, might influence security awareness and practices differently. Therefore, the findings should be interpreted with caution and may not be directly transferable to other populations without further validation.
- Geographic and Cultural Specificity: While the sample included participants from various nationalities, the primary recruitment was likely concentrated within specific geographic or cultural contexts (e.g., Turkey and surrounding regions). Security awareness and behavior can be influenced by local cybersecurity landscapes, prevalent threats, and cultural attitudes towards privacy and

technology. The study's findings may therefore reflect these specific contexts and might not be universally applicable.

- Questionnaire Scope: While comprehensive, a 55-item questionnaire, by its nature, cannot delve into every conceivable aspect of smartphone security. Certain niche threats, advanced security configurations, or highly specific behavioral nuances might not have been fully captured.

These limitations underscore the need for future research to build upon the findings of this study, employing diverse methodologies, larger and more representative samples, and longitudinal designs to provide a more holistic understanding of smartphone security awareness.

3.10 Chapter Summary

This chapter has provided a detailed exposition of the methodology employed in this empirical analysis of smartphone users' security awareness. Adopting a quantitative, descriptive, and cross-sectional research design, the study utilized a structured, 55-item questionnaire administered to a convenience sample of 145 smartphone users, primarily within the 18-30 age demographic. Rigorous measures were taken to ensure the validity and reliability of the instrument, including pilot testing and the application of Cronbach's Alpha. Data collection adhered to strict ethical guidelines, emphasizing informed consent, anonymity, and data confidentiality. The collected data were analyzed using SPSS Version 24, employing descriptive statistics, chi-square tests, and cross-tabulations to explore awareness levels, behavioral patterns, and relationships between demographic variables and security practices. While acknowledging the limitations inherent in self-reported data, a cross-sectional design, and convenience sampling, this methodological framework provides a robust foundation for the study's findings and contributes valuable insights to the ongoing discourse on smartphone security.

CHAPTER 4

RESULTS BASED ON DESCRIPTIVE STATISTICS

This chapter presents the descriptive statistical findings obtained from the survey responses. It provides a summary of participants' demographic profiles and examines key aspects of their smartphone security behaviors and awareness levels. The data highlight general trends and patterns that help frame the users' security practices, forming the basis for deeper analysis in the next chapter.

4.1. Demographics

Table 4.1 Participant demographics

		n	%
Where are you from?	Turkey	55	37,9
	Somalia	12	8,3
	Sudan	7	4,8
	Djibouti	6	4,1
	Jordan	5	3,4
	Kenya	5	3,4
	Yemen	5	3,4
	Iraq	4	2,8
	Pakistan	4	2,8
	Saudi Arabia	4	2,8
	Algeria	3	2,1
	Iran	3	2,1
	Morocco	3	2,1
	Nigeria	3	2,1
	Palestine	3	2,1
	Qatar	3	2,1

Table 4.1 Participant demographics (continued)

	Syria	3	2,1
	Egypt	2	1,4
	United Kingdom	2	1,4
	Afghanistan	1	0,7
	Albania	1	0,7
	Around the world	1	0,7
	Azerbaijan	1	0,7
	Bahrain	1	0,7
	Kuwait	1	0,7
	Lebanon	1	0,7
	Libya	1	0,7
	Oman	1	0,7
	Tunisia	1	0,7
	Uruguay	1	0,7
	US	1	0,7
	Uzbekistan	1	0,7
Which age range do you fall under?	18–23	83	57,2
	24–30	62	42,8
What is your gender?	Male	74	51,0
	Female	57	49
What is the highest level of education that you have accomplished?	University student	100	69,0
	University graduate	24	16,6
	Master student	13	9,0
	High school graduate	4	2,8
	Master graduate	3	2,1
	High school student	1	0,7

The demographic characteristics of the participants are summarized in Table 4.1. A total of 145 respondents participated in the study, with the majority being from Turkey (37.9%). Participants also hailed from various other countries, including Somalia (8.3%), Sudan (4.8%), Djibouti (4.1%), and Jordan, Kenya, and Yemen, each representing 3.4%

of the sample. The remaining participants were distributed across multiple countries, each accounting for less than 3% of the sample. Countries with the lowest representation (0.7% each) included Afghanistan, Albania, Azerbaijan, Bahrain, Kuwait, Lebanon, Libya, Oman, Tunisia, Uruguay, the United States, and Uzbekistan, among others.

In terms of age distribution, the majority of participants fell within the 18–23 age range (57.2%), followed by those aged 24–30 years (42.8%). Gender distribution showed a slightly higher proportion of male participants (51.0%) compared to female participants (39.3%).

Regarding educational background, the majority of participants were university students, constituting 69.0% of the sample. This was followed by university graduates (16.6%), master's students (9.0%), and high school graduates (2.8%). Master's graduates and high school students were the least represented groups, comprising 2.1% and 0.7% of the sample, respectively.

4.2. Device Ownership and Usage (like network and connectivity)

Table 4.2 Smartphone ownership and usage

		n	%
Do you have a smartphone?	Yes	145	100,0
If you answered yes to question 6, which operating system (OS) is your phone running?	Android	75	51,7
	iOS	67	46,2
	Other (please specify)	1	0,7
My mobile phone	Is always in my possession	134	92,4
	Is sometimes left unattended (e.g., occasionally I forget it on my desk; leave it on the bar when going to the restroom)	8	5,5
	Is often left unattended (e.g., is on my desk during lunch break; left at home when I am out)	2	1,4
Do you use publicly available Wi-Fi's/Hotspots (e.g., at Starbucks, McDonalds, Hotels or Airports	Yes, but I use additional encryption (e.g., a VPN software)	77	53,1

Table 4.2 Smartphone ownership and usage (continued)

etc...)?	Yes, but only for browsing; no sensitive information is transferred (e.g., I am not using Banking Apps)	41	28,3
	Yes, always	19	13,1
	No, I don't use Public WiFi's	7	4,8
Does your device automatically connect to Wi-Fi networks?	Yes, to known ones (the ones I accessed in the past)	126	86,9
	Yes, to any open Wi-Fi	9	6,2
	No	5	3,4
	I'm not sure	2	1,4
On average, how many hours a day is your Bluetooth enabled?	24 hours	8	5,5
	Between 2 and 4 hours	16	11,0
	Between 4 and 8 hours	7	4,8
	Between 8 and 12 hours	1	0,7
	I'm not sure	4	2,8
	Less than 2 hours	100	69,0
	Never	9	6,2
On average, how many hours a day is your location/GPS enabled?	24 hours	9	6,2
	Between 2 and 4 hours	67	46,2
	Between 4 and 8 hours	8	5,5
	Between 8 and 12 hours	2	1,4
	I'm not sure	8	5,5
	Less than 2 hours	41	28,3
	Never	10	6,9

The data presented in Table 4.2 provide insights into participants' smartphone ownership and usage habits. All respondents (100.0%) reported owning a smartphone, establishing a uniform baseline for the analysis.

When I asked about the operating system (OS) of their smartphones, the majority indicated using Android devices (51.7%), followed closely by iOS users, who comprised

46.2% of the sample. A negligible proportion (0.7%) reported using other operating systems.

Regarding the possession habits of their mobile phones, most participants (92.4%) stated that their smartphones are always in their possession. A smaller proportion (5.5%) admitted that their phones are sometimes left unattended, such as when temporarily forgotten on a desk or a bar. Only 1.4% of respondents reported often leaving their phones unattended, such as on a desk during a lunch break or at home while they are out.

A majority of participants (53.1%) reported using public Wi-Fi networks or hotspots with additional encryption measures, such as VPN software, reflecting a relatively high level of security awareness. Meanwhile, 28.3% stated they use public Wi-Fi only for browsing purposes and avoid transferring sensitive information, such as banking activities. A smaller percentage (13.1%) admitted to always using public Wi-Fi without specific precautions. Notably, 4.8% of participants reported completely avoiding public Wi-Fi usage, demonstrating a cautious approach to potential security risks.

Regarding automatic connection settings, most participants (86.9%) indicated that their devices automatically connect only to previously accessed (known) Wi-Fi networks. However, 6.2% allowed their devices to connect to any open Wi-Fi network, potentially increasing their exposure to security risks. A minority (3.4%) disabled automatic connections altogether, while 1.4% were unsure of their device's connection settings.

