I Was Told to Install the Antivirus App, but I'm Not Sure I Need It: Understanding Smartphone Antivirus Software Adoption and User Perceptions

Seyoung Jin
Sungkyunkwan University
Suwon, Republic of Korea
22sysy@skku.edu

Heewon Baek
Sungkyunkwan University
Suwon, Republic of Korea
heewb9818@skku.edu

Uichin Lee
School of Computing
KAIST
Daejeon, Republic of Korea
uclee@kaist.edu

Hyoungshick Kim
Sungkyunkwan University
Suwon, Republic of Korea
hyoung@skku.edu

Abstract

The rising threat of mobile malware has prompted security vendors to recommend antivirus software for smartphones, yet user misconceptions, regulatory requirements, and improper use undermine its effectiveness. Our mixed-method study, consisting of in-depth interviews with 23 participants and a survey of 250 participants, examines smartphone antivirus software adoption in South Korea, where mandatory installation for banking and other financial apps is common. Many users confuse antivirus software with general security tools and remain unaware of its limited scope. Adoption is significantly influenced by *perceived vulnerability*, *response efficacy*, *self-efficacy*, *social norms*, and *awareness*, while concerns about system performance and skepticism about necessity lead to discontinuation or non-use. Mandatory installations for financial apps in South Korea contribute to user misconceptions, negative perceptions, and a false sense of security. These findings highlight the need for targeted user education, clearer communication about mobile-specific threats, and efforts to promote informed and effective engagement with antivirus software.

CCS Concepts

• **Human-centered computing → User studies**; • **Security and privacy → Usability in security and privacy**.

Keywords

Smartphone Security, Antivirus, Malware

ACM Reference Format:
Seyoung Jin, Heewon Baek, Uichin Lee, and Hyoungshick Kim. 2025. I Was Told to Install the Antivirus App, but I'm Not Sure I Need It: Understanding Smartphone Antivirus Software Adoption and User Perceptions. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3706598.3713452

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713452

1 Introduction

The rapid proliferation of smartphones has fundamentally transformed the mobile security landscape, presenting unprecedented challenges due to malware attacks. Despite security vendors' recommendations, mobile antivirus adoption rates remain critically low across various countries. In South Korea, only 31% of smartphone users utilized protective software as of 2020 [37], while in the U.S., the adoption rate was even lower at 17% [52]. These low rates are especially concerning given the escalating threat landscape. Kaspersky's Q1 2024 report, for instance, documented the prevention of 10.1 million malware attacks by antivirus software software [32].

While these growing threats are widely recognized, there remains a critical gap in understanding how users perceive and experience antivirus software during real-world use. Existing studies have largely neglected users' real-world experiences interacting with antivirus software and have predominantly focused on PC environments [12, 13, 38]. As Thompson *et al.* [57] emphasized, the factors influencing security behavior differ significantly across platforms, yet little attention has been paid to how users engage with these tools in practice.

Our research highlights a critical gap between the growing mobile security threats and users' understanding and adoption of antivirus software. This issue is particularly concerning for Android users, as the possibility of installing apps from unofficial sources greatly increases the risks of malware.

To mitigate malware threats, many Korean financial institutions mandate the installation of security apps with antivirus functionality on Android devices. These apps, serving as auxiliary tools for primary applications (e.g., banking, credit card, or shopping apps), differ from traditional antivirus software in execution, protection, and scope, creating a complex landscape for users. In this context, our study emphasizes the need to reinterpret smartphone antivirus adoption in Korea, considering the country's mandatory regulations. This approach is similar to the technology non-use research methodology, which is considered valuable from an HCI perspective [6, 66]. Non-use research broadens the definition of technology users to include those who do not use technology, referred to as non-users, and uncovers biases or limitations in design and accessibility [51].

Ultimately, it is akin to studying technology use itself but with a focus on technology non-adoption and abandonment. We advocate for an in-depth analysis of antivirus (non-)adoption and abandonment, exploring user perceptions, misconceptions, and behaviors while also highlighting Korea's security software regulations and their implications. Understanding the various forms of technology non-use, different types of non-users, and their sociocultural contexts provides deeper insights into complex socio-technical systems.

Our research questions are as follows:

- **RQ1:** What are smartphone users' perceptions and usage patterns regarding antivirus software?
- **RQ2:** What are the reasons for smartphone users' adoption, discontinuation, or non-use of antivirus software?
- **RQ3:** How do users' usage patterns and reasons differ between smartphones and PCs?

To address these questions, we conducted a two-phase study combining qualitative and quantitative methods. First, we conducted an in-depth user study to investigate users' perceptions and usage patterns of antivirus software on smartphones. This qualitative phase revealed several key insights. Many users misunderstand the purpose and functionality of antivirus software, often conflating it with general security features or performance optimization tools. Moreover, this lack of clarity leads to the adoption of auxiliary antivirus software with limited security effectiveness. Participants adopt antivirus software to prevent malware or meet requirements. Non-use is due to low perceived risk, reliance on built-in features, doubts, and lack of confidence. Our study shows that indifference, lack of knowledge, and external influences from others also impact adoption, extending beyond the traditional PMT model.

Building on these qualitative insights, we refined the Protection Motivation Theory (PMT) [49, 50] by incorporating *social norms* and *awareness*, identified in our study, as additional components, and conducted a large-scale online survey with 250 participants to systematically assess the key drivers of antivirus adoption on smartphones. The survey was designed to explore the factors influencing users' decisions to adopt antivirus software on smartphones, as well as how users' antivirus software usage patterns and reasons differ between smartphones and PCs.

Our findings reveal that the key factors driving antivirus software adoption on smartphones extend beyond traditional PMT components (*response efficacy*, *perceived vulnerability*, *self-efficacy*), with *social norms* and *awareness* emerging as additional critical factors. While *response efficacy*, *response cost*, and *self-efficacy* are significant in PC environments, *perceived severity* plays a lesser role in smartphone users' decisions, suggesting platform-specific differences in security behavior. In South Korea, where banks mandate antivirus software installation for Android banking apps, 66% of PC users and 54% of smartphone users have antivirus software installed. PC users tend to use antivirus software consistently, whereas smartphone users often encounter it passively, as it is automatically activated alongside main apps like banking or financial services.

This study advances the theoretical understanding of security software adoption by extending PMT to better reflect the mobile security context. Through our mixed-methods approach, we demonstrate how mandatory installation requirements and platform-specific characteristics influence user behavior and decision-making in mobile security. These insights contribute to both theoretical frameworks for understanding security software adoption and practical knowledge about user behavior in environments where security software installation is required.

2 Background and Related Work

2.1 Mobile Malware and Antivirus

Mobile malware refers to intrusive programs that breach handheld devices, such as phones, tablets, and fitness trackers. Its goal is to disrupt normal device operations, steal private information, or gain unauthorized access [62]. The Android operating system is a particularly attractive target for malware developers due to its dominant global market share and open ecosystem [18]. Unlike closed platforms like iOS, Android allows users to install apps from third-party sources, increasing the risk of downloading malicious apps. A significant portion of Android users are still exposed to malware, particularly when installing apps from unofficial sources [58].

The importance of establishing and rapidly implementing defenses against mobile-based threats has grown. The need for antivirus software for smartphones has long been evident [64]. Antivirus software is a security program to prevent, detect, search for, and remove various types of malware from computers, networks, and other devices [56]. This helps protect the potential vulnerabilities of the user's device, limits the spread of malware, and provides comprehensive protection within the mobile security ecosystem.

2.2 Security Regulations in South Korea

The mandatory installation of security software in South Korea originates from the government's early efforts to enhance electronic financial security [16] — the Korean banks mandated various security features, including firewalls, anti-keylogging software, and anomaly detection software, to protect financial transactions [33]. Today, banking applications in South Korea automatically bundle mandatory security software for Android users, including antivirus applications (*e.g.,* V3 Mobile Plus [28] and V-Guard for Web [41]). This Android-specific requirement exists because Android users can install applications from sources outside the official Google Play Store, increasing potential malware risks. This security concern is particularly significant in South Korea, where Android smartphones account for 75.85% of the mobile operating system market share in 2024 [17]. Consequently, most Korean financial institutions mandate antivirus software for Android devices, while such requirements are not applied to iOS devices, where apps can only be installed through the official App Store.

Such security requirements for financial transactions are not unique to South Korea, as similar mandates exist in other countries. For example, India's Reserve Bank mandates Guardsquare security software for mobile banking users [26], while Brazilian banks require the Warsaw security module for secure transactions on Windows and macOS [23]. Beyond banking, several countries have implemented broader security software mandates, often raising significant concerns about security and privacy [14, 30, 43]. South Korea's approach, including its required security applications for

Windows PC access to financial and government services [1], exemplifies how different nations adapt their cybersecurity requirements to address specific market conditions and security challenges.

2.3 Antivirus Software Adoption

Most studies on antivirus software adoption have focused on PCs, using quantitative analysis with PMT to examine user intentions. These studies span various domains, including antivirus [10, 12, 48, 59], anti-spyware [22, 27], organizational security compliance [8, 31, 39], and general security behavior [20, 29, 38, 57, 63, 66]. However, the findings are often inconsistent. For instance, Gurung *et al.* [27] highlighted the importance of *response efficacy*, *self-efficacy*, and *perceived severity*, while Woon *et al.* [63] emphasized *perceived severity*, *response efficacy*, *response cost*, and *self-efficacy*. As shown later, we found that neither of these sets of factors was significant in our study. This discrepancy may stem from the differences between PC and mobile environments, where free antivirus software is more common, and users may rely more heavily on built-in security features on smartphones.

Smartphone antivirus adoption has received limited attention in academia. While Al-Ghaith [3] demonstrated the relevance of *subjective norms* in smartphone antivirus adoption by extending the traditional PMT model, our study expands this understanding by incorporating both *subjective* and *descriptive norms* under the broader concept of *social norms*, and by identifying awareness as an additional significant factor. Our mixed-methods approach, combining qualitative interviews with quantitative survey data, offers insights into the factors influencing smartphone antivirus adoption patterns. This integrated approach provides a deeper understanding of how users make decisions regarding mobile security.

2.4 Adoption of Security Protection Measures

Understanding how users adopt and engage with security protections is crucial for developing effective security technologies. Research has consistently revealed a gap between security awareness and implementation. Multiple studies [7, 11, 66] have documented that while users understand security's importance, they often fail to implement protective measures effectively. Vaniea *et al.* [60] found that negative experiences with previous updates significantly decreased users' willingness to install future security updates. Their research highlighted how users struggle to distinguish security updates from general software updates, which corresponds to our findings about users confusing security features with performance optimization tools. Anderson *et al.* [4] investigated the phenomenon of security warning desensitization, finding that frequent exposure to warnings can diminish user attention and affect the adoption of protective measures. This aligns with findings from Sunshine *et al.* [55], who identified warning fatigue as a critical challenge in security adoption.

While these studies provide valuable insights into security adoption behaviors, our research reveals additional factors affecting antivirus software adoption in mobile settings. Unlike traditional security measures where individual user experiences drive adoption decisions, our study results demonstrate that regulatory requirements and social influence significantly shape adoption patterns. This suggests the need to examine security adoption through both individual behavioral factors and broader institutional influences.

3 User Study Methods

To answer **RQ1** and **RQ2**, we conducted interviews with 23 participants to explore the adoption and usage of antivirus software.