Regarding Bluetooth usage, the majority of participants (69.0%) reported enabling Bluetooth for less than 2 hours per day, indicating a conscious effort to minimize exposure to potential security vulnerabilities. A smaller proportion (11.0%) used Bluetooth between 2 and 4 hours daily, while 4.8% reported usage between 4 and 8 hours. Only 5.5% of participants kept Bluetooth enabled for the entire day (24 hours). Notably, 6.2% of respondents never enabled Bluetooth, and 2.8% were unsure about their usage patterns.

In terms of location/GPS services, 46.2% of participants indicated enabling this feature for 2 to 4 hours daily, representing the largest group. Another 28.3% limited their GPS usage to less than 2 hours per day, while 5.5% used it for 4 to 8 hours. A small proportion

(6.2%) reported keeping GPS enabled for 24 hours daily. Interestingly, 6.9% of participants stated that they never used location services, and 5.5% were unsure of their usage habits.

Regarding device preference, Android was slightly more popular among the younger age group (18-23) at 54.2%, while iOS was favored by the older group (24-30) at 51.6%. "Other" operating systems had minimal representation in both groups. Across both age groups, a high percentage of participants reported always having their phone with them (92.8% for 18-23 and 91.9% for 24-30). Instances of leaving phones unattended were rare.

Both age groups frequently used public Wi-Fi with added encryption like a VPN, with the 24-30 age group showing slightly higher usage (59.7%) compared to the 18-23 group (48.2%). A significant portion also used public Wi-Fi only for Browse, avoiding sensitive information transfers. Most participants in both groups had their devices set to automatically connect to known Wi-Fi networks (86.7% for 18-23 and 87.1% for 24-30). Very few allowed automatic connections to any open Wi-Fi or were unsure of their settings.

For Bluetooth usage, the majority in both age groups enabled it for less than two hours per day (66.3% for 18-23 and 72.6% for 24-30). A small percentage never enabled Bluetooth. GPS usage showed notable differences: 37.3% of 18-23-year-olds used it for 2-4 hours daily, compared to 58.1% of 24-30-year-olds. The younger group relied less on GPS, with 36.1% using it for less than two hours daily, versus 17.7% in the older group. VPN usage was slightly higher in the 24-30 age group (83.9%) compared to the 18-23 group (71.1%). Virus scanner usage was consistent, with about three-quarters of both groups using this tool. Most devices in both groups were encrypted by default (73.5% for 18-23 and 75.8% for 24-30). A small number manually enabled encryption or had unencrypted devices.

When comparing by gender, females predominantly used iOS (75.4%), while males mostly used Android devices (71.6%). The "Other" category was negligible for both.

Males reported having their phones in possession more often (97.3%) than females (93.0%). Females were slightly more likely to sometimes leave their phones unattended (5.3%), a behavior not reported by males. Both genders commonly used public Wi-Fi with encryption (56.1% for females and 54.1% for males). Males were slightly more likely to always use public Wi-Fi or avoid it entirely. Most devices for both genders automatically connected to known Wi-Fi networks. However, males were more likely to be unsure about their settings or allow automatic connections to any open Wi-Fi. Both genders typically used Bluetooth for less than two hours daily. Males, however, were slightly more prone to using Bluetooth for longer durations (4-8 hours or 24 hours). Females used GPS for 2-4 hours daily more often (66.7%) than males (37.8%). Males were more likely to use GPS for less than two hours or continuously for 24 hours

4.3. Lock settings and Device security

Table 4.3 Lock settings and security preferences

		n	%
Do you enter your Social Security Number on your device? - Mobile Phone	No, I've never entered it	99	68,3
	Yes, I enter it when needed	38	26,2
	Yes, it is stored on my device	7	4,8
Which lock settings do you have in place on your phone? (check all that apply)	Fingerprint	108	74,5
	Pin (4 digits or less)	81	55,9
	Face	74	51,0
	Pin (5 digits or more)	60	41,4
	Voice	2	1,4
Would you use a different lock setting if it was available on your phone? (check all that apply)	Fingerprint	105	72,4
	Face	93	64,1
How long after inactivity on your device does your device become locked?	1 Minute	97	66,9
	2 Minutes	8	5,5
	3 Minutes	2	1,4
	30 Seconds	30	20,7
	4 Minutes	1	0,7

Table 4.3 Lock settings and security preferences (continued)

	5 Minutes	2	1,4
	More than 5 minutes	1	0,7
	Never	3	2,1
If you use a pin (numbers only) to lock/unlock your device, how many different digits does your pin consist of?	Four (e.g., 4567 or 8403)	75	51,7
	More than four	49	33,8
	None of the above	6	4,1
	One (e.g., 1111 or 2222)	4	2,8
	Three (e.g., 4432 or 4899)	8	5,5
	Two (e.g., 1122 or 5656)	3	2,1
How often do you update your lock settings? (e.g., Change your pin from 0000 to 1111)	About every 30 days	5	3,4
	About every 6 months	77	53,1
	About every 90 days	25	17,2
	About every year	3	2,1
	Never	5	3,4
	When given a reason to (i.e., someone knows your passcode)	28	19,3
Which reasoning best explains why you chose the lock settings that you have?	Convenience	17	11,7
	Default Phone Settings	2	1,4
	Forgetfulness	3	2,1
	No opinion	6	4,1
	Security	117	80,7
Do you favor biometric lock options (e.g., fingerprint) over knowledge-based options (e.g., password)?	Yes	131	90,3
	No	10	6,9

Regarding the entry of Social Security Numbers (SSNs) on mobile phones, a majority (68.3%) reported never entering their SSN into their devices. However, 26.2% indicated that they entered it when necessary, and 4.8% stored it on their devices, which may pose security risks if proper precautions are not in place.

For phone lock settings, fingerprint authentication emerged as the most commonly used method, adopted by 74.5% of participants. Other frequently used lock methods included PINs with 4 digits or fewer (55.9%), face recognition (51.0%), and PINs with 5 or more digits (41.4%). Voice authentication was the least utilized, with only 1.4% of participants reporting its use. When asked about preferred alternative lock settings, 72.4% expressed interest in using fingerprint authentication, and 64.1% preferred face recognition, indicating these methods' perceived convenience and reliability.

Regarding the time taken for devices to lock after inactivity, the majority of participants (66.9%) reported that their devices lock after 1 minute, indicating a widespread adherence to quick locking practices for enhanced security. A smaller proportion reported shorter durations, with 20.7% opting for a 30-second auto-lock. Other durations included 2 minutes (5.5%), 3 minutes (1.4%), 4 minutes (0.7%), and 5 minutes (1.4%). A minimal percentage of participants (0.7%) set their devices to lock after more than 5 minutes, and 2.1% stated that their devices never lock automatically, representing a potential security risk.

In terms of PIN complexity, most participants (51.7%) reported using four-digit PINs for locking/unlocking their devices. A significant proportion (33.8%) used PINs with more than four digits, reflecting a preference for enhanced security. A small number of participants reported using less secure options, such as one-digit PINs (2.8%), two-digit PINs (2.1%), and three-digit PINs (5.5%).

When asked about the frequency of updating lock settings, the majority (53.1%) updated their settings approximately every six months, reflecting a periodic approach to maintaining security. Other participants updated their settings every 90 days (17.2%) or every 30 days (3.4%). A small percentage updated their lock settings only when necessary (19.3%), such as when someone learned their passcode, while 3.4% reported never updating their settings, and 2.1% updated them approximately once a year.

When asked about the primary reasoning for their chosen lock settings, the majority of participants (80.7%) cited security as the key factor, reflecting a strong awareness of the importance of protecting their devices. Other reasons included convenience (11.7%), no specific opinion (4.1%), forgetfulness (2.1%), and default phone settings (1.4%).

An overwhelming majority (90.3%) preferred biometric lock options like fingerprints over knowledge-based options such as passwords, valuing their convenience and effectiveness. Only a small proportion (6.9%) preferred knowledge-based options. Most participants in both age groups enabled message previews on their locked screens (75.9% for 18-23 and 79.0% for 24-30). Face recognition was more common among the 24-30 age group (59.7%) than the 18-23 group (44.6%). Both age groups showed strong interest in using fingerprint (67.5% for 18-23 and 79.0% for 24-30) and face recognition (61.4% for 18-23 and 67.7% for 24-30).

For lock duration, 72.3% of 18-23-year-olds set it to 1 minute, compared to 59.7% of 24-30-year-olds. A 30-second lock duration was more common in the older group (30.6%) than the younger group (13.3%). Four-digit PINs were the most popular in both age groups (49.4% for 18-23 and 54.8% for 24-30), followed by PINs with more than four digits. Updating lock settings approximately every six months was the most common practice in both age groups. A large majority in both age groups favored biometric options (88.0% for 18-23 and 93.5% for 24-30).

Females were more likely to have message previews enabled on their locked screens (91.2%) compared to males (73.0%). Males were more likely to disable this feature. For PINs, more females used four digits or less (77.2%) compared to males (45.9%). Conversely, males were more likely to use PINs with five or more digits (52.7%). Both genders frequently used fingerprint locks, with slightly higher rates among females (80.7%). Face recognition was significantly more common among females (82.5%) than males (32.4%). Similarly, females were more likely to prefer using fingerprint locks (82.5%) and face recognition (84.2%) compared to males. Both genders commonly set their devices to lock after 1 minute, with males reporting a higher rate (75.7%). However, females were more likely to choose a 30-second lock duration (22.8%). Females predominantly used simpler four-digit PINs (75.4%), while males preferred longer PINs. Other PIN configurations were infrequent. Males were more likely to update their lock settings every six months (66.2%), whereas females were more likely to update every 90 days (36.8%). A small proportion of males never updated their lock settings, which was not observed among females. Security was the primary reason for lock settings for both genders, with similar proportions. Convenience was more frequently cited by males

(12.2%) than females (7.0%). A large majority in both groups preferred biometric locks, with females showing a slightly higher preference (94.7%).

4.4. Data Storage and Backup

Table 4.4 PIN preferences and lock timeout settings

		n	%
Which of the following information do you store on your phone? (check all that apply)	Email	136	93,8
	Contacts	133	91,7
	Social Media Applications (i.e. Facebook, Twitter, Snapchat)	132	91,0
	Personal Photographs	130	89,7
	Wallet (i.e. Apple pay, Samsung pay, Android Pay)	47	32,4
How often do you perform backups on your Mobile phone?	Never	8	5,5
	Once a month	21	14,5
	Once a week	11	7,6
	Once a year	5	3,4
	Once every 3 months	66	45,5
	Twice a year	16	11,0
	When prompted by my device	16	11,0
Do you regularly back up the data on your smartphone (e.g., using cloud services, an external hard drive, or local backups)?	Sometimes	76	52,4
	Always	59	40,7
	Never	7	4,8
	I don't know how to back up my data	1	0,7
Which method do you primarily use to back up the data on your smartphone?	Google Drive (for Android users)	82	56,6
	iCloud (for iOS users)	56	38,6
Have you ever experienced a security breach or data loss on your smartphone (e.g., unauthorized access, data theft, malware, etc.)?	No	132	91,0
	Yes	8	5,5
	I'm not sure	4	2,8

In terms of the types of information stored on their smartphones, email accounts were the most commonly stored data (93.8%), followed closely by contacts (91.7%), social media applications (91.0%), and personal photographs (89.7%). Conversely, digital wallets (e.g., Apple Pay, Samsung Pay) were stored by 32.4% of participants, indicating a relatively lower adoption of this feature.

When asked about backup frequency, the largest group of participants (45.5%) reported performing backups once every three months, indicating a periodic but consistent approach to data security. Other common practices included backing up once a month (14.5%) and twice a year (11.0%). A smaller proportion backed up weekly (7.6%), yearly (3.4%), or only when prompted by their device (11.0%). Notably, 5.5% of participants stated they never performed backups, representing a potential security vulnerability.

For data backup practices, the largest group (52.4%) stated they occasionally backed up their data, while 40.7% always performed regular backups. A small number (4.8%) reported never backing up their data, and 0.7% admitted they did not know how to back up their data, highlighting an area for potential education.

Regarding data backup methods, the majority of participants (56.6%) primarily used Google Drive, reflecting the prevalence of Android users in the sample. Another significant portion (38.6%) used iCloud, aligning with iOS users.

Finally, when asked about experiences with security breaches or data loss, an overwhelming majority (91.0%) reported no such incidents, suggesting effective protective measures among most participants. However, 5.5% had experienced breaches or losses, and 2.8% were unsure, emphasizing the importance of continued vigilance.

Participants aged 24-30 were more likely to store digital wallets (45.2%) than those aged 18-23 (22.9%), suggesting higher adoption of mobile payment technologies in the older group. The most common backup frequency for both age groups was once every three months. The majority in both age groups reported never entering their Social Security Numbers (SSNs). A higher proportion of 24-30-year-olds always backed up their data (51.6%) compared to 18-23-year-olds (32.5%). "Sometimes" was the most common response for the younger group. Instances of never backing up data were minimal. Most participants in both groups regularly engaged in some form of data backup. iCloud usage was slightly higher in the 24-30 age group (43.5%). Google Drive was the most commonly used backup method across both age groups. Participants aged 24-30 were more likely to report no data loss due to regular backups (80.6%). However, a higher percentage of 18-23-year-olds reported experiencing data loss (15.7%), indicating a potential gap in consistent backup practices among the younger group.

Both genders frequently stored contacts and email data, with similar high percentages. Females were significantly more likely to store wallet applications (66.7%) compared to males (9.5%). The most common backup frequency for females was once every three months (57.9%), while males were more likely to back up twice a year (20.3%). Females were slightly more likely to back up when prompted by their devices. The majority in both groups reported never entering their SSNs. Neither group reported a lack of knowledge about data backup. However, a small proportion of males (2.7%) were unsure if they regularly backed up their data, which was not observed among females. Females were more likely to use iCloud for backups (66.7%), while males showed a strong preference for Google Drive (75.7%).

4.5. Updates and Maintenance

Table 4.5 Update practices and notification methods

		n	%
Did you change your default browser settings?	No	113	77,9
	Yes	25	17,2
Do you regularly update your smartphone's operating system and apps to protect against security vulnerabilities?	Yes, regularly	121	83,4
	Occasionally	16	11,0
	No	4	2,8
	I'm not sure how to do this	2	1,4
What are the primary reasons for updating your smartphone's OS? (Select all that apply)	Security patches and bug fixes	124	85,5
	New features and enhancements	50	34,5
	Improved performance and stability	117	80,7

Table 4.5 Update practices and notification methods (continued)

How do you typically receive notifications about available OS updates for your smartphone?	Automatic notifications from the device	133	91,7
	Notifications from the smartphone manufacturer	4	2,8
	Through news articles or online forums	4	2,8
	Notifications from the mobile carrier	3	2,1
When prompted to install an OS update on your smartphone, how likely are you to install it immediately?	Very likely	67	46,2
	Somewhat likely	60	41,4
	Neutral	12	8,3
	Somewhat unlikely	2	1,4
	Very unlikely	2	1,4
Have you ever delayed or skipped installing OS updates on your smartphone? If yes, what were the reasons? (Select all that apply)	Lack of time to install updates	124	85,5
	Concerns about compatibility issues with existing apps	15	10,3
What factors influence your decision to update applications on your smartphone? (Select all that apply)	Security updates and vulnerability fixes	122	84,1
	New features and functionalities	86	59,3
	Performance improvements	83	57,2
Do you believe that regularly updating your smartphone's OS and applications is essential for maintaining its security integrity?	Strongly agree	111	76,6
	Agree	16	11,0
	Neutral	16	11,0
	Disagree	1	0,7

When asked whether they changed their default browser settings, the majority of participants (77.9%) reported not making any changes, while 17.2% indicated they had modified these settings, reflecting some awareness of browser security customization.

For updating their smartphone’s operating system and applications to address security vulnerabilities, the majority of participants (83.4%) reported updating regularly, demonstrating a strong commitment to maintaining device security. A smaller percentage (11.0%) updated occasionally, while 2.8% admitted not updating their devices.

Additionally, 1.4% were unsure how to perform updates, highlighting a potential area for user education.

Regarding the primary reasons for updating their smartphone's OS, the majority of participants (85.5%) cited security patches and bug fixes as the main motivation, highlighting a strong focus on maintaining security. Additionally, 80.7% indicated that they update for improved performance and stability, while 34.5% were motivated by new features and enhancements.

In terms of how participants receive notifications about OS updates, the vast majority (91.7%) reported receiving automatic notifications directly from their devices. A smaller proportion received notifications from the smartphone manufacturer (2.8%), through news articles or online forums (2.8%), or from their mobile carrier (2.1%).

When prompted to install an OS update, 46.2% of participants stated they were very likely to install it immediately, while 41.4% were somewhat likely. A smaller group reported being neutral (8.3%), somewhat unlikely (1.4%), or very unlikely (1.4%) to install updates promptly.