3.1 Interview Structure

The interview consisted of two sections: the first section about smartphone antivirus software usage and the second section for demographics and security knowledge assessment.

The first section explored participants' awareness and experience with antivirus software. We first asked participants to describe their understanding of antivirus software's purpose. We then discussed their usage patterns, including specific applications, key features used, and usage frequency. Finally, we examined their reasons for adopting, discontinuing, or not using antivirus software.

The second section collected demographic information and included a security knowledge quiz adapted from a previous study [44] to assess participants' understanding of mobile malware threats. The complete interview questionnaire is available in Appendix A.

During our pilot study with six participants, we found that some were unfamiliar with the term "antivirus software." We addressed this by including "vaccine software," a more recognizable term in our target population. Before continuing the interview, we referenced two well-known South Korean antivirus products (listed in Appendix A) for participants unfamiliar with both terms.

The study protocol was approved by the university's Institutional Review Board (IRB).

3.2 Recruitment

We recruited 24 participants, by posting announcements on our university's website and Danggeun Market (https://www.daangn.com/), a popular online flea market platform in South Korea. The eligibility criteria were: (1) being over 18 years old, (2) proficiency in Korean, and (3) experience with Android smartphones. We specifically targeted individuals without a security background to better understand how people with limited security knowledge interact with antivirus software and respond to malware. Furthermore, our participant selection process was guided by the 2023 Korean smartphone user demographics [36], aiming for a diverse representation of gender and age. Each participant was compensated 50,000 KRW, which is approximately USD 38, for the two-hour study.

One participant was excluded after recruitment due to insufficient Android experience, resulting in a final sample of 23 participants. The age range of participants (24-68 years) was evenly distributed, with a slight overrepresentation in the 39–48 and 49–58 age groups, reflecting the demographic proportions of smartphone users in Korea. Gender distribution was nearly equal, with 11 males and 12 females across all age subgroups. Among the participants, one (P5) worked as an iOS app developer, and another (P17) had a background in computer science. Table 1 provides detailed demographic information and interview results for all participants.

Table 1: Demographics and Antivirus Usage of Interview Participants. ID: Unique identifier (bold indicates actual adoption); Age: Age range; Gender; Education: MS (Middle school or less), HS (High school or equivalent), AD (Associate's Degree), BD (Bachelor's degree), GD (Graduate degree); Smartphone Model: OS type; CS Background: Computer Science experience; # of Answers: Correct responses out of 3 security assessment questions; Usage Experience: Antivirus usage history; Type: Antivirus category; Scan Frequency: Malware scan usage.

ID	Age	Gender	Education	Smartphone Model	CS Background	# of Answers	Usage Experience	Type	Scan Frequency
P1	39-48	Female	BD	Android Only	No	3	Adopted	Both of two types	Event-driven
P2	59+	Female	BD	Android Only	No	1	Adopted	Plugin	-
P3	29-38	Female	BD	Android to iOS	No	3	Never used	-	-
P4	49-58	Male	HS	Android to iOS	No	2	Discontinued	Both of two types	Event-driven
P5	29-38	Male	BD	Android to iOS	iOS App Developer	2	Discontinued	Plugin	-
P6	49-58	Female	BD	Android to iOS	No	3	Discontinued	Plugin	-
P7	49-58	Male	BD	Android Only	No	3	Adopted	Plugin	-
P8	39-48	Female	GD	Android Only	No	3	Adopted	Plugin	-
P9	39-48	Male	GD	Android to iOS	No	2	Discontinued	Plugin	-
P10	49-58	Female	BD	Android Only	No	0	Adopted	Plugin	-
P11	29-38	Male	BD	Android Only	No	3	Discontinued	Standalone	Always
P12	59+	Male	MS	Android Only	No	1	Adopted	Plugin	-
P13	59+	Female	HS	Android Only	No	1	Adopted*	Standalone	Never
P14	59+	Male	BD	Android Only	No	2	Adopted	Plugin	-
P15	19-28	Female	AD	Android to iOS	No	2	Discontinued	Plugin	-
P16	19-28	Female	HS	Android to iOS	No	1	Never used	-	-
P17	19-28	Male	BD	Android Only	CS Major	2	Adopted	Both of two types	1-2 times a year
P18	39-48	Female	GD	Android Only	No	1	Never used	-	-
P19	49-58	Male	AD	Android to iOS	No	1	Discontinued	Both of two types	Event-driven
P20	49-58	Female	BD	Android Only	No	1	Adopted	Plugin	-
P21	19-28	Male	BD	Android to iOS	No	1	Discontinued	Standalone	Rarely
P22	39-48	Male	AD	Android Only	No	2	Adopted	Plugin	-
P23	29-38	Female	AD	Android to iOS	No	1	Never used	-	-

Note: Bold text in **ID** refers to users classified as actual adoption based on their usage experience, type of antivirus software, and usage pattern.
*In the case of P13, it is simply in an installed state because the initial permission settings were not completed.

3.3 Data Analysis

We analyzed the interview responses through iterative qualitative coding. The primary coder developed an initial codebook based on their analysis. A second researcher then independently coded all responses while providing feedback on the codebook structure. Through collaborative discussions, we refined the codebook to improve theme categorization. After several rounds of independent coding and codebook refinement, our final coding using the agreed-upon codebook achieved an inter-coder agreement of 95.87% (Cohen's kappa) [25]. We resolved all remaining discrepancies through discussion and allowed multiple codes per response when necessary to capture complex responses fully.

4 User Study Results

4.1 Perceptions and Usage Patterns of Smartphone Antivirus Software

4.1.1 Knowledge Gaps in Smartphone Antivirus Software. To assess participants' mental models of antivirus software, we asked about their familiarity with the terms "Antivirus software" or "Vaccine software" in the context of smartphones. Our findings revealed that 17 out of 23 participants were familiar with one or both terms, while 6 were not. Interestingly, when presented with the names of well-known antivirus products in South Korea, all participants reported having heard of at least one of these products.

Overall, a substantial proportion of the participants (13 out of 23) demonstrated a clear understanding of antivirus software, mentioning malware, such as personal data theft apps and smartphone camera hacking apps, and the proactive role that antivirus software plays in preventing malware. For example, P4 stated, "*I understand that antivirus apps are created to filter out malicious apps or things like that to prevent hacking of my phone.*"

However, the rest of the participants (10 out of 23) showed varying levels of understanding. Three participants (P10, P12, and P21) had a limited understanding. P10 and P12 described the software's purpose as simply protecting the smartphone, while P21 stated, "*I think it might block things like bad transmissions or malicious codes.*" In particular, P10 expressed disinterest, saying, "*I've never learned about it, and I'm not curious.*" Participants (P8, P19, and P23) confused general security features with specific antivirus functions. Their limited mental models associated antivirus software with preventing personal information leaks during web browsing (P19), filtering suspicious calls (P23), and blocking harmful website pop-ups (P8). Participants (P1, P19, and P22) linked smartphone optimization or performance improvement features to the primary purpose of antivirus software, reflecting a misunderstanding of its intended role. P1 stated, "*Well, it seems like it catches things like malicious codes, optimizes the battery, and also gets rid of duplicate files and the trash, making it a bit more optimized for using the phone.*" Similarly, P22 remarked, "*For example, when playing a game, I think lag is caused by a virus... It solves the problem of smartphones slowing down due to viruses.*" Notably, two participants (P13 and P16) were unable to explain the purpose of antivirus software on smartphones at all.

4.1.2 Smartphone Antivirus Software Usage Patterns and Their Influence on Security Perceptions. We investigated the adoption and usage patterns and their influence on security perceptions of antivirus software. To do so, we first briefly explained its purpose and features to participants and then asked them to describe their experiences, including the specific software they used, and when and how often they used the primary features.

Our analysis revealed two distinct categories of antivirus software: STANDALONE and PLUGIN. STANDALONE software operates independently as a standalone app, providing comprehensive, continuous protection through features such as security checks and real-time scanning. In contrast, PLUGIN software is activated alongside other main applications (*e.g.,* banking, credit card, or shopping apps) to ensure a secure environment by detecting malicious apps while these services are in use. Unlike STANDALONE, PLUGIN software serves as auxiliary tools for main applications, as mandated by South Korean financial institutions to install security software. Both types provide antivirus functions on smartphones, but they differ in execution requirements, protection duration, and targets.

As shown in Table 1, 19 out of 23 participants had experience with antivirus software, either by using it or discontinuing its use. Among them, 7 had used either STANDALONE software or a combination of both types, while 12 had used PLUGIN software only (7 of whom used the same software—AhnLab's V3 Mobile Plus). Notably, two participants (P5 and P6) who had ceased using antivirus software could not recall the specific names of their previously used programs. However, they said that the software had been a mandatory requirement for using banking applications. Given this context, these two participants were classified within the PLUGIN software group.

We identified distinct usage patterns that varied depending on the type of antivirus software used. For STANDALONE type software, most participants (6 out of 7) primarily used malware scanning features, though their scanning habits and motivations varied significantly. Among them, three participants (P1, P4, and P19) scanned irregularly, typically prompted by specific events such as installing new applications, receiving scan reminders, or hearing news about emerging mobile malware. They also frequently used cleanup features for device optimization or to prevent overheating. Two other participants (P17 and P21) scanned infrequently, generally only twice a year or less, as they had never encountered malware on their smartphones and believed that nothing would appear even if they did scan. Only one participant (P11) used the real-time detection and premium security features requiring a paid subscription, stating, "*Ransomware was a big issue for a while, and I was also worried about personal information leakage. Since they were offering a discount on the paid subscription, I decided to try it for about a year to see how different it would be. I always kept the real-time detection on, and I usually did a manual scan before going to bed.*"

Notably, P13 never used the antivirus software on her device due to unfamiliarity with its operation—although it was installed, the initial permissions necessary for its functionality were not properly configured. P13 explained, "*I don't use my phone much. I only use it for basic things like calls and texts. I know I should use it, but I don't have much knowledge about them or smartphones in general. Instead, I just avoid responding to strange texts and stick to the basics.*"

For PLUGIN type software, the most common pattern among users was a lack of active engagement. Nearly all participants (9 out of 12) encountered the antivirus software only when it automatically activated alongside their banking or financial apps. As P8 expressed, "*When I open a financial or investment app, I think the antivirus app runs automatically in the background, but I'm not really sure. To be honest, I just use the main app without thinking much about the antivirus thing.*"

Three other participants (P6, P12, and P22) reported rarely or never using the antivirus software, having either forgotten about it (P6), not knowing how to use it (P12), or even being unaware of its installation prior to the interview (P22). P9 reported only using the optimization features to improve smartphone battery efficiency.

Our participants were often unaware of the limited protection (because it only runs in the background while the main application is active) and associated risks provided by PLUGIN antivirus software. When we informed the 12 participants who had only used this type of antivirus software that it did not offer continuous protection, half of them were unaware of this limitation and risk. P9 remarked, "*I didn't know there was no real-time detection, but even if I had known, I wouldn't have used it. Real-time protection can sometimes be a distraction.*"

When considering only voluntary antivirus software adoption, the proper usage of STANDALONE antivirus software is low. Of the 23 total participants, 7 participants had experience with STANDALONE antivirus software (including both standalone and both types). Among them, 2 participants (P1 and P17) are currently using both types, 1 participant (P13) installed the standalone type but never actually used it, and 4 participants (P4, P11, P19, P21) have discontinued use (P4 and P19 used both types, while P11 and P21 used standalone).