For those who delayed or skipped installing updates, the most common reason was a lack of time (85.5%), reflecting a practical barrier to immediate adoption. A smaller proportion (10.3%) expressed concerns about compatibility issues with existing apps.

The primary factor influencing application updates for the majority of participants (84.1%) was security updates and vulnerability fixes. New features (59.3%) and performance improvements (57.2%) were also motivating factors. A large majority (76.6%) strongly agreed that regularly updating their smartphone's OS and applications is necessary for security. Updating only when there was a specific reason, such as someone learning the passcode, was more prevalent among the younger group (24.1% for 18-23 vs. 12.9% for 24-30). Most in both groups regularly updated their OS. Very few updated occasionally, not at all, or were unsure how to update. The majority relied on automatic device notifications for updates. Notifications from carriers, manufacturers, or online sources were reported by a minimal number of participants. Both groups tended to install updates promptly, with the 24-30 age group more likely to install immediately (54.8%) than the 18-23 group (39.8%). Neutral and less likely responses were uncommon. Lack of time was the most common reason for delayed updates for both groups. Concerns about compatibility were also cited. The older group (24-30) was more likely to cite this as a reason (71.0%) compared to the younger group (50.6%). However, both groups frequently cited security updates as a primary factor. The majority in both groups strongly agreed with the importance of updates.

Both genders reported high rates of regularly updating their OS and applications. Occasional updating was more common among males (9.5%) than females (8.8%). Females were more likely to cite performance and stability improvements as a reason for updating (89.5%) than males (82.4%). Security patches, bug fixes, new features, and enhancements were frequently cited by both genders with no significant differences. Females were more likely to install updates immediately (73.7%) than males (24.3%). Males were more likely to be somewhat likely to install updates. Neutral responses were higher among males. Both genders cited lack of time as the primary reason for delayed updates. Concerns about compatibility issues were less frequently cited and showed no significant differences. Security updates and vulnerability fixes were primary factors for both genders. Females were significantly more likely to update for new features and functionalities (82.5%) compared to males (41.9%). Males were more likely to prioritize performance improvements (73.0%) than females (40.4%).

4.6. Phishing and cybersecurity threats

Table 4.6 Phishing experiences and recognition skills

		n	%
Have you ever lost important data on your smartphone due to not having a backup?	No, I have not experienced data loss as I regularly back up my data.	108	74,5
	Yes, I have experienced data loss.	17	11,7
	Not sure/I don't remember.	10	6,9
	No, I have not experienced data	8	5,5

Table 4.6 Phishing experiences and recognition skills (continued)

	loss even though I do not back up my data.		
Have you ever experienced security incidents or breaches on your smartphone due to delayed or neglected updates?	No	135	93,1
	Yes	8	5,5
How confident are you in your ability to differentiate between legitimate update notifications and phishing attempts disguised as update alerts on your smartphone?	Somewhat confident	111	76,6
	Very confident	15	10,3
	Neutral	12	8,3
	Somewhat uncertain	4	2,8
	Not confident	2	1,4
How confident are you in your ability to identify potential phishing attempts on your smartphone?	Somewhat confident	103	71,0
	Very confident	21	14,5
	Neutral	19	13,1
	Somewhat uncertain	1	0,7
How often do you receive unsolicited emails or text messages asking for personal information (e.g., passwords, credit card details) on your smartphone?	Occasionally	112	77,2
	Rarely	27	18,6
	Frequently	4	2,8
	Almost daily	1	0,7
Have you ever fallen victim to a phishing attack on your smartphone?	No	133	91,7
	Yes	8	5,5
How often do you review the sender's email address or phone number before responding to an email or text message on your smartphone?	Always	121	83,4
	Sometimes	12	8,3
	Rarely	7	4,8
	Never	3	2,1
How often do you click on links or download attachments from unknown or suspicious sources on your smartphone?	Never	117	80,7
	Rarely	15	10,3
	Sometimes	7	4,8
	Often	4	2,8
When logging into sensitive accounts (e.g., banking, email), do you verify the legitimacy of the website or app	Always	127	87,6
	Sometimes	12	8,3

Table 4.6 Phishing experiences and recognition skills (continued)

before entering your login credentials on your smartphone?	Never	3	2,1
	Rarely	2	1,4

When asked about experiences with data loss due to a lack of backups, 74.5% of participants reported no data loss because they regularly backed up their data, indicating effective preventative practices. However, 11.7% acknowledged having experienced data loss, while 6.9% were unsure or did not remember. Notably, 5.5% stated they had not experienced data loss despite not performing backups, which might reflect a combination of caution and fortunate circumstances.

Regarding experiences with security incidents or breaches due to delayed or neglected updates, an overwhelming majority (93.1%) reported no such incidents, suggesting effective updating practices among most participants. However, 5.5% acknowledged experiencing security issues, emphasizing the importance of timely updates to prevent vulnerabilities.

In terms of confidence in distinguishing legitimate update notifications from phishing attempts disguised as update alerts, the majority of participants (76.6%) reported being somewhat confident in their ability. A smaller proportion (10.3%) expressed a high level of confidence, while others reported being neutral (8.3%), somewhat uncertain (2.8%), or not confident (1.4%).

Regarding their confidence in identifying potential phishing attempts on their smartphones, 71.0% of participants reported being somewhat confident, while 14.5% were very confident. Others expressed neutrality (13.1%) or slight uncertainty (0.7%), highlighting varying levels of self-assurance in their ability to detect phishing schemes.

In terms of the frequency of receiving unsolicited emails or text messages asking for personal information, the majority (77.2%) reported experiencing such occurrences occasionally. Additionally, 18.6% stated they rarely received such messages, while a smaller group encountered them frequently (2.8%) or almost daily (0.7%).

Regarding phishing attacks, the vast majority of participants (91.7%) reported never falling victim to such an attack, indicating a general effectiveness in avoiding phishing schemes. However, 5.5% acknowledged having been targeted successfully, emphasizing the need for continued education and vigilance.

In terms of reviewing the sender's email address or phone number before responding to messages, most participants (83.4%) reported always performing this check, reflecting a strong precautionary habit. A smaller percentage reviewed sender information sometimes (8.3%), rarely (4.8%), or never (2.1%).

When asked about clicking on links or downloading attachments from unknown or suspicious sources, 80.7% of participants stated they never engaged in such behaviors, while 10.3% reported rarely doing so. A minority admitted to sometimes (4.8%) or often (2.8%) interacting with potentially harmful links or attachments, indicating areas of potential risk.

Regarding verification of website or app legitimacy when logging into sensitive accounts, the majority of participants (87.6%) reported always verifying legitimacy before entering credentials, demonstrating strong security awareness. Smaller groups verified legitimacy sometimes (8.3%), never (2.1%), or rarely (1.4%).

The majority of participants in both age groups were somewhat confident in their ability to identify and avoid phishing attempts (74.7% for 18-23 and 79.0% for 24-30). "Very confident" responses were slightly higher among the younger group. Both groups predominantly reported being somewhat confident in their overall online security. "Very confident" responses were more common among the 24-30 age group (19.4%). Most in both groups occasionally received suspicious messages. Very few reported receiving such messages almost daily. The vast majority in both groups reported never being victimized by phishing (90.4% for 18-23 and 93.5% for 24-30). A small proportion were successfully targeted. The majority always reviewed sender information. Rarely or never performing this check was uncommon. Participants aged 24-30 were more likely to report never engaging in risky interactions like clicking unknown links (91.9%) compared to 18-23-year-olds (72.3%). Rare and "sometimes" risky behaviors were more common in the younger group. The majority in both groups always verified legitimacy. Not verifying legitimacy was uncommon.

Both genders commonly followed news on related topics, with slightly higher rates among males (79.7%). Females were more likely to have self-taught about cybersecurity (12.3%) compared to males (6.8%). Males were slightly more likely to have taken courses in related topics. Females were more likely to report no data loss due to regular backups (82.5%) than males (73.0%). Males were more likely to report experiencing data loss (13.5%) or not backing up despite avoiding data loss. A small percentage of both groups were unsure about their data loss experiences. Females were more likely to be "somewhat confident" in avoiding phishing (77.2%) compared to males (71.6%). Males were slightly more likely to be "very confident" (14.9%). The majority of both groups reported not falling victim to phishing. However, males were slightly more likely to have fallen victim (4.1%). Both genders predominantly always reviewed sender details. Most participants reported never clicking unknown links or downloading attachments, with slightly higher rates among females (86.0%). Males were slightly more common in rarely clicking unknown links or downloading attachments.

4.7. General security awareness and Practices

Table 4.7 General security awareness and tool usage

Table 4.7 General security awareness and tool usage (continued)		n	%
If you receive a text when your phone is locked, does it show a preview of the message on the screen?	Yes	112	77,2
	No	32	22,1
Are you concerned about the privacy and security of information stored on your mobile phone?	Yes, this worries me, so I secure my device as well as I can	108	74,5
	Yes, this is somewhat worrisome to me	22	15,2
	Yes, but it does not worry me	11	7,6
	No	4	2,8
How would you rate your level of security awareness regarding smartphone practices?	High	59	40,7
	Low	6	4,1
	Moderate	75	51,7
	Very High	2	1,4
	Very Low	2	1,4

Table 4.7 General security awareness and tool usage (continued)

How familiar are you with cybersecurity?	I follow the news of related topics	103	71,0
	I have no knowledge of related topics	17	11,7
	I have read/taught myself about related topics	13	9,0
	I have taken one or more courses in a related topic	9	6,2
	I have a degree in this or a related field	1	0,7
How familiar are you with the security features on your phone?	I change the default settings as issues come to my attention	116	80,0
	I have checked all the settings on my phone to secure it the best I can	19	13,1
	I use the default options	8	5,5
Which applications, if any, do you use to protect your phone and the data on it? (check all that apply)	Virtual Private Network (VPN)	111	76,6
	Virus Scanner	108	74,5
Is your device encrypted? - Mobile Phone	Yes, by default	108	74,5
	Yes, I changed it	14	9,7
	I don't know, I use the default settings	12	8,3
	No	8	5,5

When asked whether a preview of text messages appears on the screen when their phone is locked, the majority of participants (77.2%) reported that message previews are enabled. In contrast, 22.1% indicated that previews are not shown, reflecting a proactive approach to maintaining privacy.

Regarding concerns about the privacy and security of information stored on their mobile phones, 74.5% of participants expressed significant concern and reported taking measures to secure their devices. An additional 15.2% indicated that while this issue was somewhat worrisome, they did not take substantial actions to secure their devices. A smaller proportion (7.6%) acknowledged concern but dismissed it as negligible, while only 2.8% of respondents reported no concern at all.

In terms of self-assessed security awareness levels, most participants (51.7%) rated their awareness as moderate, while 40.7% considered it high. A small number reported very high (1.4%), low (4.1%), or very low (1.4%) levels of security awareness, suggesting some variability in confidence regarding security practices.

Regarding familiarity with cybersecurity, the majority of participants (71.0%) reported following news related to cybersecurity topics, indicating an interest in staying informed. A smaller proportion (9.0%) stated they had independently read or taught themselves about related topics, while 6.2% had taken one or more courses in a cybersecurity-related subject. Only 0.7% of participants held a degree in cybersecurity or a related field, suggesting limited formal education on the topic. Notably, 11.7% of respondents reported having no knowledge of cybersecurity topics.

When asked about familiarity with their phone’s security features, 80.0% of participants reported changing the default settings as issues came to their attention, reflecting a reactive approach to securing their devices. Additionally, 13.1% stated they had proactively checked all settings on their phones to secure them to the best of their ability. A minority (5.5%) indicated they relied on default security options, which may present vulnerabilities.

In terms of applications used to protect their phones and data, Virtual Private Network (VPN) software was utilized by 76.6% of participants, and 74.5% used a virus scanner, indicating a strong adoption of security tools.

Regarding device encryption, 74.5% of participants reported their devices were encrypted by default. A smaller proportion (9.7%) indicated they actively enabled encryption themselves, while 8.3% were unsure of their device's encryption status, relying on default settings. Only 5.5% reported their devices were not encrypted.

The majority in both groups expressed strong concerns about privacy and took measures to secure their devices (72.3% for 18-23 and 77.4% for 24-30). Few reported no concerns. Security was the most common reason for device security practices for both age groups. Convenience was the next most cited reason. Other reasons were infrequently reported.

Both groups most commonly rated their awareness as moderate (55.4% for 18-23 and 46.8% for 24-30), followed by high. Very low awareness was rarely reported. "I follow the news of related topics" was the most common response for learning about cybersecurity. A small proportion in the older group had a degree in cybersecurity, while 15.7% of the younger group had no knowledge. The majority in both age groups reported changing default settings as issues arose. A smaller percentage proactively checked all settings to secure their phones, and very few relied solely on default options. Most participants in both groups did not change these settings.

Females were slightly more likely to express worry and actively secure their devices (80.7%) compared to males (73.0%). Males were slightly more likely to be somewhat worried but not actively securing their devices. Females were significantly more likely to rate their security awareness as high (68.4%) compared to males (23.0%). Males more commonly rated their awareness as moderate (71.6%). Very high, low, and very low awareness ratings were infrequent. Females were more likely to change default settings as issues arose (89.5%) than males (81.1%). Males were slightly more likely to have checked all settings or use default options. A higher proportion of males (17.6%) reported changing default browser settings compared to females (8.8%). Most participants in both groups did not modify their browser settings. Females were more likely to use a VPN (86.0%) compared to males (75.7%). Both genders reported similar usage rates for virus scanners. Females were less likely to be unsure about their device's encryption status (1.8%) compared to males (12.2%). The majority in both groups reported their devices were encrypted by default. Few manually enabled encryption or had unencrypted devices. The majority in both groups reported no security incidents. Females were more likely to be "somewhat confident" in their ability to handle security incidents (87.7%) compared to males (74.3%). Males were more likely to be "very confident" or neutral about their confidence.

CHAPTER 5

DISCUSSION

This chapter synthesizes the findings presented in the preceding chapter, interpreting them in the context of the research questions that guided this study and the broader landscape of smartphone security awareness literature. The aim is to provide a cohesive analysis of what the data reveal about smartphone users' security awareness levels, their practices concerning device and data protection, and the interplay between perceived security and actual behavior, based on a descriptive analysis of the survey data.

Revisiting the Research Questions

The descriptive analysis undertaken in this thesis sought to answer five key research questions. The following discussion will address each question, integrating the descriptive statistical findings to offer comprehensive insights.

RQ1: What is the level of security awareness among smartphone users?

The findings suggest a multifaceted level of security awareness among smartphone users. A significant majority of participants rated their security awareness as "Moderate" (51.7%), with a substantial portion (40.7%) rating it as "High". This self-perception is somewhat supported by their familiarity with cybersecurity, where 71% reported following news on related topics.

However, deeper behavioral indicators reveal a more nuanced picture. For instance, while most users (83.4%) regularly update their operating systems and apps , a practice crucial for security, a considerable number (77.9%) have not changed their default browser settings, which could leave them vulnerable. Confidence in identifying phishing attempts was generally "Somewhat confident" for 71% of users , and a high percentage (91.7%) reported never falling victim to a phishing attack. This indicates a baseline level of awareness regarding common threats. However, the reliance on automatic notifications for OS updates (91.7%) and the tendency to change phone security settings only when issues arise (80%) suggest that awareness might be more reactive than proactive for many. This aligns with existing literature that points to an "awareness-practice gap," where general knowledge does not always translate into consistent, proactive security behaviors.

A descriptive comparison also showed that females rated their security awareness notably higher (68.4% "High") compared to males (23.0% "High"), who more commonly rated their awareness as "Moderate" (71.6%). This suggests that self-perceived awareness can vary by demographic factors.

RQ2: Do owners of smartphones select the proper lock (screen) settings for their devices?

The data indicate a strong inclination towards using lock screen settings, with fingerprint (74.5%) and PIN (4 digits or less: 55.9%; 5 digits or more: 41.4%) being the most prevalent. The overwhelming preference for biometric options (90.3%) over knowledge-based ones underscores a prioritization of convenience, a significant factor in user adoption of security features. Most users (80.7%) cited "Security" as the primary reason for their lock settings, and a majority (66.9%) had their devices lock after 1 minute of inactivity, suggesting an understanding of basic access control.

However, the common use of 4-digit PINs (51.7%) might be a point of concern, as longer, more complex PINs offer greater security. The frequency of updating lock settings also varied, with the most common interval being "About every 6 months" (53.1%). Descriptive comparisons revealed interesting gender differences: females were more likely to use 4-digit PINs (77.2%) and face recognition (82.5%), while males were more inclined towards longer PINs (52.7%). This suggests that "proper" lock settings are not uniformly adopted and are influenced by demographic factors.