Takeaway 1: Our analysis of smartphone antivirus software perceptions and usage patterns revealed distinct insights across 23 participants. While 13 users demonstrated accurate comprehension of core features like malware prevention, 10 showed limited understanding, either confusing it with general security features or performance optimization capabilities. Usage patterns differed significantly between STANDALONE and PLUGIN types: STANDALONE users mainly performed irregular malware scans with only one participant utilizing premium features, while PLUGIN users typically encountered the software only during automatic activation with banking apps, with half unaware of its limited protection scope. These findings indicate opportunities for improving both user education and security solution design, particularly given the low rate of proper voluntary usage of STANDALONE software and limited awareness of PLUGIN software's constraints.

4.2 Reasons for Adoption, Discontinuation, and Non-Use

We examined participants' reasons for adopting, discontinuing, or not using antivirus software. As shown in Table 1, participants were categorized into three groups: current users (11), those who discontinued use (8), and those who never used such software (4). To understand the various factors influencing participants' security decisions, we analyzed responses across these groups. For example, adoption reasons came from both current users and those who had discontinued use, providing insights into initial motivations regardless of current usage. Similarly, the reasons for non-use were gathered from three groups: participants who have never used antivirus software, those who discontinued its use with no intention of resuming, and current plugin users who expressed no interest in adopting standalone software. The detailed codebook is provided in Appendix B.

4.2.1 Adoption. Our findings were based on 19 participants who either used or discontinued antivirus software about their reasons for adopting it. Among the 7 participants who adopted standalone antivirus software, 6 participants voluntarily installed the software primarily to prevent malware. They demonstrated a clear understanding of malware threats on Android OS smartphones, citing smartphone security vulnerabilities, ransomware, and the risks associated with installing game APK files downloaded from unofficial Android markets. They favored products that allowed quick scans with a single click, finding them convenient to use, and selected antivirus software based on its popularity in online communities or its development by companies where their acquaintances worked.

Additionally, three participants (P1, P4, and P21) mentioned that having antivirus software gave them a sense of comfort. They habitually installed it when purchasing electronic devices or continued to use it even though they did not fully understand security. Interestingly, P13 reported that her family members installed the antivirus software without her consent, as she was reluctant to use it due to her unfamiliarity with smartphones.

The adoption of plugin antivirus software showed a different trend. Of the 12 participants in this category, 7 participants installed it reluctantly to use other security-sensitive apps such as those for finance, shopping, or securities. Three participants criticized the mandatory installation practice. P6's comment encapsulates this sentiment: *"I was told to install the (antivirus) app if I wanted to use banking apps, so I just installed it, but I don't know if I'm not sure I need it. Even if I don't want to, I have no choice but to install it."* Only P7 viewed it positively, stating, *"I'm worried about economic loss if there's hacking when doing internet banking or stock trading... It may not provide perfect protection, but I think it's better than nothing."*

Some participants were uncertain about their reasons for installation. Two (P2 and P20) could not recall how the software was installed but kept it due to its security-related appearance. P2 said, "*I'm not exactly sure, but I don't think I installed it myself. I just assumed that as long as there was some kind of security app, my phone would be safe.*" However, three others (P6, P9, and P12) intentionally installed the software for general smartphone security, citing concerns about credential leakage on shopping websites and malware infection. P9 said, "*I installed it myself after reading the news, thinking that 'maybe I needed something like that..?', so I tried it.*"

4.2.2 Discontinuation. Our findings were based on the 8 participants who discontinued antivirus software for various reasons. Among the 4 participants who discontinued standalone antivirus software, three participants (P11, P19, and P21) believed that their cautious smartphone usage habits reduced their risk of malware infections. They avoided potentially harmful activities, such as visiting malicious websites (*e.g.,* pornographic websites or unofficial game APK sites), primarily stuck on well-known safe sites (*e.g.,* YouTube and Google). Additionally, they reported spending minimal time browsing the web. P11, who was the only one to use the paid subscription, mentioned, "*After using it, I didn't see any difference between using it and not using it... even though I paid. Free apps don't make a big difference either. In fact, the real-time detection just slowed down my phone, and since I don't use the internet much, I had fewer chances of being exposed to viruses. So, I stopped using it after that.*"

The perceived security strength of certain devices also influenced the decision to discontinue antivirus use, regardless of the type (standalone or plugin). Three participants (P4, P9, and P19) cited their iPhone's perceived strong security as a reason for stopping antivirus use. For example, P4 said, "*After switching [from an Android phone] to an iPhone, I thought phishing wouldn't happen because the App Store is closed, so I didn't feel the need for a security app.*" The belief that iOS is inherently more secure than Android is widespread; however, this is a misconception, as incidents like the Pegasus spyware attack [15] and iOS's susceptibility to zero-day vulnerabilities [46] demonstrate that no system is entirely immune to threats.

Among the 4 participants who discontinued plugin antivirus software, two participants (P5 and P15) mentioned that they were not asked to install it. P15 said, "*When I switched to an iPhone and used services like banking, I was not asked to install something like this (antivirus apps). I'm not knowledgeable about this stuff, so I just used my phone whether it had it installed or not.*"

Two participants (P6 and P9) believed their smartphone contained minimal sensitive information. For example, P9 said, "*If I had something worth protecting, I'd probably pay for security. Usually, stuff on computers, like company info, is important, but I don't have anything like that on my phone. I do have some digital certificates, but since nothing bad has happened so far, I haven't really felt the need to be extra careful.*"

Additionally, P5 expressed a deeper concern, voicing distrust in the antivirus software itself, mentioning, "*. . . I'm not sure if antivirus apps are trustworthy, and there are many examples of them being misused, so I even think those things themselves are risky. My parents use Android phones, and I tend to delete apps that check things and clean up junk and stuff like that for them.*" They feared that malicious actors could potentially disguise malware as antivirus software or exploit vulnerabilities in legitimate antivirus programs to launch attacks, adding another layer of complexity to users' decision-making process regarding antivirus adoption.

4.2.3 Non-use. We identified three distinct groups of participants who chose not to use antivirus software: those who never used it, those who discontinued with no intention to resume, and current plugin users who showed no interest in adopting standalone software. Their reasons ranged from deliberate risk management strategies to a lack of awareness. Two participants who never used antivirus software (P3 and P18) acknowledged the seriousness of personal data breaches but chose to manage risks through personal strategies. They deliberately limit sensitive information on their smartphones, such as avoiding stored login credentials (P18) or having minimal need for banking and shopping apps as a stay-at-home individual (P3). P18 explained, "*I always think there's a chance I could lose my phone anytime, so I try not to keep anything important on it.*" The lack of prior security incidents (reported by P3 and P16) reinforced their belief in these strategies. In contrast, P23 simply lacked awareness of mobile antivirus solutions, stating, "*I knew about it for PCs, but not for phones.*"

Among those who discontinued use or used only PLUGIN software, participants expressed more skeptical views. Two participants (P5, former PLUGIN user, and P20, current PLUGIN user) believed careful smartphone usage eliminated the need for additional protection. Three others (P10, P15, and P22) considered personal information leaks harmless, deferring responsibility to external organizations. As P22 explained, "*What I mean is a worst case if there is a data breach, you'll receive spam texts from unknown numbers. Even if a telecommunications company leaks customer information, customers do not make a big fuss or worry, and the company does not even provide compensation. Moreover, even if hackers try to create a fake bank account using my personal information, it is useless because financial authorities monitor everything.*" P15 shared a similar disinterest in security measures, stating, "*Honestly, I'm not really interested in security, so I don't think my phone's security is strong. If someone wanted to, they could break into my phone. But who would want to hack me? I don't know where or how my data is being used, so I'm not sure how serious it is, and I have never felt the need to take action. If someone suggested I try to use it, I might have tried it, but no one around me uses it.*"

Beyond risk perceptions, participants questioned antivirus software's necessity and effectiveness. Two participants (P10 and P18) considered PLUGIN software sufficient, believing built-in security measures adequately protected financial services. Three participants (P14, P5, and P20) expressed deeper skepticism, citing concerns about deceptive practices, potential exploitation by malicious actors, and usability challenges. P20 exemplified this perspective, saying, "*To be honest, even if I have an antivirus, I don't know how to use it... but if I avoid clicking on links or opening suspicious items, I think I'll be fine.*"

Takeaway 2: Among our 23 participants, 11 currently use antivirus software, 8 have discontinued its use (2 stating no intention to resume), and 4 have never used it. Participants using PLUGIN antivirus reported installing it primarily because it was mandated and bundled with banking apps. In contrast, participants using STANDALONE antivirus described security concerns as their primary reason for adoption. Those who discontinued or never used antivirus software mentioned several reasons: they perceived smartphones as having low-security risks, trusted built-in security features, or questioned antivirus software's effectiveness based on past experiences. Social influences also played a role in these decisions: some participants selected software based on online community recommendations and acquaintances' experiences, while others noted how the lack of antivirus use in their social circle contributed to their non-adoption.

5 Survey Study Methods

We conducted a large-scale online survey with 250 participants to validate the insights from the interview study and investigate key factors influencing antivirus software adoption across a broader population (**RQ2**). The survey also compared how users' antivirus software usage patterns and their reasons differ between smartphones and PCs (**RQ3**).

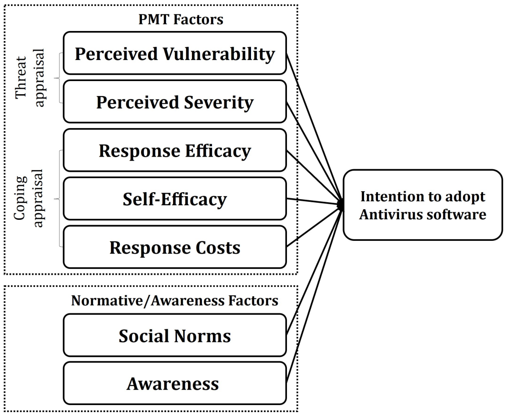

Figure 1: Research Model for Antivirus Software Adoption.

We grounded our survey on the theoretical framework of Protection Motivation Theory (PMT) [49, 50] to systematically analyze the factors influencing antivirus software adoption. Over the years, PMT has been widely applied across various fields, including information security[5, 57, 61]. Our interview findings, however, revealed several factors beyond traditional PMT components. We observed that participants' adoption decisions were significantly influenced by their social circle's security practices and recommendations. Additionally, many participants showed varying levels of awareness about antivirus software, with some expressing complete disinterest or limited understanding of its purpose. To address these motivations, we incorporated *social norms* and *awareness* as additional components, drawing from existing literature. This theoretically informed approach allows us to explain the underlying mechanisms driving antivirus software adoption on smartphones, providing a more generalizable understanding of adoption behaviors.

5.1 Research Model for Antivirus Adoption

Model Factors. Figure 1 illustrates our expanded PMT model, refined to include the factors identified in our interviews and applied in the online survey. PMT explains how individuals engage in protective behaviors through two cognitive processes: threat appraisal and coping appraisal. Threat appraisal refers to an individual's evaluation of a threat's seriousness and likelihood of encountering it, corresponding to *perceived severity* and *perceived vulnerability*, respectively. Coping appraisals include an individual's expectation of the effectiveness of the recommended action (*response efficacy*), confidence in one's ability to perform it successfully (*self-efficacy*), and any associated costs, such as time, effort, and financial costs (*response costs*). Protection motivation mediates these processes by arousing, sustaining, and directing protective behavior, typically measured by behavioral intentions [9]. Perceived severity, perceived vulnerability, response efficacy, and self-efficacy positively influence behavioral intentions, such as adopting antivirus software on smartphones, whereas response costs have a negative effect.