RQ3: Do smartphone users (beyond locking their devices) adhere to best practices for data security?

Beyond screen locking, adherence to data security best practices appears inconsistent. A positive sign is the widespread use of protective applications like VPNs (76.6%) and virus scanners (74.5%). Most users (74.5%) also reported their devices were encrypted by default.

However, other behaviors raise concerns. For example, while a majority (68.3%) never entered their Social Security Number (SSN) on their device, a notable 26.2% did so when needed, and 4.8% stored it on their device. The use of public Wi-Fi also presents a mixed picture: 53.1% used additional encryption (e.g., VPN), but 13.1% "always" used public Wi-Fi without explicit mention of extra precautions. This indicates that while some users are taking steps to secure their data in transit, a significant portion may be exposing themselves to vulnerabilities.

RQ4: How aware are users of the importance of routine data backup, and how capable are they of recovering data in case of loss?

Awareness of the importance of data backup seems present, but practices are varied. The most common backup frequency was "Once every 3 months" (45.5%), and a significant portion (52.4%) reported backing up "Sometimes" rather than "Always" (40.7%). While 74.5% reported not experiencing data loss due to regular backups, 11.7% had experienced data loss, indicating that current backup routines are not universally effective.

A descriptive comparison showed that younger users (18-23) were more likely to have experienced data loss (15.7%) compared to the older group (6.5%). Furthermore, there were notable gender differences in backup frequency; females were far more likely to "Always" back up data (71.9%) compared to males (17.6%). This highlights that backup behavior is not uniform and is influenced by demographic variables.

RQ5: Do users prioritize hard security (device access control) over soft security (data privacy and protection)?

The findings suggest a tendency to prioritize hard security measures, such as device locking, over more nuanced soft security practices. As discussed under RQ2, the adoption of screen locks is high. Users also reported their phone "Is always in my possession" (92.4%), indicating a strong focus on physical device security.

In contrast, soft security practices show more variability. While many use VPNs and virus scanners, behaviors like entering SSNs on devices or connecting to public Wi-Fi without guaranteed encryption point to areas where data protection could be enhanced.

The concern for privacy and security was high (74.5% "worries me, so I secure my device as well as I can"), yet this concern doesn't always translate into comprehensive soft security measures. For example, 77.2% had message previews on their lock screen, which could inadvertently expose sensitive information. This suggests users find tangible security measures (like locks) easier to implement than more abstract data protection concepts.

Broader Implications and Connection to Literature

When I look at what my study found and compare it to what other researchers have discovered, a few key things really jump out.

The Knowing-Doing Gap: It's pretty clear from my numbers that there's often a big difference between people knowing about a security risk and actually doing something about it. This is something [9] also talked about. For example, in my study, a lot of people (83.4%) were on top of updating their phone's main system and apps. That’s a good security step. But then, a large number (77.9%) hadn't touched their phone's standard internet browser settings (Table 4.5), which can be a security weak spot. So, even if they're doing one thing right (updates), they're missing another (browser security). This really shows what Adams and Sasse meant when they said people's security knowledge can be a bit all over the place.

Easy Does It - Convenience is King: My findings really hammered home how much people prefer security that's easy to use. For instance, a whopping 90.3% of the people I surveyed preferred using fingerprint or face ID to unlock their phones (Table 4.3). Also, 91.7% just let their phones handle updates automatically (Table 4.5). What’s telling is that even though most (80.7%) said "security" was the main reason they picked their lock settings (Table 4.3), they still went for the simplest, most convenient options. This lines up perfectly with what [23] [20] found – we all say we want security, but if it's a hassle, we're far less likely to bother.

Phishing - Confident but Still Vulnerable: When it came to spotting phishing scams, most of my participants (71%) felt "Somewhat confident" (Table 4.6). And it’s a good sign that 83.4% said they "Always" check who an email or text message is from before responding (Table 4.6). However, despite this, 5.5% of them had actually been tricked by a phishing attack (Table 4.6). This tells me that even when people feel pretty sure and try to be careful, these scams are sophisticated enough to catch some out. This situation is exactly what Bada et al. discussed regarding the cleverness of phishing attacks, and the global statistics from Control D show just how common these attacks are. So, that 5.5% in my study, while it sounds small, represents real people being affected.

Public Wi-Fi Risks - A Bit of a Gamble: Using public Wi-Fi was another area where I saw some interesting behaviors. More than half of the people in my study (53.1%) said they use encryption, like a VPN, when they're on public Wi-Fi, which is a smart move (Table 4.2). But, if you combine the others, you get 41.4% who either always use public Wi-Fi without mentioning any extra safety steps or say they only use it for browsing things they don't consider sensitive (Table 4.2). The problem, as [22] pointed out in their major review of mobile security concerns, is that using public Wi-Fi without solid protection is risky, regardless of what you think you're doing. My numbers show that even among people who are generally familiar with technology, many are still taking these chances, likely because the ease of getting online quickly feels more pressing than less obvious security concerns.

Limitations

It is important to acknowledge the limitations of this study, as outlined in Chapter 3. The reliance on self-reported data may be subject to social desirability or recall bias. The convenience sampling method, while providing a diverse group of participants, primarily from a university setting and specific age groups (18-30), may limit the generalizability of the findings to the broader smartphone user population. The cross-sectional nature of the study provides a snapshot in time and does not capture the evolution of security behaviors or awareness. These limitations suggest that the findings should be interpreted with these contexts in mind.

Recommendations and Future Research Directions

Based on the findings, several recommendations emerge. Firstly, cybersecurity awareness campaigns should continue to emphasize not just the "what" but the "how" and "why" of security practices, aiming to bridge the awareness-practice gap. These campaigns should be tailored to specific demographic groups, considering the observed differences in behavior and perception. For instance, interventions for younger users might focus on the practical importance of consistent backups, while messages for different genders could address their specific patterns of security feature adoption.

Secondly, there is a need to promote a more proactive security posture. Encouraging users to regularly review and update security settings, understand the implications of app permissions, and be cautious with default configurations is crucial. Educational efforts should also aim to balance the understanding of hard and soft security, emphasizing that data protection is an ongoing process beyond just locking the device.

Future research could build upon these findings in several ways. Longitudinal studies could track how security awareness and behaviors change over time, especially in response to new technologies or security incidents. Qualitative research, such as in-depth interviews, could provide richer insights into the reasoning behind users' security decisions and the specific barriers they face. Further investigation into the effectiveness of different educational interventions, perhaps incorporating gamification as suggested by [11], would be valuable. Exploring the security practices of older demographics or users in different socio-economic contexts would also broaden the understanding of smartphone security awareness. Finally, research into designing security features that are both highly secure and intuitively align with user convenience could help mitigate the security-usability trade-off.

CHAPTER 6

CONCLUSION

This thesis set out to gain a clearer understanding of how smartphone users think about and act on security. Our main goal was to figure out how well people protect their phones and the personal information they store on them. What we found contributes to the larger conversation about cybersecurity by highlighting specific behaviors and areas where users are falling short.

Looking back at our findings, a few key things really stand out. On the positive side, it's clear that most users are pretty good at the basics when it comes to phone security. For example, almost everyone uses a lock screen, and many use advanced features like fingerprint or face recognition. It's also encouraging that a good chunk of users regularly updates their devices, which shows they understand how important those updates are for patching up weaknesses.

However, our study also brought to light some significant gaps in people's security habits. Even though basic measures are often in place, many users tend to skip more advanced, yet crucial, practices like regularly backing up data or being super careful about phishing attempts. It was also quite telling that people often prioritize physical security over "soft" security measures, such as truly protecting their online accounts and personal data.

In essence, this research provides a detailed, descriptive look into the security awareness levels and real-world practices of smartphone users. The insights we've gathered can be really helpful for designing cybersecurity awareness campaigns that are more targeted and effective. By digging into user practices, we've pinpointed some key areas where users are most vulnerable. Our findings also underline how inconsistent data backup habits are, with many users just not backing up their information regularly.

Ultimately, this thesis contributes to the broader field by showing how important it is to increase awareness of cybersecurity threats. The data indicating that a large majority of participants have never been victims of phishing attacks suggests a good level of self-protective behavior. However, the small percentage who have fallen victim really points out the ongoing vulnerabilities.

In summary, this study provides a clear and descriptive look at how aware smartphone users are about security. It shows us the strengths in basic device protection but also highlights significant weaknesses in more advanced ways to secure data. When we compare our findings with other studies, it confirms that even when people know about security, there’s often a gap between that knowledge and actually putting it into practice. The interesting differences we found based on age and gender further suggest that cybersecurity education needs to be more personalized. By shedding light on these crucial areas, our research moves the needle forward in the ongoing effort to make smartphone use safer for everyone.

REFERENCES

[1] M. Esmaeili, “Assessment of users’ information security behavior in smartphone networks,” Ph.D. dissertation, Eastern Michigan Univ., Ypsilanti, MI, USA, 2014.

[2] E. E. Müezzin, “A Review on the Psychological Effects of Smartphone Addiction,” Cyprus Turkish Journal of Psychiatry & Psychology, vol. 5, no. 4, pp. 361–367, 2023.

[3] U. e. al, “The Smartphone Theft Epidemic: A Growing Concern,”. https://www.bitdefender.com/box/solutions/the-smartphone-theft-epidemic pp. 50-100, 2012- 2017.

[4] A. Chin, B. Jones, and P. Little, “A Comparative Analysis of Smartphone Security Behaviors and Practices,” International Journal of Education and Development using Information and Communication Technology, vol. 17, no. 3, pp. 57–80, 2021.

[5] M. Alsaleh, N. Alomar, and A. Alarifi, “Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods,” PLoS ONE, vol. 12, no. 3, p. e0173284, 2017.

[6] C. Abreu and P. F. Campos, “Raising Awareness of Smartphone Overuse among University Students: A Persuasive Systems Approach,” Informatics, vol. 9, no. 1, p. 15, 2022.

[7] M. Koyuncu and T. Pusatlı, “Security Awareness Level of Smartphone Users: An Exploratory Case Study,” Mobile Information Systems, vol. 2019, pp. 1–11, 2019.

[8] Ş. Gökçearslan, F. K. Mumcu, T. Haşlaman, and Y. D. Çevik, “Modelling smartphone addiction: The role of smartphone usage, self-regulation, general self-efficacy and cyberloafing in university students,” Computers in Human Behavior, vol. 63, pp. 639–649, Oct. 2016.

[9] B. L. Gross and C. J. Dommeyer, “Consumer Awareness and Behavior Towards Data Security: A Review,” Journal of Information Security, vol. 12, pp. 34–51, 2021.

[10] B. A. Kurdi, M. A. A. Al Anasweh, H. M. Alzoubi, A. A. Al Fouri, D. S. Sakher, and M. T. Alshurideh, “The Impact of Digital Education on Acquiring Cybersecurity Skills among the Students of the Faculty of Medicine at Al-Balqa Applied University,” Migration Letters, vol. 20, no. 5, pp. 370–387, Aug. 2023.

[11] L. A. Thompson, N. Melendez, J. Hempson-Jones, and F. Salvi, “Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning,” in Proc. European Conf. on Games- Based Learning, 2022, pp. 562–569.

[12] J. Quinn and M. L. Quinn, “The Importance of Cybersecurity Education: Addressing the Gaps in Awareness and Practice,” Journal of Cybersecurity Education, Research and Practice, vol. 2020, no. 2,
pp. 40–60, 2020.

[13] R. Torten, C. Reaiche, and S. Boyle, “The Impact of Age on Information Security Awareness and Behavior,” Journal of Information Security & Privacy, vol. 3, no. 4, pp. 123–145, 2018.

[14] V. Singh and K. Sharma, “Smartphone Security: Review of Challenges and Solutions,” International Journal of Computer Applications, vol. 177, no. 34, pp. 1–14, 2020.

[15] L. M. Powell, J. Swartz, and M. Hendon, “Improving Security Awareness: Obstacles and Suggestions,” Issues in Information Systems, vol. 12, no. 1, pp. 67–88, 2011.

[16] O. Ogochukwu and A. Chinedum, “Awareness of Phishing Attacks in Institutions of Higher Learning,” Journal of Cybersecurity Technologies, vol. 4, no. 2, pp. 23–34, 2021.

[17] Lookout, “Mobile Threat Landscape.” https://www.lookout.com/threat-intelligence/report/q1-2024-mobile-landscape-threat-report, Jul. 15, 2025.

[18] H. D. Surdjono et al., “Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene,” International Journal of Information and Education Technology, vol. 15, no. 2, pp. 220–229, 2025.

[19] S. S. U. H. Khan, A. Ghani, and M. A. Al-Sharafi, “A Review on Secure Authentication Mechanisms for Mobile Security,” Sensors, vol. 25, no. 3, Art. no. 700, 2025.

[20] F. Bemmann and S. Mayer, “The Impact of Data Privacy on Users’ Smartphone App Adoption Decisions,” Proc. ACM Hum.–Comput. Interact., vol. 8, no. ICM, Art. no. 113, 2024.

[21] O. Husain, “99 Global Phishing Statistics & Industry Trends (2023–2025),” Control D Blog, https://controld.com/blog/phishing-statistics-industry-trends, Feb. 6, 2025.

[22] N. Mpekoa, “Cybersecurity Concerns on Mobile Phones: A Systematic Review,” in Proc. 20th Int. Conf. Cyber Warfare and Security (ICCWS),

2025, pp. 295–303.

[23] S. Saeed, “Usable Privacy and Security in Mobile Applications: Perception of Mobile End Users in Saudi Arabia,” Big Data and Cognitive Computing, vol. 8, no. 11, Art. no. 162, 2024.

[24] J. D. Mugisha et al., “A Demographic Perspective of Smartphone Security and Its Redesigned Notifications,” Journal of Cybersecurity Education, Research and Practice, 2023, pp. 1–30.

[25] H. P. Bulsara and E. A. Pandya, “Influence of Demographic Factors on Security and Privacy Concerns in Mobile Payments,” Int. J. Innov. Technol. Explor. Eng., vol. 9, no. 2, pp. 5136–5138, 2020.

[26] S. P. K. Sari, P. W. Handayani, and A. N. Hidayanto, “Demographic Comparison of Information Security Behavior Toward Health Information System Protection: Survey Study,” JMIR Formative Research, vol. 7, no. 8, Art. no. e49439, 2023.

[27] M. Yildirim and V. Demirer, “A Scale Development and Application Study on Smartphone Security Awareness,” Gazi Univ. J. Sci., vol. 37, no. 4, pp. 1691–1705, 2024.

APPENDIX

SURVEY QUESTIONNAIRE

1. Where are you from

2.Where do you currently live? (country and city)

3. Which age range do you fall under?

- 18–23
- 24–30
- 31–40
- 41–50
- 51–60

Over 60

- I prefer not to answer

4. I identify as:

- Male
- Female
- Other (please specify)
- I prefer not to answer

5. What is the highest level of education that you have accomplished?

- Some high school
- High school graduate
- Technical training
- Some college
- College graduate
- Some postgraduate
- Postgraduate degree

6. Do you have a smartphone?

- Yes
- No
- I have a phone that is not a smartphone.
- I'm not sure

7. If you answered yes to question 5, which operating system (OS) is your phone running? Otherwise select N/A

- iOS
- Android
- Blackberry
- Windows
- I'm not sure
- Other (please specify)
- N/A

8. My mobile phone:

- Is always in my possession
- Is often left unattended (e.g., is on my desk during lunch break; left at home when I am out)
- Is sometimes left unattended (e.g., occasionally I forget it on my desk; leave it on the bar when going to the restroom)
- Habits:

9. Do you use public available Wi-Fi's/Hotspots (e.g., at Starbucks, McDonalds, Hotels or Airports)?

- Yes, always
- Yes, but only for browsing; no sensitive information is transferred (e.g., I am not using Banking Apps)
- Yes, but I use additional encryption (e.g., a VPN software)
- No, I don't use Public WiFi's

10. Does your device automatically connect to Wi-Fi networks?

- Yes, to any open Wi-Fi
- Yes, to known ones (the ones I accessed in the past)
- No
- I'm not sure

11. On average, how many hours a day is your Bluetooth enabled?

- Less than 2 hours
- Between 2 and 4 hours
- Between 4 and 8 hours
- Between 8 and 12 hours
- 24 hours
- I'm not sure
- Never

12. On average, how many hours a day is your location/GPS enabled?

- Less than 2 hours
- Between 2 and 4 hours
- Between 4 and 8 hours
- Between 8 and 12 hours
- 24 hours
- I'm not sure
- Never