Beyond traditional PMT factors, our interview findings revealed that social influences play a significant role in antivirus software adoption. While PMT focuses on individual threat and coping appraisals, participants were significantly influenced by various social factors: some based their software selection on popularity in online communities and recommendations from acquaintances, others had family members directly intervene in their security decisions, and several noted how the absence of antivirus use in their social circle affected their choices. To capture these social dynamics, we expanded our model to include *social norms*, combining both *subjective norms* and *descriptive norms* based on our pilot study's factor analysis. *Subjective norms* reflect perceived expectations from significant others to use antivirus software [2], while *descriptive norms* represent the perception that most people use such software [47]. Previous research has shown that these social factors significantly influence security behavior intentions [3, 57].

In addition, to examine how users' limited understanding of antivirus software impacts their intention, we incorporate *awareness*, which refers to users' consciousness and concern regarding technological issues and strategies to address them [21, 22]. It means that users who are more informed about security threats and protective measures are more likely to develop a positive attitude toward using protective technology.

Survey Items Development. We developed survey items and ensured their validity and reliability through several steps. We comprehensively reviewed studies on user security behavior intention based on PMT and selected validated items indicating potential subjective agreement among researchers that these measures accurately reflect the constructs of interest. The survey items were slightly reworded to fit the context of antivirus software adoption when necessary. We then conducted two pilot studies to refine the survey instrument. The initial pilot with 13 participants led to several improvements: simplifying malware descriptions, adding illustrations for clarity, and converting open-ended product names to multiple-choice options. A second pilot with 22 participants validated these modifications. Based on the observed average completion time of 15 minutes, we established a 5-minute minimum threshold for the main survey to ensure response quality. A larger study involving 250 participants was subsequently conducted, followed by a factor analysis, as mentioned earlier. Details of the items for each construct, along with their sources, are provided in Appendix C.

5.2 Survey Organization

Our main survey was organized into three sections as follows: The first section focused on identifying key factors influencing smartphone users' intentions to use antivirus software, utilizing our research model. Before this section, we assessed participants' awareness of antivirus software through two simple questions and provided brief explanations of malware and antivirus software to ensure clarity throughout the survey. The second section explored participants' experiences with antivirus software on both smartphones and PCs. Questions covered usage frequency, specific products used, and reasons for installing, uninstalling, or not using the software (with open-ended responses), mirroring the approach used in our interview study. The final section gathered comprehensive demographic data, including gender, age, education level, experience in computer science/IT, current occupation, and projected total household income for the year. The online survey questionnaire details are provided in Appendix D.

5.3 Data Analysis Methods

We employed a multiple linear regression using ordinary least squares estimation [19] to identify factors influencing antivirus software adoption on smartphones. Our analysis process began with a reliability assessment using Cronbach's α to measure the internal consistency of each construct. Following established practices [34, 42], we set a threshold of 0.7, above which the items were considered reliably measuring the same construct. To avoid multicollinearity, we examined the variance inflation for each independent variable and removed independent variables with high values (above 10). Standardized coefficients (β) in our regression model were reported in the table. These coefficients allow us to compare the relative impact of different factors on antivirus software adoption. Factors with p-values < 0.05 were considered statistically significant.

We used a qualitative coding method similar to our interview study to analyze open-ended responses. The interview responses were independently coded by two researchers, who engaged in iterative discussions to refine the codebook. During this process, codes were added, removed, modified, or merged as necessary. Following the resolution of coding disagreements, the inter-coder agreement reached 94.98%, as measured by Cohen's kappa [25], demonstrigh level of coding consistency. All remaining minor discrepancies were then resolved through discussion.

5.4 Recruitment

We recruited participants through a research company using their established panel for online surveys, ensuring the sample was statistically representative of Korean smartphone users aged 19 to 74. The largest age group was 35–44 (33.6%), followed by 45–54 (28.0%), with 66.0% identifying as female. Chi-square tests showed no significant differences in gender ($\chi^2(1) = 2.34$, $p = 0.126$) and age distributions ($\chi^2(5) = 9.78$, $p = 0.082$) compared to the general Korean smartphone user population, confirming the sample's representativeness.

Eligible participants were Korean-speaking adults (aged 18 and older) using both Windows PCs and Android smartphones, reflecting the dominant market share and malware prevalence for these platforms in South Korea. We specifically targeted individual users with full control over their personal devices, excluding those subject to workplace security policies. This approach allowed us to focus on personal choices regarding antivirus software usage, free from corporate influences or pre-installed solutions, thus capturing typical consumer behavior.

In two simple quizzes assessing awareness of malware and antivirus software, 90% of participants indicated familiarity with malware, while 81% were aware of antivirus software. These results suggest that the majority had a basic knowledge of malware and antivirus software, with only 10% unaware of malware and 4% unfamiliar with antivirus software.

We implemented rigorous quality control measures, including pre-survey screening, attention checks, and the exclusion of rapid responses (completed in less than 5 minutes). Our target sample size of 250 participants exceeded the minimum of 153 calculated using G*Power software [24] (medium effect size: 0.15, power: 0.95, number of constructs: 7), aligning with previous studies [54, 59]. From 389 initial respondents, we retained 250 valid responses after applying our quality criteria. Participants received approximately 2 USD compensation for their time. Detailed demographics of our survey participants are provided in Appendix E.

6 Survey Study Results

6.1 Factors Impacting the Intention to Adopt Antivirus Software on Smartphones

Reliability and Validity Checks. To assess the fit of the survey questionnaire, we conducted reliability and multicollinearity tests on the measured construct variables. As shown in Table 2, the Cronbach's α values for all constructs, ranging from 0.804 to 0.934, exceed the recommended threshold of 0.7, indicating that the internal consistency of these measurements is satisfactory. As shown in Table 3, the VIF scores for all constructs were below 10, with the highest being 1.520, and the correlation values across all pairs of constructs were below the recommended threshold of 0.8, indicating no problematic multicollinearity between the considered constructs.

Table 2: Construct Reliability.

Constructs	Cronbach' α	Mean	SD
Perceived Vulnerability	0.848	2.988	0.73
Perceived Severity	0.874	4.148	0.88
Response Efficacy	0.836	3.985	0.55
Self-Efficacy	0.856	3.688	0.71
Response Costs	0.804	3.095	0.66
Social Norms	0.934	3.459	0.82
Awareness	0.811	3.390	0.66
Intention to adopt	0.869	3.712	0.79

Table 3: Correlations and Variance Inflation Factors (VIF) for Constructs. Constructs: PV (Perceived Vulnerability), PS (Perceived Severity), RE (Response Efficacy), SE (Self-Efficacy), RC (Response Costs), SN (Social Norms), AW (Awareness), IA (Intention to adopt antivirus software).

Constructs	PV	PS	RE	SE	RC	SN	AW	IA	VIF
PV	1								1.209
PS	0.220***	1							1.160
RE	0.137*	0.237***	1						1.417
SE	0.063	0.076	0.308***	1					1.198
RC	0.200**	-0.041	-0.196**	-0.263***	1				1.239
SN	0.178**	0.035	0.455***	0.289***	-0.26***	1			1.520
AW	0.297***	0.244***	0.308***	0.203**	0.034	0.372***	1		1.345
IA	0.284***	0.136*	0.491***	0.349***	-0.228***	0.645***	0.391***	1	-

Correlation is significant at the 0.05 level (2-tailed)*, at the 0.01 level (2-tailed)**, at the 0.001 level (2-tailed)***.

Regression analysis results. The results of our regression model, which identifies key factors influencing users' intentions to adopt antivirus software on their smartphones, are presented in Table 4. The model showed a good fit, with an R^2 value of 0.519 and an adjusted R^2 value of 0.505, indicating that approximately 50% of the variance in the dependent variable is explained by the model, demonstrating substantial explanatory power [45]. However, a significant portion of the variance remains unexplained, likely due to external factors such as the mandatory installation of antivirus software for services like banking and government platforms–mentioned in 43 (18%) open-ended responses–yet not captured by traditional PMT constructs.

Table 4: Multiple Regression Results.

Construct	Standardized (β)	P>|t|
Perceived Vulnerability	0.1586	0.001
Perceived Severity	0.0056	0.907
Response Efficacy	0.1850	0.001
Self-Efficacy	0.1117	0.023
Response Costs	-0.0823	0.099
Social Norms	0.4413	0.000
Awareness	0.1017	0.050
R^2	0.519	
Adjusted R^2	0.505	

Our regression model results showed that *social norms*, *response efficacy*, *perceived vulnerability*, *self-efficacy*, and *awareness* were found to significantly influence individuals' intention to adopt antivirus software on their smartphones. *Social norms* ($\beta = 0.4413$; $p < 0.000$) was revealed to be the most influential factor, suggesting that individuals who believe that important others or peers want them to use antivirus software and who perceive that most people are using antivirus software are more likely to intend to use the tool. *Response efficacy* ($\beta = 0.1850$; $p < 0.001$) emerged as the second most powerful factor, indicating that individuals who believe antivirus software effectively protects their smartphones from malware or security threats are more likely to adopt it. *Perceived vulnerability* ($\beta = 0.1586$; $p < 0.001$) was also significant, suggesting that individuals who believe they are likely to face malware threats on their smartphones are inclined to adopt antivirus software. *Self-efficacy* ($\beta = 0.1117$; $p = 0.023$) and *awareness* ($\beta = 0.1017$; $p = 0.05$) also positively influenced the intention to adopt antivirus software. These findings highlight the importance of individuals' confidence in their ability to use antivirus software effectively and the role of users' concern and awareness about security threats and protective measures.

In contrast, *perceived severity* and *response costs* were not significantly related to their intention to adopt antivirus software. This indicates that although users recognize the seriousness of potential threats, this awareness does not necessarily encourage them to adopt antivirus software. Additionally, the perceived costs associated with adopting antivirus software were not a significant barrier to their decision.

> **Takeaway 3:** *Social norms*, *response efficacy*, *perceived vulnerability*, *self-efficacy*, and *awareness* are significant factors influencing users' intentions to adopt antivirus software on smartphones. Therefore, these factors should be considered when effectively promoting the adoption of antivirus software.

6.2 Antivirus Software Adoption: Smartphones vs. PCs

6.2.1 Adoption and Usage Patterns. Our analysis reveals distinct patterns in how individuals engage with antivirus software across devices. 54% of participants reported using antivirus software on their smartphones, compared to 66% on their PCs ($X^2 = 11.9286$, $p < 0.005$), as shown in Table 5. The smartphone adoption rate notably exceeds the global average of 17% [52], likely due to South Korea's mandatory antivirus requirements for mobile banking and government services. While PCs have no such requirements, they show higher adoption rates, suggesting different security perceptions across platforms. Antivirus non-use is twice as common on smartphones compared to PCs, highlighting a greater reluctance to use antivirus software on mobile devices, even though it is required.

Table 5: Adoption of Antivirus Software.

Usage Status	Smartphones	PCs
Adoption	134 (54%)	166 (66%)
Discontinued	65 (26%)	58 (23%)
Non-use	51 (20%)	26 (10%)
Total	250 (100%)	250 (100%)

Table 6 reveals distinct patterns in antivirus scanning behavior across devices. Users tended to conduct on-demand scans on their smartphones (28%, 55/199), while opting for continuous real-time protection on their PCs (25%, 56/224). For both devices, users primarily initiated on-demand scans when they noticed performance slowdown (smartphones: 21/55; PCs: 17/38). This pattern suggests a more proactive security approach in PC usage, contrasting with the reactive, performance-driven scanning behavior in smartphone usage.

Table 6: Frequency of Using Malware Scanning Feature.

Frequency	Smartphones	PCs
Always	28 (14%)	56 (25%)
More than once a day	19 (10%)	16 (7%)
1-2 times a week	41 (21%)	48 (21%)
1-2 times a month	42 (21%)	50 (22%)
1-2 times a year	2 (1%)	3 (1%)
Only when needed	55 (28%)	38 (17%)
Rarely used	12 (6%)	13 (6%)
Total	199 (100%)	224 (100%)

Regarding scan triggers, smartphones were scanned more frequently than PCs during financial/payment activities (11 on smartphones vs. 3 on PCs) and when a threat was perceived (11 vs. 2), such as opening suspicious links, installing new apps, or experiencing malfunctions. Spam messages were a unique trigger for smartphone scans (3 on smartphones). Triggers reported across both platforms included occasional scans (10 on smartphones vs. 5 on PCs) and scans prompted by notifications or widespread public awareness of malware (6 vs. 9).

Among the 199 participants who currently adopt (134) or previously adopted (65) antivirus software on their phones, V3 Mobile Plus was the most popular (58%), followed by AlyacM (48%) and V3 Mobile Security (33%). Adoption patterns showed 43% using both STANDALONE and PLUGIN, 35% using only STANDALONE, and 18% using only PLUGIN. 4% were unsure of their software. For PC antivirus software, out of 224 current or former adopters, AhnLab V3 365 Clinic was most common (43%), followed by AhnLab V3 Endpoint Security 9.0 (37%) and Microsoft Defender Antivirus (17%).

6.2.2 Reasons. In open-ended responses, we asked participants to explain their reasons for using, discontinuing, or avoiding antivirus software on both their PCs and smartphones. To provide more informative results, we do not report reasons coded as unclear (*i.e.*, not understandable or irrelevant), and we partially include responses that do not explain the two reasons for starting and then discontinuing use in the discontinuation group. Table 7 provides the top five reasons for adoption, discontinuation, and non-use.

Table 7: Top Five Reasons for Adoption, Discontinuation, and Non-use of Antivirus Software on Smartphones and PCs.

Smartphones	Count (%)	PCs	Count (%)
Top coded reasons for adoption: smartphones (n=243) vs. PCs (n=244)			
Personal information leak	47 (19%)	Malware prevention/detection	59 (24%)
A requirement for other services	43 (18%)	Personal information leak	37 (15%)
Malware prevention/detection	30 (12%)	Pre/Auto-installed	27 (11%)
Smartphone optimization	20 (8%)	Personal data protection	21 (9%)
Pre/Auto-installed	18 (7%)	Direct damage experience	18 (7%)
Top coded reasons for discontinuation: smartphones (n=72) vs. PCs (n=53)			
System overhead	26 (35%)	Financial costs	10 (19%)
Not-needed/Not vulnerable	13 (17%)	Inconvenience to use	9 (17%)
Do not reinstall on new device	9 (12%)	Sufficient-built-in-tool	8 (15%)
Inconvenience to use	8 (11%)	System overhead	6 (11%)
Doubt effectiveness/Distrust antivirus	6 (8%)	Do not reinstall on new device	6 (11%)
Top coded reasons for non-use: smartphones (n=68) vs. PCs (n=25)			
Lack of knowledge to install/use	16 (24%)	Limited device proficiency/Infrequent use	6 (22%)
Not-needed	12 (18%)	Lack of knowledge to install/use	5 (19%)
Inconvenient to use	11 (16%)	Not-needed	4 (15%)
System overhead	10 (15%)	Not vulnerable/experience	3 (11%)
Not vulnerable/experience	6 (9%)	Inconvenient to use	2 (7%)

Regarding reasons for adoption, personal information leakage was the most common concern related to malware (19% for smartphones, 24% for PCs). However, personal data protection against malware-related data loss was more frequently mentioned for PCs (1% for smartphones, 9% for PCs). Additionally, concerns about protecting work data (3%) or the PC itself (3%) were raised exclusively in the PC context.

Malware prevention and detection were the primary reasons for adopting antivirus software in both environments. Factors related to malware vulnerability awareness, such as financial transactions (4%) and spam SMS/voice phishing attacks (4%), were mentioned only in the smartphone environment.

The results also showed that non-security-related reasons, such as involuntary adoption as part of other services (18%) and optimization goals (8%), were more prominent on smartphones, aligning with the interview findings. In contrast, risk perception through direct malware-related damage (7%) was three times higher on PCs than on smartphones.

As shown in Table 5, antivirus adoption was higher on PCs (66%) compared to smartphones (54%). This difference in adoption rates reflects the varying perceptions of vulnerability and the different usage patterns between the two platforms.

For discontinuation, the main reasons are system overhead (35%) (*e.g.*, insufficient storage, slow device, app crashes) in the smartphone environment and financial costs (19%) in the PC environment. While system overhead was a common issue in both environments, the significantly higher level of dissatisfaction with system overhead on smartphones (26 participants) compared to PCs (6 participants)—about four times greater—suggests that users are more sensitive to performance issues on smartphones than on PCs, given that participants use both types of devices.

Furthermore, participants were more likely to switch to built-in security tools (*e.g.,* Windows Defender) on their PCs to avoid perceived issues such as cost burden, while on their smartphones, they were more likely to abandon antivirus software altogether.

In terms of reasons for non-use, in the smartphone environment, participants frequently encountered difficulties with installation and operation (24%), particularly in selecting the appropriate product. This represents a fundamental barrier during the initial stages of adoption that may have been previously overlooked.

In contrast, in the PC environment, participants often reject adopting antivirus software due to a lack of proficiency or infrequent use of their PCs (22%). Some participants indicated that they do not use antivirus software because it is a personal PC (7%), which is a unique response in the PC environment. Other reasons cited include a lack of perceived need, inconvenience of use, and concerns about system overhead.

Takeaway 4: Participants reported distinct usage patterns and adoption barriers between PCs and smartphones. While PC antivirus adoption was higher (66%) than smartphones (54%). On smartphones, system overhead was the primary concern for discontinuation (35% of responses), which was four times higher than on PCs (11%). Financial costs were the main barrier for PCs (19% of discontinuation responses). Installation and usage challenges also varied: on smartphones, 24% of non-users reported difficulties with installation and product selection. In contrast, on PCs, 22% of non-users attributed their non-adoption to infrequent device use and low proficiency. These differences in adoption barriers reflect how users perceive and interact with security software differently across devices.

7 Discussion

7.1 Antivirus Software Usage Under Mandatory Requirements

Recent HCI research has highlighted the value of studying technology non-use alongside traditional usage patterns [51, 53]. This perspective helps understand biases in technology design and accessibility [66] while revealing how different types of users interact with technology in complex socio-technical systems [6]. Our study examines how mandatory installation requirements influence antivirus software adoption through this non-use lens.

The mandatory antivirus software requirements for Android banking apps in South Korea have created a complex security landscape. While this policy has achieved higher adoption rates compared to global figures, our findings reveal significant implementation challenges. Users often demonstrate a limited understanding of antivirus software capabilities, particularly regarding PLUGIN software bundled with financial apps. Many confuse these auxiliary security tools with general security features, leading to negative perceptions and, paradoxically, a false sense of security.

Based on these findings, we offer the following recommendations for improving mobile antivirus adoption and usage. Financial institutions should develop more effective approaches to enhance user understanding of antivirus software protection. They should clearly convey the distinct roles and limitations of bundled security tools when users install financial apps, helping users better understand the scope of protection provided. Security software developers should prioritize demonstrating effectiveness against mobile-specific threats while addressing system overhead concerns that emerged as a primary barrier to continued use. For researchers, critical areas for investigation include bridging the gap between adoption and active engagement, examining methods to improve user awareness of antivirus software's protection scope and requirements, and leveraging social influences identified in our model. These targeted approaches could help transform passive installation into meaningful security practices.

7.2 Comparative Analysis of Our Findings

The user motivations identified in our interviews aligned closely with those observed in the survey. Both studies revealed two primary patterns for antivirus software adoption: voluntary adoption for malware prevention and mandatory installation for using other apps. Both studies also consistently identified key barriers to adoption, including low threat awareness (*e.g.,* belief in one's safe usage habits, belief in being invulnerable) and concerns about system overhead. While interview participants often emphasized the low perceived seriousness of personal data breaches, survey respondents primarily cited limited knowledge of antivirus software as their main reason for non-use. Despite this difference in emphasis, the fundamental reasons for non-use remained consistent across both studies.

Our qualitative findings revealed several key factors influencing non-use: perceptions of low smartphone security risks, trust in built-in security features, doubts about antivirus software effectiveness, and low confidence in using the software. The survey study statistically validated these factors through our theoretical model constructs: *response efficacy*, *perceived vulnerability*, *self-efficacy*, and *awareness*.

Notably, the survey's qualitative findings highlight system overhead is the primary reason for discontinuing antivirus software on smartphones. Smartphone users tend to engage with antivirus software only when necessary and often believe that it slows down their devices. However, the related factor of *response costs* was not found to be statistically significant in the model for smartphone antivirus software adoption. This discrepancy suggests that while performance issues may not significantly affect initial adoption, they are a key factor in discontinuation. To mitigate this, security software developers should optimize performance to minimize system overhead, and service providers requiring or recommending antivirus software should ensure it meets efficiency standards to prevent user disengagement due to slowdowns.

7.3 Factors Influencing Antivirus Software Adoption on Smartphones

Our study suggests differences in antivirus software adoption patterns between PCs and smartphones. While previous research identified *perceived severity*, *response efficacy*, and *self-efficacy* as factors for PC users [27, 40], our findings indicate that smartphone adoption appears to be influenced by additional factors including *social norms*, *response efficacy*, *perceived vulnerability*, *self-efficacy*, and *awareness*. Notably, *social norms*, such as peer recommendations and social pressures, emerged as a factor that may be particularly relevant to smartphone users.

Our findings suggest that external factors may often outweigh individual risk assessments, with mandatory installations for banking apps being commonly cited as an adoption driver. We also observed that users' security perceptions tend to vary between platforms, with participants often expressing trust in built-in smartphone security features while showing different concerns about malware-induced data loss on PCs. This difference in platform-specific risk perception may help explain why *perceived severity*, highlighted in PC-focused studies [10, 27, 40, 57], might be less prominent in smartphone antivirus adoption.

These observations point to potential differences in how users approach security across platforms. Future research could explore these platform-specific variations in security behavior and their implications for security solution design.

7.4 Limitations

Our study has several limitations. First, the regulatory environment in South Korea, which mandates antivirus software installation for specific services [35], may limit the generalizability of our findings to regions with differing regulatory frameworks. Second, our regression analysis yielded an adjusted R^2 of 0.505, suggesting that a significant portion of the variance in antivirus software adoption remains unexplained. To address this, existing theoretical models should be expanded to account for diverse geographical, regulatory, and cultural factors.

8 Conclusion

Our study on smartphone antivirus adoption offers key insights into mobile security behaviors. We identified that users' adoption and usage patterns are influenced by both individual security decisions and external requirements. In South Korea's mandatory installation context, we found distinct categories of usage: while some users actively chose antivirus software for security protection, many installed it primarily due to service requirements.

We found significant knowledge gaps in users' understanding of antivirus protection, with many mistaking it for general security tools or performance optimization software. Our theoretical analysis revealed that *perceived vulnerability*, *response efficacy*, *self-efficacy*, *social norms*, and *awareness* are the primary factors influencing adoption, differing from traditional PC-focused studies.

Future work should examine the effectiveness of these strategies across different regulatory environments and cultural contexts, considering how varying mandatory installation policies affect user perceptions and behaviors.

Acknowledgments

We sincerely thank the reviewers for their valuable feedback. Hyoungshick Kim is the corresponding author. This work was supported by the Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2024-00439762, 2022-0-00688, 2022-0-01199, and 2022-0-00495).

References

[1] Government 24. 2017. Customer Service Center's Announcement for Downloading the Security Program (Windows). https://www.gov.kr/portal/ntcItm/39696 [Online; accessed 10.02.2025].

[2] Icek Ajzen. 1991. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes* (1991).

[3] Waleed Al-Ghaith. 2016. Extending Protection Motivation Pheory to Understand Security Determinants of Anti-Virus Software Usage on Mobile Devices. *International Journal of Computers* (2016).

[4] Bonnie Brinton Anderson, Anthony Vance, C Brock Kirwan, Jeffrey L Jenkins, and David Eargle. 2016. From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It. *Journal of Management Information Systems* (2016).

[5] Salvatore Aurigemma and Thomas Mattson. 2018. Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions. *Computers & Security* (2018).

[6] Eric PS Baumer, Morgan G Ames, Jed R Brubaker, Jenna Burrell, and Paul Dourish. 2014. Refusing, Limiting, Departing: Why We Should Study Technology Non-use. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.

[7] Ron Bitton, Kobi Boymgold, Rami Puzis, and Asaf Shabtai. 2020. Evaluating the Information Security Awareness of Smartphone Users. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.

[8] John M Blythe and Lynne Coventry. 2018. Costly But Effective: Comparing the Factors That Influence Employee Anti-Malware Behaviours. *Computers in Human Behavior* (2018).

[9] Hendrik Boer and Erwin R Seydel. 1996. Protection Motivation Theory. In *Predicting Health Behaviour: Research and Practice with Social Cognition Models*.

[10] Scott R Boss, Dennis F Galletta, Paul Benjamin Lowry, Gregory D Moody, and Peter Polak. 2015. What Do Systems Users Have To Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly* (2015).

[11] Frank Breitinger, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2020. A Survey on Smartphone User's Security Choices, Awareness and Education. *Computers & Security* (2020).

[12] Tim Chenoweth, Robert Minch, and Tom Gattiker. 2009. Application of Protection Motivation Theory to Adoption of Protective Technologies. In *Hawaii International Conference on System Sciences*.

[13] Chet L Claar and Jeffrey Johnson. 2012. Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems* (2012).

[14] CNBC. 2019. Russia's Controversial 'Sovereign Internet' Law Goes into Force. https://www.cnbc.com/2019/11/01/russiacontroversial-sovereign-internet-lawgoes-into-force.html [Online; accessed 9.12.2024].

[15] CNBC. 2021. Apple iPhones Can Be Hacked with Spyware Even If You Don't Click on a Link, Amnesty International Says. https://www.cnbc.com/2021/07/19/apple-iphones-can-be-hacked-even-if-the-user-never-clicks-a-link-amnesty-international-says.html [Online; accessed 8.12.2024].

[16] Financial Services Commission. 2007. Regulation on Supervision of Electronic Financial Transactions Taking Effect. https://www.fsc.go.kr/eng/pr010101/21742 [Online; accessed 7.12.2024].

[17] Stat Counter. 2024. Mobile Operating System Market Share South Korea. https://gs.statcounter.com/os-market-share/mobile/south-korea [Online; accessed 9.12.2024].

[18] Stat Counter. 2024. Mobile Operating System Market Share Worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide [Online; accessed 9.12.2024].

[19] BD Craven and Sardar MN Islam. 2011. Ordinary Least-Squares Regression. *The SAGE Dictionary of Quantitative Management Research* (2011).

[20] Robert Crossler and France Bélanger. 2014. An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *DATABASE for Advances in Information Systems* (2014).

[21] Tamara Dinev and Paul Hart. 2005. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce* (2005).

[22] Tamara Dinev and Qing Hu. 2007. The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies. *Journal of the Association for Information Systems* (2007).

[23] Banco do Brasil. 2024. Banco do Brasil. https://seg.bb.com.br/home.html [Online; accessed 7.12.2024].

[24] Franz Faul, Edgar Erdfelder, Axel Buchner, and Albert-Georg Lang. 2009. Statistical Power Analyses Using G* Power 3.1: Tests For Correlation and Regression Analyses. *Behavior Research Methods* (2009).

[25] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. 2013. *Statistical Methods for Rates and Proportions*. John Wiley & Sons.

[26] Guardsquare. 2024. Mobile Finance App Security Compliance in India. https://www.guardsquare.com/india-financial-app-security-compliance [Online; accessed 7.12.2024].

[27] Anil Gurung, Xin Luo, and Qinyu Liao. 2009. Consumer Motivations in Taking Action Against Spyware: An Empirical Investigation. *Information Management & Computer Security* (2009).

[28] AhnLab Inc. 2024. V3 Mobile Plus. https://play.google.com/store/search?q=V3%20Mobile%20Plus&c=apps&hl=en [Online; accessed 5.12.2024].

[29] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[30] ITPro. 2019. Kazakh Government Will Intercept the Nation's HTTPS Traffic. https://www.itpro.com/network-internet/34051/kazakh-government-will-interceptthe-nation-s-https-traffic [Online; accessed 9.12.2024].

[31] Allen C Johnston and Merrill Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* (2010).

[32] Kaspersky. 2024. IT Threat Evolution in Q1 2024. Mobile Statistics. https://securelist.com/it-threat-evolution-q1-2024-mobile-statistics/112750/ [Online; accessed 14.11.2024].

[33] Hyoungshick Kim, Jun Ho Huh, and Ross Anderson. 2010. On the Security of Internet Banking in South Korea. *Oxford University Computing Laboratory* (2010).

[34] Paul Kline. 2013. *Handbook of Psychological Testing*. Routledge.

[35] ABK Korea. 2024. Online Banking in Korea. https://www.abk-korea.com/en/publications/online-banking-in-korea [Online; accessed 14.11.2024].

[36] Gallup Korea. 2023. 2012-2023 Survey on Smartphone Usage, Brands, Smartwatches, and Wireless Earbuds. https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1405 [Online; accessed 14.11.2024].

[37] TechM Korea. 2020. "Usage Rate Only 30%?" In the Era of Nationwide Hacking, Citizens Shun 'Mobile Antivirus Apps'. https://www.techm.kr/news/articleView.html?idxno=72785 [Online; accessed 31.01.2025].

[38] Doohwang Lee, Robert Larose, and Nora Rifon. 2008. Keeping Our Network Safe: A Model of Online Protection Behavior. *Behaviour & Information Technology* (2008).

[39] Younghwa Lee and Kai R Larsen. 2009. Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. *European Journal of Information Systems* (2009).

[40] Huigang Liang and Yajiong Lucky Xue. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems* (2010).

[41] Infraware Ltd. 2024. V-Guard for Web. https://play.google.com/store/apps/details?id=kr.co.shiftworks.vguardweb&hl=en [Online; accessed 5.12.2024].

[42] Ioana Andreea Marin, Pavlo Burda, Nicola Zannone, and Luca Allodi. 2023. The Influence of Human Factors on the Intention to Report Phishing Emails. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.

[43] BBC News. 2009. China Defends 'Green Dam' Software. http://news.bbc.co.uk/2/hi/asia-pacific/8091044.stm [Online; accessed 9.12.2024].

[44] Sanghak Oh, Kiho Lee, Seonhye Park, Doowon Kim, and Hyoungshick Kim. 2024. Poisoned ChatGPT Finds Work for Idle Hands: Exploring Developers' Coding Practices with Insecure Suggestions from Poisoned AI Models. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.

[45] Peterson K Ozili. 2023. The Acceptable R-Square in Empirical Modelling for Social Science Research. In *Social Research Methodology and Publishing Results*.

[46] PCMag. 2021. Apple Patches New Zero-Day iOS Vulnerability Possibly Under Exploitation. https://www.pcmag.com/news/apple-patches-new-zero-day-ios-vulnerability-possibly-under-exploitation [Online; accessed 8.12.2024].

[47] Amanda Rivis and Paschal Sheeran. 2003. Descriptive Norms as an Additional Predictor in the Theory of Planned Behaviour: A Meta-Analysis. *Current Psychology* (2003).

[48] Gerrianne Roberts and Shawon SM Rahman. 2021. Does Digital Native Status Impact End-User Antivirus Usage? *International Journal of Computer Networks & Communications (IJCNC)* (2021).

[49] Ronald W Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology* (1975).

[50] Ronald W Rogers. 1983. Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. *Social Psychology: A Source Book* (1983).

[51] Christine Satchell and Paul Dourish. 2009. Beyond the User: Use and Non-Use in HCI. In *In Proceedings of the Australian Computer-Human Interaction Special Interest Group (OZCHI)*.

[52] Security.org. 2024. 2024 Antivirus Trends, Statistics, and Market Report. https://www.security.org/antivirus/antivirus-consumer-report-annual/ [Online; accessed 14.11.2024].

[53] Neil Selwyn. 2003. Apart from Technology: Understanding People's Non-Use of Information and Communication Technologies in Everyday Life. *Technology in Society* (2003).

[54] Noor Suhani Sulaiman, Muhammad Ashraf Fauzi, Suhaidah Hussain, and Walton Wider. 2022. Cybersecurity Behavior Among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information* (2022).

[55] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the USENIX Security Symposium (USENIX Security)*.

[56] TechTarget. 2023. Antivirus Software. https://www.techtarget.com/searchsecurity/definition/antivirus-software [Online; accessed 14.11.2024].

[57] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. 2017. "Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior. *Computers & Security* (2017).

[58] TODAY. 2024. Explainer: Why Are Android Devices Prone to Malware and How Can Users Guard Against It? https://www.todayonline.com/singapore/explainer-why-android-devices-prone-online-scams-users-guard-against-it-2252066 [Online; accessed 14.11.2024].

[59] Ali Vafaei-Zadeh, Ramayah Thurasamy, and Haniruzila Hanifah. 2019. Modeling Anti-Malware Use Intention of University Students in A Developing Country Using the Theory of Planned Behavior. *Kybernetes* (2019).

[60] Kami E Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by Updates: How Negative Experiences Affect Future Security. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.

[61] Silas Formunyuy Verkijika. 2018. Understanding Smartphone Security Behaviors: An Extension of the Protection Motivation Theory With Anticipated Regret. *Computers & Security* (2018).

[62] Wallarm. 2024. Mobile Malware. https://www.wallarm.com/what/mobile-malware [Online; accessed 2.9.2024].

[63] Irene Woon, Gek-Woo Tan, and R Low. 2005. A Protection Motivation Theory Approach to Home Wireless Security. In *Proceedings of the International Conference on Information Systems (ICIS)*.

[64] Jorja Wright, Maurice E Dawson Jr, and Marwan Omar. 2012. Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smart Phones. *Journal of Information Systems Technology and Planning (JISTP)* (2012).

[65] Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J Aviv, and Florian Schaub. 2024. Nudging Users to Change Breached Passwords Using the Protection Motivation Theory. *arXiv preprint arXiv:2405.15308* (2024).

[66] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.

A Interview Questionnaire

Part 1. Antivirus Software Adoption.

Q1: Have you ever heard of "Antivirus software" or "Vaccine software"? If so, please explain the purpose of antivirus software. [If participants are unfamiliar with both terms, we provide the names of well-known antivirus products in the Republic of Korea (*e.g.*, 'ALYac'[1] and 'V3'[2]) to proceed with the interview.]

Q2: Antivirus software is a security program designed to prevent, detect, search for, and remove various types of malware from computers, networks, and other devices. Have you ever used antivirus software on your smartphone? If yes, please share the list of antivirus software you currently use (or have used) with us.

Q2-1: When, how often, and which features of the antivirus software do (or did) you primarily use? [if applicable]

Q3: What reasons led you to (start using it / start and then stop using it / decide not to use it)?

Part 2. Demographic and Security Knowledge.

Q4: What gender do you identify with?

Q5: What is your age range?

- 19-28
- 29-38
- 39-48
- 49-58
- 59+

Q6: What is the highest degree or level of school that you have completed?

- Middle school or Less
- High school or equivalent

[1] 'ALYac' developed by EST Security (https://en.estsecurity.com/product/alyac)

[2] 'V3' developed by AhnLab (https://www.ahnlab.com/en/product/v3-mobile-plus)

- Associate's Degree
- Bachelor's degree
- Master's degree
- PhD
- Others
- I prefer not to answer.

Q7: Do you have any experience in computer science? If so, what is it?
Q8: Which of the following is not a type of malware?

- Worm
- Trojan
- Firewall
- Virus
- I don't know.

Q9: What is the main purpose of ransomware?

- It places unwanted advertisements on your computer.
- It monitors and tracks the user's search history.
- It encrypts the user's files and asks for money to restore them.
- It takes control of your computer and deletes files.
- I don't know.

Q10: How does the 'Drive-by Download' method distribute malware?

- Malware is inserted into websites visited by users and automatically downloaded.
- It is distributed by encouraging users who receive emails containing malicious code to download attached files or click links.
- It spreads malware using Wi-Fi networks connected to users.
- Files containing malware are spread through file-sharing programs.
- I don't know.

B Interview Codebook

Table 8 presents the complete interview codebook from the interview study. The codebook includes codes for three open-ended questions concerning participants' motivations for adopting, discontinuing, or not using antivirus software.

C Items in our research model

Table 9 presents the items for each construct, along with their sources, utilized in our extended PMT research model.

D Survey Questionnaire

[Screening Questions]
Title: Survey on Smartphone Usage Patterns
This survey aims to understand your smartphone usage patterns. To ensure that this survey is relevant to you, we will first check your eligibility. Thank you for your cooperation.
SQ1: What is the operating system (OS) of your smartphone? [Single choice; Proceed with respondents who select the 'Android' option only]

- Android
- iOS
- Don't know or Do not use a smartphone
- Prefer not to answer

SQ2: Are you currently employed? If so, does your workplace's security policy affect your smartphone usage? [Single choice; Proceed with respondents who select the 'No' option only]

- Yes. I am required to install either a security app developed by my workplace or a commercial/free security app on my smartphone.
- No. My smartphone usage is not affected by my workplace's security policies.

SQ3: What is the operating system (OS) of your personal PC/laptop (*e.g.*, computer or laptop used at home)? If you use more than one device, please select all that apply. [Multiple choice; Proceed with respondents who select the 'Microsoft Windows' option]

- Windows
- Mac
- Don't know or Do not use a personal PC/laptop
- Prefer not to answer

SQ4: Does your workplace's security policy affect your use of a personal Windows PC/laptop? [Single choice; Proceed with respondents who select the 'No' option only]

- Yes. I am required to install either a security program developed by my workplace or a commercial/free security program on my personal Windows PC/laptop.
- No. My use of a personal Windows computer/laptop is not affected by my workplace's security policies.

[Main Survey]
This survey investigates your perceptions and experiences with antivirus software. It is composed of three sections:
Section 1: Questions about your perception of antivirus software for smartphones.
Section 2: Questions about your experience using such software on your smartphone and personal PC/laptop.
Section 3: Questions about your general demographic information.

Consent Form: You are invited to voluntarily participate in this survey and have the right to withdraw at any time without providing a reason. The data collected will be used solely for academic publications and will not be shared outside of the research team. All collected information will be deleted upon the completion of the study. The survey is expected to take approximately 15 minutes to complete. Upon completion, you will receive a compensation of 2,500 KRW. If you have any questions about the survey or wish to have your responses deleted after submission, please contact the researcher at 22sysy@skku.edu.
If you want to proceed, please click the "Next" button below.

Section 1. Questions about your perception of antivirus software for smartphones.
Q1: Are you familiar with the term "malware"? [single choice]

- Yes, I am familiar with it.
- No, I am not familiar with it.
- Unsure.

Q2: Are you familiar with the term "Antivirus Software"? [single choice]

- Yes, I am familiar with it.
- No, I am not familiar with it.
- Unsure.

Please read the following explanation carefully before responding to the subsequent questions.
Malware is a type of software designed to infiltrate electronic devices such as computers, smartphones, or tablets and perform actions that the user did not intend or that are malicious in nature. Malware can take various forms and serve different purposes, such as stealing personal information without the user's consent or damaging the functionality of electronic devices.
Antivirus software is security software designed to protect users' electronic devices, like computers or smartphones, from malware. These programs work in various ways to prevent, detect, and remove malware. By doing so, they protect devices from threats such as personal data breaches, financial losses, and damage to the device's functionality. Examples of such products include AlyacM, V3, McAfee, and Norton.

Table 8: Codebook for Interview.

No.	Codes	# Responses
A	**Reasons to adopt**	**22**
A.1	**Standalone Antivirus Software**	
A.1.1	To prevent malware	6
A.1.2	Psychological comfort (*e.g.*, habitual use, for reassurance)	3
A.1.3	Installed by family	1
A.2	**Plugin Antivirus Software**	
A.2.1	Unwanted, but necessary to use other services (*e.g.*, finance, shopping, and securities services)	7
A.2.2	For general smartphone security (*e.g.*, to prevent credentials leakage, malware infections, and security incidents)	3
A.2.3	Not remembered, but kept due to its security-related appearance	2
B	**Reasons to discontinue**	**15**
B.1	**Standalone Antivirus Software**	
B.1.1	Not engaging in risky behavior (*e.g.*, avoiding malicious websites, minimizing internet usage)	3
B.1.2	The iPhone is secure from malware	2
B.1.3	Not feeling the effect of the software (*e.g.*, not noticing any difference between using and not using the software)	1
B.1.4	Performance degradation (*e.g.*, reduced performance, increased battery drain, unnecessary features like VPNs)	1
B.2	**Plugin Antivirus Software**	
B.2.1	Not required to install (*e.g.*, when using a banking app after switching to iPhone)	2
B.2.2	No valuable information to safeguard on smartphones	2
B.2.3	The iPhone is secure from malware	1
B.2.4	Ineffectiveness (*e.g.*, ineffective in preventing credential leaks)	1
B.2.5	No security issues (*e.g.*, malware infection, security incidents, information leak)	1
B.2.6	Concerns about the software being exploited by malicious actors or malware	1
C	**Reasons to not use**	**20**
C.1	Belief in data breaches have no major harm (*e.g.*, trusting financial authorities, not feeling the severity)	3
C.2	Data is valuable, but there is no data to protect on smartphones	2
C.3	Security-critical services already have built-in security measures (*e.g.*, banking app)	2
C.4	No security incidents experienced so far (*e.g.*, malware infection, hacking)	2
C.5	Belief in not being a likely hacking target (*e.g.*, not having enough financial capital, not a key person in the organization)	2
C.6	Doubts about the effectiveness of the software (*e.g.*, excessive hype, low reputation of the manufacturer)	2
C.7	No need (*e.g.*, careful use of the phone can prevent malware infection)	2
C.8	No one around using the apps	2
C.9	The iPhone is secure from malware	1
C.10	Inconvenient to use (*e.g.*, frequent software updates are required)	1
C.11	Not aware that antivirus software existed for smartphones	1

Figure 2: Malware.

Figure 3: Antivirus Software.

Q3: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

- I follow news and advancements in smartphone malware technology.
- I discuss security issues related to smartphone malware with friends and people around me.
- I read about the problems of malicious applications intruding on smartphone users' devices.
- I seek advice on the Internet or in communities about antivirus products.
- I am aware of the problems and consequences associated with smartphone malware.

Q4: How likely or unlikely do you think you are to experience the following incidents? [Array of single-choice questions; 5-point scale with endpoints "Very Unlikely" and "Very Likely"]

- My smartphone is infected with malware.
- I am the target of a malware attack.

Q5: Please rate to what extent the following incidents would be a serious problem for you. [Array of single-choice questions; 5-point scale with endpoints "Not At All serious" and "Very Serious"]

- Personal information on my smartphone leaks because of malware.
- The performance of my smartphone slows down due to malware.
- Economic losses are incurred due to malware.

Q6: This is an attention check question, so please click on the answer 'Neutral.' [5-point scale: "Strongly Disagree", "Disagree", "Neutral", "Agree" and "Strongly Agree"]

Q7: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

Table 9: Items for Each Construct in Our Research Model.

Construct	Items	Measure (5-point Likert scale)	Ref
Perceived Vulnerability (PV)	How likely or unlikely do you think you are to experience the following incidents? PV1. My smartphone is infected with malware. PV2. I am the target of a malware attack.	Very Unlikely to Very Likely	[27, 63, 65]
Perceived Severity (PS)	Please rate to what extent the following incidents would be a serious problem for you. PS1. Personal information on my smartphone leaks because of malware. PS2. The performance of my smartphone slows down due to malware. PS3. Economic losses are incurred due to malware.	Not At All Serious to Very Serious	[27, 65]
Response Efficacy (RE)	Please rate your level of disagreement or agreement with the following statement. RE1. Antivirus software can prevent malware infections on my smartphone. RE2. Antivirus software can detect and remove malware present on my smartphone. RE3. Antivirus software is the best solution for counteracting problems caused by malware. RE4. Antivirus software can significantly reduce the threats posed by malware on my smartphone.	Strongly Disagree to Strongly Agree	[3, 39]
Self-Efficacy (SE)	Please rate your level of disagreement or agreement with the following statement. SE1. I can select the appropriate antivirus software for my smartphone. SE2. I can correctly install antivirus software on my smartphone. SE3. I can correctly detect and remove malware from my smartphone using antivirus software. SE4. I can use antivirus software even if I have never used a system like it before. SE5. I can solve potential system problems that may arise during the operation of antivirus software, such as system crashes.	Strongly Disagree to Strongly Agree	[3, 13]
Response Costs (RC)	Please rate your level of disagreement or agreement with the following statement. RC1. Antivirus software is expensive to purchase and operate. RC2. Installing antivirus software on my smartphone would require a significant amount of time RC3. Using antivirus software on my smartphone would require a significant investment of effort. RC4. Employing antivirus software often leads to significant system overhead issues (*e.g.,* slow performance, lack of space, etc.). RC5. Using antivirus software causes conflicts with other applications on my smartphone. RC6. Using antivirus software is a hassle for me.	Strongly Disagree to Strongly Agree	[3, 10, 39, 57]
Social Norms (SN)	Please rate your level of disagreement or agreement with the following statement. SN1. My family recommends installing and using antivirus software on my smartphone. SN2. My friends recommend installing and using antivirus software on my smartphone. SN3. My organization or co-workers recommend installing and using antivirus software on my smartphone. DN1. I believe that most smartphone users have antivirus software on their smartphones. DN2. I believe that the smartphone users around me have antivirus software on their smartphones.	Strongly Disagree to Strongly Agree	[3, 57]
Awareness (AW)	Please rate your level of disagreement or agreement with the following statement. AW1. I follow news and advancements in smartphone malware technology. AW2. I discuss security issues related to smartphone malware with friends and people around me. AW3. I read about the problems of malicious applications intruding on smartphone users' devices. AW4. I seek advice on the Internet or in communities about antivirus products. AW5. I am aware of the problems and consequences associated with smartphone malware.	Strongly Disagree to Strongly Agree	[22]
Intent to Adopt Antivirus Software (IA)	Please rate your level of disagreement or agreement with the following statement. IA1. I intend to install and use antivirus software on my smartphone within the next three months. IA2. I intend to run antivirus software on my smartphone as needed. IA3. I intend to ensure that antivirus software is always active on my smartphone.	Strongly Disagree to Strongly Agree	[3]
Attention Check	This is an attention check question, so please click on the answer 'Neutral'.	Strongly Disagree to Strongly Agree	

Note that *social norms* combine *subjective norms* and *descriptive norms (DN1 and DN2)*, based on the results of our pilot study's factor analysis.

- Antivirus software can prevent malware infections on my smartphone.
- Antivirus software can detect and remove malware present on my smartphone.
- Antivirus software is the best solution for counteracting problems caused by malware.
- Antivirus software can significantly reduce the threats posed by malware on my smartphone.

Q8: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

- I can select the appropriate antivirus software for my smartphone.
- I can correctly install antivirus software on my smartphone.
- I can correctly detect and remove malware from my smartphone using antivirus software.
- I can use antivirus software even if I have never used a system like it before.
- I can solve potential system problems that may arise during the operation of antivirus software, such as system crashes.

Q9: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

- Antivirus software is expensive to purchase and operate.
- Installing antivirus software on my smartphone would require a significant amount of time.
- Using antivirus software on my smartphone would require a significant investment of effort.
- Employing antivirus software often leads to significant system overhead issues (*e.g.,* slow performance, lack of space, etc.).
- Using antivirus software causes conflicts with other applications on my smartphone.
- Using antivirus software is a hassle for me.

Q10: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

- My family recommends installing and using antivirus software on my smartphone.
- My friends recommend installing and using antivirus software on my smartphone.
- My organization or co-workers recommend installing and using antivirus software on my smartphone.
- I believe that most smartphone users have antivirus software on their smartphones.

- I believe that the smartphone users around me have antivirus software on their smartphones.

Q11: Please rate your level of disagreement or agreement with the following statement. [Array of single-choice questions; 5-point scale with endpoints "Strongly Disagree" and "Strongly Agree"]

- I intend to install and use antivirus software on my smartphone within the next three months.
- I intend to run antivirus software on my smartphone as needed.
- I intend to ensure that antivirus software is always active on my smartphone.

Section 2. Questions about your experience using such software on your smartphone and personal PCs/laptop (Windows only).
Section 2.1. Smartphone
Q1: Have you ever used antivirus software on your smartphone?

- Yes, I am currently using it. (Proceed to Q2-1.)
- Yes, I have used it in the past. (Proceed to Q2-2.)
- No, I have never used one. (Proceed to Q2-3.)

Q2-1: What reasons led you to start using it? [free text] (Proceed to Q3)
Q2-2: What reasons led you to start and then stop using it? [free text] (Proceed to Q3)
Q2-3: What reasons led you to decide not to use one? [free text] (Proceed to Section 2.2. PCs/laptop)
Q3: How often do (or did) you scan your smartphone with antivirus software? [single choice]

- Always (*e.g.*, real-time detection feature)
- More than once a day
- 1-2 times a week
- 1-2 times a month
- 1-2 times a year
- Only when needed (In what situations do you perform scans? Please specify)
- Rarely used (Why do you not use it more frequently? Please specify)
- Others (Please specify):

Q4: Please select the names of all antivirus software you are currently using (or have used) on your smartphone. The software is listed in alphabetical order. If your software is not listed, please write its name in the "Others" field at the bottom. [multiple choice]

- Naver Vaccine
- Citizen Conan – Phishing Eyes Police, Voice Phishing, Smishing
- AlyacM – All-in-One Smartphone Security/Protection/Care/Shopping
- Phone Guardian: Protects Personal Information with Anti-Hacking VPN Technology
- TouchEn M-Vaccine for Web (Enterprise)
- TouchEn M-Vaccine for App (Enterprise)
- SK Shieldus Mobile Guard – Antivirus, Security, Smishing/Virus Scan
- Antivirus AI
- Anti-virus Dr.Web Light
- Anti Spyware: Spy Detector, Virus Protection
- Avast Security – Antivirus/Cleaner/Security
- AVG Smartphone Virus Removal Security App
- AVG Protection
- Avira Security Antivirus & VPN
- Bitdefender Mobile Security
- Bitdefender Antivirus
- Certo: Anti Spyware & Security
- C-Prot Antivirus Security
- ESET Mobile Security Antivirus
- F-Secure: Total Security & VPN
- Kaspersky: VPN & Security
- Malwarebytes Mobile Security
- McAfee Security: Antivirus VPN
- Microsoft Defender: Antivirus
- Norton 360: Mobile Security
- Sophos Intercept X for Mobile
- V3 Mobile Plus
- V3 Mobile Security – Antivirus/Cleaner/Security
- V-Guard2 for App
- V-Guard2 for Web
- TotalAV Mobile Security
- Others (Please specify):
- Do not recall

Section 2.2. PCs/laptops (Windows OS only)
Q1: Have you ever used antivirus software on your personal PCs/laptops?

- Yes, I am currently using it. (Proceed to Q2-1.)
- Yes, I have used it in the past. (Proceed to Q2-2.)
- No, I have never used one. (Proceed to Q2-3.)

Q2-1: What reasons led you to start using it? [free text] (Proceed to Q18)
Q2-2: What reasons led you to start and then stop using it? [free text] (Proceed to Q18)
Q2-3: What reasons led you to decide not to use one? [free text] (Proceed to Section 3. Demographic)

Q3: How often do (or did) you scan your PCs/laptops with antivirus software? [single choice]

- Always (*e.g.*, real-time detection feature)
- More than once a day
- 1-2 times a week
- 1-2 times a month
- 1-2 times a year
- Only when needed (In what situations do you perform scans? Please specify)
- Rarely used (Why do you not use it more frequently? Please specify)
- Others (Please specify):

Q4: Please select the names of all antivirus software you are currently using (or have used) on your PCs/laptops. The software is listed in alphabetical order. If your software is not listed, please write its name in the "Others" field at the bottom. [multiple choice]

- ALYac25
- AhnLab V3 Endpoint Security 9.0
- AhnLab V3 365 Clinic
- AVG™ Internet Security
- Avira Internet Security
- Bitdefender Total Security
- Cyber Protect
- eScan Internet Security Suite
- ESET Security Ultimate
- F-Secure Total
- G DATA Internet Security
- K7 SECURITY Total Security
- Kaspersky Plus
- McAfee Total Protection
- Microsoft Defender Antivirus
- Norton 360
- PC Matic Application Allowlisting
- TOTALAV Total AV
- TREND MICRO Internet Security
- Others (Please specify):

- Do not recall

Section 3. Questions about your general demographic information.

Q1: What is your gender?

- Male
- Female
- Others (Non-binary/Third gender)
- Prefer not to answer

Q2: What is your age range?

- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 years or older
- Prefer not to disclose

Q3: What is the highest degree or level of school you have completed?

- Less than high school
- High school or equivalent
- Associate's degree
- Bachelor's degree
- Graduate degree or Master's degree
- Doctorate degree
- Prefer not to answer
- Others

Q4: What is your current occupation?

- Architect
- Artist
- Developer
- Designer
- Dentist
- Doctor
- Engineer
- Home-maker
- Judge
- Journalist
- Lawyer
- Musician
- Nurse
- Paralegal
- Pharmacist
- Professor
- Student
- Self-employed
- Teacher
- Veterinarian
- Writer
- Unemployed
- Retired
- Prefer not to answer
- Others

Q5: Which of the following best describes your educational background or job field?

- I have an education in, or work in, the field of computer science, computer engineering, or IT.
- I do not have an education in, nor do I work in, the fields of computer science, computer engineering, or IT.

Q6: Please estimate your total household income for this year.

- Less than ₩10 million
- ₩10-₩20 million
- ₩20-₩40 million
- ₩40-₩60 million
- ₩60-₩80 million
- ₩80-₩100 million
- ₩100 million or more
- Prefer not to answer

E Survey Demographics

Table 10: Demographics in the Online Survey.

Age		
18-24	9	(3.6%)
25-34	48	(19.2%)
35-44	84	(33.6%)
45-54	70	(28.0%)
55-64	30	(12.0%)
65+	9	(3.6%)
Gender		
Male	85	(34.0%)
Female	165	(66.0%)
Others	0	(0.0%)
Refer not to Disclose	0	(0.0%)
Education Level		
Less than high school	1	(0.4%)
High school or equivalent	40	(16.0%)
Associate's degree	53	(21.2%)
Bachelor's degree	132	(52.8%)
Graduate degree or Master's degree	19	(7.6%)
Doctorate degree	3	(1.2%)
Prefer not to answer	1	(0.4%)
Other	1	(0.4%)
Occupation		
Homemaker	49	(19.6%)
Unemployed	19	(7.6%)
Office worker	15	(6.0%)
Engineer	13	(5.2%)
Education field	11	(4.4%)
Self-employed	9	(3.6%)
Designer	8	(3.2%)
Medical field	7	(2.8%)
Student	7	(2.8%)
Architect	4	(1.6%)
Retired	4	(1.6%)
Artist	3	(1.2%)
Developer	2	(0.8%)
Prefer not to answer	33	(13.2%)
Other	66	(26.4%)
CS Background		
Yes	31	(12.4%)
No	219	(87.6%)
Income		
Less than ₩10 million	40	(16.0%)
₩10-₩20 million	20	(8.0%)
₩20-₩40 million	78	(31.2%)
₩40-₩60 million	56	(22.4%)
₩60-₩80 million	22	(8.8%)
₩80-₩100 million	9	(3.6%)
₩100 million or more	5	(2.0%)
Prefer not to answer	20	(8.0%)