13. If you receive a text when your phone is locked, does it show a preview of the message on the screen?

- Yes
- No
- I'm not sure

14. Have you ever thought about all the information that is stored on your mobile phone?

- Yes, this worries me, so I secure my device as well as I can
- Yes, this is somewhat worrisome to me
- Yes, but it does not worry me
- No

15. Which of the following information do you have stored on your phone? (check all that apply)

- Autofill Saved Credit/Debit Card Information
- Autofill Saved Passwords
- Autofill Banking Information
- Calendar (i.e. Saved Events)
- Personal Photographs
- Cash Exchange Applications (i.e. Cash App, Paypal, Venmo)
- Contacts
- Email
- Health Information (i.e. Documents, Stored Health Data)
- IOT Applications/Autofill IOT Website Data (i.e. Thermostat Controls, Light Controls, House Alarm Controls)
- Maps (i.e. Saved Home Address)
- Social Media Applications (i.e. Facebook, Twitter, Snapchat)
- Voice Assistant (i.e. Siri, Google Now, Cortina)
- Wallet (i.e. Apple pay, Samsung pay, Android Pay)
- None

16. How often do you perform backups on your Mobile phone?

- Once a week
- Once a month
- Once every 3 months
- Twice a year

- Once a year
- Never
- When prompted by my device

17. Do you enter your Social Security Number on your device? - Mobile Phone

- Yes, it is stored on my device
- Yes, I enter it when needed
- No, I’ve never entered it

18. Which lock settings do you have in place on your phone? (check all that apply)

- None, I can use it immediately
- Pin (4 digits or less)
- Pin (5 digits or more)
- Password (has at least one character)
- Pattern (most commonly on Androids)
- Voice
- Fingerprint
- Face
- Lock your Android Phone from Device Manager
- Trusted Places (unlock when certain locations are reached)
- Keep your device unlocked when it is in your hand
- Unlock with trusted devices
- Other (please specify)

19. Would you use a different lock setting if it was available on your phone? (check all that apply)

- None, I can use it immediately
- Pin (4 digits or less)
- Pin (5 digits or more)

- Password (has at least one character)
- Pattern (most commonly on Androids)
- Voice
- Fingerprint
- Face
- Lock your Android Phone from Device Manager
- Trusted Places (unlock when certain locations are reached)
- Keep your device unlocked when it is in your hand
- Unlock with trusted devices
- Other (please specify)

20. How long after inactivity on your device does your device become locked?

- 30 Seconds
- 1 Minute
- 2 Minutes
- 3 Minutes
- 4 Minutes
- 5 Minutes
- More than 5 minutes
- Never

21. If you use a pin (numbers only) to lock/unlock your device, how many different digits does your pin consist of?

- One (e.g., 1111 or 2222)
- Two (e.g., 1122 or 5656)
- Three (e.g., 4432 or 4899)
- Four (e.g., 4567 or 8403)
- More than four
- N/A

22. How often do you update your lock settings? (e.g., Change your pin from 0000 to 1111)

- About every 30 days
- About every 90 days
- About every 6 months
- About every year
- Never
- When given a reason to (i.e., someone knows your passcode)

23. Which reasoning best explains why you chose the lock settings that you have?

- Convenience
- Forgetfulness
- Security
- Default Phone Settings
- No opinion

24. Do you favor biometric lock options (e.g., fingerprint) over knowledge-based options (e.g., password)?

- Yes
- No

25. How would you rate your level of security awareness regarding smartphone practices?

- Very Low
- Low
- Moderate
- High
- Very High

26. How familiar are you with cybersecurity (on a scale of 1–5)?

- I have no knowledge of related topics
- I follow the news of related topics
- I have read/taught myself about related topics
- I have taken one or more courses in a related topic
- I have a degree in this or a related field
- Security Devices:

27. How familiar are you with the security features on your phone?

- I have checked all the settings on my phone to secure it the best I can
- I change the default settings as issues come to my attention
- I use the default options

28. Did you change your default browser settings?

- Yes
- No
- I use the default options

29. Which applications, if any, do you use to protect your phone and the data on it? (check all that apply)

- Applications to Securely Delete Files (i.e., CCleaner)
- Password Handling Applications (i.e., LastPass)
- Secure Messaging Applications (i.e., Signal)
- Virtual Private Network (VPN)
- Virus Scanner
- I’m not sure
- None

30. Is your device encrypted? - Mobile Phone

- Yes, I changed it
- Yes, by default
- No

- I don’t know, I use the default settings

31. Do you use anything else to protect your phone? Please explain

32. Have you ever lost important data on your smartphone (e.g., contacts, photos, documents) due to a malfunction or other issues?

- Yes
- No
- I'm not sure

33. Do you regularly back up the data on your smartphone (e.g., using cloud services, an external hard drive, or local backups)?

- Always
- Sometimes
- Never
- I don't know how to back up my data

34. How often do you take out insurance of smartphone's data?

- Always
- Sometimes
- Never

35. Have you ever experienced a security breach or data loss on your smartphone (e.g., unauthorized access, data theft, malware, etc.)?

- Yes
- No
- I'm not sure

36. How often do you perform data wiping upon disposal of smartphone's data?

- Always
- Sometimes
- Never

37. Which method do you primarily use to back up the data on your smartphone?

- iCloud (for iOS users)
- Google Drive (for Android users)
- External hard drive
- Online cloud storage service (e.g., Dropbox)

38. Have you ever lost important data on your smartphone due to not having a backup?

- Yes, I have experienced data loss.
- No, I have not experienced data loss as I regularly back up my data.
- No, I have not experienced data loss even though I do not back up my data.
- Not sure/I don't remember.

39. Do you regularly update your smartphone's operating system and apps to protect against security vulnerabilities?

- Yes, regularly
- Occasionally
- No
- I'm not sure how to do this

40. What are the primary reasons for updating your smartphone's OS? (Select all that apply)

- Security patches and bug fixes
- New features and enhancements
- Improved performance and stability
- To stay protected against cyber threats

- Others (please specify)

41. How do you typically receive notifications about available OS updates for your smartphone?

- Automatic notifications from the device
- Notifications from the smartphone manufacturer
- Notifications from the mobile carrier
- Through news articles or online forums
- Other (please specify)

42. When prompted to install an OS update on your smartphone, how likely are you to install it immediately?

- Very likely
- Somewhat likely
- Neutral
- Somewhat unlikely
- Very unlikely

43. Have you ever delayed or skipped installing OS updates on your smartphone? If yes, what were the reasons? (Select all that apply)

- Concerns about compatibility issues with existing apps
- Lack of time to install updates
- Unawareness of the importance of updates
- Preference for the current OS version
- Fear of potential disruptions to device functionality
- Other (please specify)

44. How often do you update the applications installed on your smartphone to the latest versions available?

- Daily
- Weekly

- Monthly
- Occasionally
- Rarely
- Never

45. What factors influence your decision to update applications on your smartphone? (Select all that apply)

- Security updates and vulnerability fixes
- New features and functionalities
- Performance improvements
- Notifications from app developers
- Peer recommendations
- Others (please specify)

46. Have you ever experienced security incidents or breaches on your smartphone due to delayed or neglected updates?

- Yes
- No

47. How confident are you in your ability to differentiate between legitimate update notifications and phishing attempts disguised as update alerts on your smartphone?

- Very confident
- Somewhat confident
- Neutral
- Somewhat uncertain
- Not confident

48. Do you believe that regularly updating your smartphone's OS and applications is essential for maintaining its security integrity?

- Strongly agree

- Agree
- Neutral
- Disagree
- Strongly disagree

49. On a scale of 1 to 5, where 1 represents "Not at all confident" and 5 represents "Extremely confident," how confident are you in your ability to identify potential phishing attempts on your smartphone?

- Very confident
- Somewhat confident
- Neutral
- Somewhat uncertain
- Not confident

50. How often do you receive unsolicited emails or text messages asking for personal information (e.g., passwords, credit card details) on your smartphone?

- Rarely
- Occasionally
- Frequently
- Almost daily

51. Have you ever fallen victim to a phishing attack on your smartphone?

- Yes
- No

52. How often do you review the sender's email address or phone number before responding to an email or text message on your smartphone?

- Always
- Sometimes
- Rarely

- Never

53. How often do you click on links or download attachments from unknown or suspicious sources on your smartphone?

- Never
- Rarely
- Sometimes
- Often
- Always

54. When logging into sensitive accounts (e.g., banking, email), do you verify the legitimacy of the website or app before entering your login credentials on your smartphone?

- Always
- Sometimes
- Rarely
- Never

55. Please write any comments and/or suggestions that you may have: