Evaluating User Behavior in Smartphone Security: A Psychometric Perspective

Hsiao-Ying Huang[1], Soteris Demetriou [2], Muhammad Hassan[1], Güliz Seray Tuncay [3], Carl A. Gunter [1], and Masooda Bashir[1]

[1]University of Illinois at Urbana-Champaign, {*hhuang65*[*], *mhassa42, mnb, cgunter*}@illinois.edu
[2]Imperial College London, *s.demetriou@imperial.ac.uk*
[3]Google, *gulizseray@google.com*

Abstract

Smartphones have become an essential part of our modern society. Their popularity and ever-increasing relevance in our daily lives make these devices an integral part of our computing ecosystem. Yet, we know little about smartphone users and their security behaviors. In this paper, we report our development and testing of a new 14-item Smartphone Security Behavioral Scale (SSBS) which provides a measurement of users' smartphone security behavior considering both technical and social strategies. For example, a technical strategy would be resetting the advertising ID while a social strategy would be downloading mobile applications only from an official source.The initial analysis of two-component behavioral model, based on technical versus social protection strategies, demonstrates high reliability and good fit for the social component of the behavioral scale. The technical component of the scale, which has theoretical significance, shows a marginal fit and could benefit from further improvement. This newly developed measure of smartphone security behavior is inspired by the theory of planned behavior and draws inspiration from a well-known scale of cybersecurity behavioral intention, the Security Behavior Intention Scale (SeBIS). The psychometrics of SSBS were established by surveying 1011 participants. We believe SSBS measures can enhance the understanding of human security behavior for both security researchers and HCI designers.

[*]Hsiao-Ying Huang is best reachable at hhsiaoying@gmail.com

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, ANAHEIM, CA., USA.

1 Introduction

Smartphones have become an essential part of modern society. In 2021, about 85% of the adults in the U.S. owned smartphones, up from just 35% in 2011 [8]. Internationally, the number of global smartphones users is estimated at 6.8 billion, marking an 86.5% increase from 2016 [50]. Smartphones are now involved in almost any daily activity watched videos, and 45% did online shopping [16]. As smartphones have become a hub for storing and accessing personal sensitive information [35], an increasing number and a diverse set of malicious parties have sought to exploit security vulnerabilities of smartphones and their users.

Mobile operating system developers have consequently been dedicated to equipping their systems with numerous counter measures (e.g., discretionary and mandatory access control, trusted computing *etc.*). However, the security of such systems still heavily relies on the behavior and decision-making of users. For instance, Android and iOS feature a permission model to enable users to decide if they want to grant mobile applications access to sensitive system resources and information. Some repackaged malware apps aim to trick users by mimicking the look-and-feel of popular legitimate apps with subtle differences in their title or logo to attract users to download, trust, and grant them permissions [66]. Other attacks target the intricate configuration properties of smartphones: attackers can exploit the vulnerabilities in the permission models to elevate their privileges and obtain unauthorized access to sensitive user data [40, 60, 65]; attackers can extract users' passwords when they access sensitive web domains (*e.g.* their bank account) from their smartphones on a public network [39]. Users who have never reset their advertising ID, can be subjected to fine-grained profiling by advertising libraries [57] [63]; users who are not attentive to the information provided by websites or applications can become the victims of phishing attacks [5, 26, 45, 61]. Since users play a such critical role in smartphone security, a better understanding of their behavior is crucial to help drive the design of better security mechanisms in mobile apps as well

as in mobile operating systems.

When it comes to user behavior on smartphones, previous studies have investigated users' perceptions, attitudes, and behavior toward smartphone security. They have found that users tend to ignore warnings [6, 23, 36], have misconceptions about the operation of smartphone security features [27, 36, 46, 56], and show minimal attempts to protect their smartphones [15, 46]. Users' careless behavior on smartphones can particularly result from their misunderstanding of the capabilities of these devices. Most smartphone users view their smartphone as just a mobile device for entertainment and communication; they are not aware it is in fact a hand-held computer vulnerable to a wide range of cyber-attacks [38] . Users are highly likely to thus address security differently on smartphones than on other devices such as laptops or PCs. In this paper, we explore a system that can can measure users' smartphone security behavior in a systematic way across contexts.

Prior studies tried to operationalize security-related concepts in different ways. Some studies adopted field observation while others employed a self-reported approach [15, 22, 34, 59]. Since field observations usually require more resources and have limitations in assessing all aspects of security behavior, most studies utilized self-reported measurements. In terms of self-reported measurements, we found many studies developed their own measurements based on computer security or adopted those from smartphone measurements in other contexts. *Therefore, based on the current literature, there is a need for a measurement system for security behavior that is standardized and specific to smartphones.*

In order to fill this research gap, we made the first step towards providing a model for measuring human *smartphone* security behavior. We grounded it on the theory of reasoned action (TRA [24]) and the related theory of planned behavior (TPB) [1]. TRA is a well-established framework for conceptualizing and explaining human behavior with widespread applications. It posits that *behavior intentions* (BI) are immediate antecedents to *behavior*. Other established self-reported measures have accordingly been constructed to attempt to measure behavior, including relevant scales developed for computer security behavior intentions [20] and attitudes [22].

Similarly, we focused on developing a necessary measurement tool for recording smartphone-specific security behavior intentions. In particular, we developed a model and conducted an analysis to support a standardized scale for measuring users' smartphone security behavior intentions (BIs) to follow expert recommendations, based on a systematic psychometric approach [47]. We present a study with two phases evaluated on a total of 1011 participants. In our phase-1 study wherein we examined if the model of general computer security BIs could be applied to smartphone security BIs. We adopted four dimensions from a well-established measurement, the Security Behavior Intention Scale (SeBIS) developed by Egelman and Peer [20] and examined the fitness of these dimensions on users' smartphone security behavior by factor analysis. Our findings indicate *smartphone security BIs entail new dimensions that are different from the model of general computer security BIs*. Therefore, in our phase-2 study, we *created a new scale measurement for smartphone security using a systematic scale development procedure*. We operationalized expert-provided guidelines for securing mobile devices by aiming to capture users' intention to comply with such guidelines in a measurement. To assess if our new measurement reliably captures such intentions that represent smartphone security behavioral constructs we are interested in, we evaluated its dimensionality, scale reliability, and construct validity. Our results show that the new scale exhibits satisfactory psychometric properties: the full scale and both of its subscales have high internal consistency, all items map uniquely on one single component, and no correlation exists between the subscales. Lastly, convergent validity is also established between the new scale and SeBIS.

Our contributions are summarized as follows:

- We found that new dimensions are important when measuring smartphone security behavior. These are different from the general security behavior model.
- We introduce a new standardized scale tailored for smartphone security behavior intentions (SSBS) which is based on two factors (i.e., technical versus social) and showed good psychometric properties with high internal consistency.

The rest of the paper is organized as follows: in related work, we reviewed the literature that are most related to our study and proposed research questions based on research gap (Section 2). We then illustrated our psychometric approach and methodology (Section 3) and described the design and results of phase-1 (Section 4) and phase 2 (Section 5) studies respectively. Lastly, in Section 6 we discuss limitations and future work and conclude the paper in Section 7.

2 Background and Related Work

Theory Background. Researchers at the intersection of computer security and social sciences have grounded their analysis (e.g. the Technology Acceptance Model – TAM [17, 18]) on end-users' usage of technology based on psychological frameworks such as the theory of reasoned action (TRA [24]) and the related theory of planned behavior (TPB) [1, 42]. These posit that behavior is immediately preceded by a behavior intention (BI). In turn, behavior intention is a function of behavioral and normative beliefs, and the behavioral beliefs are determined by an individual's attitude toward performing the behavior. Understanding users' attitudes and intentions is fundamentally conducive to plausible interpretations of end-users' behavior and factors that might affect them. Researchers have only recently tried to operationalize such concepts in computer security. In particular, Faklaris et al. developed a new self-report measure (SA-6) for quantify-

ing end-user security attitudes [22], while Egelman et al. developed a 16-item self-report Security Behavior Intentions Scale (SeBIS) that they evaluated for both internal [20] and external validity [19]. However, these measures target general computer security behavior. Given the widespread use of smartphones, there is a need for complementary measurement standards targeted specifically at *smartphone* security behavior.

Smartphone Security. Prior works have examined smartphone users' behavior. Their findings can be categorized into three realms: the inattentiveness toward security warnings and messages [23, 36], the misconceptions of smartphone security [9, 36, 46, 56], and the low level of concern for smartphone security behavior [15, 37, 46]. In terms of behavioral measurements, previous studies assessed users' smartphone security behavior through field observations and self-reported measurements. For field observations, most studies focus on two aspects: users' authentication and locking behavior on smartphones [28, 29, 31, 32] and users' behavior on granting access [4, 25, 64]. Although field observation can probe into users' actual behavior in the real world, it usually focuses on a single aspect of the behavior, making it difficult to conveniently gain a comprehensive understanding on user behavior in a short period of time. Therefore, many studies adopt a self-reported approach to measure users' smartphone security behavior.

Low Level of Concern for Smartphone Security Behavior: Research has revealed that users in general exhibit a low level of behavioral security tendency on smartphones even though they perceive certain security threats (e.g., malware, data leakage) [15]. Furthermore, even though smartphone usage has increased and technology has advanced, general security awareness remains fairly low [37]. For instance, when selecting an application, most users did not pay attention to its information on security and privacy [46], even despite having the required knowledge and understanding [2].

Only a minority of users were interested in security and agreement information and they were more security and tech-savvy [46]. This suggests that smartphone security behavior is influenced by individual factors (e.g., knowledge, personal interests, and personalities) and can vary significantly between users.

Adapting General Self-Reports to Specific Domains. There are various means to measure self-reported smartphone security behavior. The most commonly used approach in prior research has been to develop measurements by adapting more general computer security assessments or by modifying a developed measurement from previous studies. For example, Das and Khan [15] generated a 6-item measure that was adapted from Microsoft's computing safety index. Jones and Chin [34] performed a survey study to investigate students' usage and security behavior on smartphones by asking seven questions about security practices. A more recent study by Thompson *et al.* [59] designed a five-item measure to assess smartphone security behavior in a personal context, which was adapted from a security behavioral assessment in personal computer usage by Liang and Xue [41]. Another recent (2018) survey study by Verkijika [62] examined South African users' smartphone security practices by using five questions that were adapted from the measurement developed by Thompson et al. [59].

While reviewing developed security measurements (see Table 6), we found there is no standardized and targeted way to measure smartphone security behavior intentions across different contexts. Existing methods are all adopted or adapted from general computer security behavior measurement tools. However, it is possible that users' smartphone behavior can deviate from their computer behavior. For instance, Chin et al. [9] found participants' behavior and activities on smartphones were quite different from their use of laptops. For example, users were less likely to purchase and perform sensitive tasks on their smartphones because of security concerns regarding mobile devices. Moreover, none of these smartphone security measures were grounded on psychological principles that can help us better interpret and compare results.

Conclusion and Main Objective. We thus identified two key gaps in the current literature: 1) there is no standardized measurement of smartphone security behavior intentions across contexts; 2) it remains unclear if *general* computer security behavior intentions can be applied to assess *smartphone* security behavior intentions. A key goal of this study was to develop the first standardized, valid, and specialized measurement of smartphone security behavior intentions that can be used in different contexts and form the basis for studying smartphone security behavior. Toward this goal, we posed the following concrete research questions:

- **RQ1:** How adequate is the adaptation of general computer security BIs measurement to smartphone security?
- **RQ2:** If this adaptation is not adequate, can we develop a measure to capture smartphone security BIs?

3 A Psychometrics Approach

To answer these research questions, we adopted a psychometric approach. Psychometrics is a scientific approach of quantifying human psychological attributes such as personality traits, cognitive abilities, and social attitudes [44]. Well developed and widely-used security-related psychometric measurements are the "self-report measure of security attitudes" (SA-6) developed by Faklaris et al. [22] and the "Security Behavior Intentions Scale" (SeBIS) developed by Egelman and Peer [20], which are both grounded on the "Theory of Reasoned Action". They conceptualize users' *general* security behavior as a psychological construct instead of an actual

behavior. We followed the same approach to conceptualize users' *smartphone* security behavior intentions.

Evaluation Properties. We developed the Smartphone Security Behavioral Scale (SSBS), a new measure for assessing users' behavior intentions to comply with good smartphone security practices. When developing a new scale, it is important to evaluate three psychometric properties of the measurement: dimensionality, scale reliability, and convergent validity [47].

Dimensionality. Identifying dimensionality of a construct is a critical part of scale development because whether the construct is uni-dimensional or multi-dimensional will affect the structure and computing approach of scale [47]. There are two statistical approaches to determine dimensionality based on the use case. If the goal of testing is to 'explore' the unknown dimensions of a construct, the Exploratory Factor Analysis (EFA) is an appropriate method to use. If the goal is to 'confirm' or examine the existing dimensions of a construct, then the Confirmatory Factor Analysis (CFA) is a standardized way to test the fitness of the model.

Scale Reliability. In psychometrics, reliability represents the consistency of a measurement, which can be evaluated in various ways [47]. In this study, we focused on assessing "internal consistency" of the scale to determine if multiple items in a scale measure the same construct by examining Cronbach's alpha [13]. Cronbach's alpha is the mean of all possible coefficients among items [12]. The cut-off point of Cronbach's alpha is 0.70 [48] and refers to the acceptable internal consistency of the scale. In addition, considering the numbers of items can affect the score of Cronbach's alpha [12, 58], we also reported the mean of inter-item correlation (ITC), which is the average pairwise correlation among all items and provides a direct indicator of homogeneity [11].

Construct Validity. Construct validity refers to the degree to which a measurement truly reflects the concept being examined [7]. One approach is to evaluate convergent validity between the newly-developed scale and an existing scale measuring the same construct [47, 49]. Convergent validity is measured by correlational coefficients between the new measure and an existing measure. In our study, we evaluated the convergent validity between our scale and SeBIS [20] and tested if our scale measures similar constructs of security behavior.

Since there has been a well-established computer security behavioral intentions scale (SeBIS), our first step was to examine if the dimensionality of SeBIS could be applied to users' smartphone security behavior intentions. Our findings indicate different dimensions of smartphone security. Therefore, we followed a standardized procedure of scale development proposed by Netemeyer [47]. Our procedure of scale development is summarized as follows:

1. Testing the fitness of dimensional model of SeBIS on smartphone security behavior by applying CFA.
2. Defining the construct that the scale attempted to measure and generating a list of candidate questions.
3. Extracting the dimensional components of the scale by performing EFA and reducing the set of items.
4. Finalizing the scale by conducting CFA to confirm the fitness of the new scale to the intended factorial model.

Methodology. The goal of this study is to develop a measurement to assess users' security behavior intentions to comply with smartphone security advice recommended by security professionals. We conducted a two-phase online survey study, approved by our Institutional Review Board. In phase-1, we tested the four dimensions used in SeBIS [20]. Our results suggest the possibility of improving on the four dimensions of SeBIS when specializing them to smartphone security behavior intentions. In other words, users' smartphone security behavior intentions could be different from their general computer security behavior intentions. We therefore conducted a phase-2 study to develop a new measurement for smartphone security behavior intentions.

For both phases, we recruited participants from the United States via Amazon Mechanical Turk (MTurk). To ensure data quality, we integrated attention-check questions in each section of the survey. The attention-check questions were randomly inserted in the questionnaire and had similar format to other questions. Participants were required to select the choice required in the statement (for instance, *I go to grocery shopping on every Thursday. Please select 'Never'*). We removed the responses from participants who failed to correctly answer attention-check questions. We next describe the details of study design and results for each phase of the study.

4 Phase-1: Building the scale upon SeBIS

4.1 Survey design and item generation

We first developed a measurement, which we call *smartphone-SeBIS*, based on the four dimensions of SeBIS: device securement, password management, proactive awareness, and update. We generated items by revising each question in SeBIS for a smartphone context. For example, we changed the wording of questions from 'computer' to 'smartphone'. However, we encountered two challenges when using this approach. First, we found that certain questions could not be readily applied to smartphones. Secondly, certain common smartphone-specific security features were not included in SeBIS, such as biometrics, usage of applications, and app permissions. To capture a more comprehensive view of users' smartphone security behavior, we recruited security experts who independently went over each item of the first version of smartphone-SeBIS and considered how to revise old items and add new items to the survey. Overall, we had four types of item modifi-

cations: word/phrase substitution, word/phrase revision, item deletion, and item addition.

Word/Phrase Substitution. we substituted words indicating the context of a laptop or desktop machine to specifically describe a smartphone. For instance, to capture the same behavior on a smartphone device, we substituted the word "smartphone" for "laptop or tablet" in the item "*I use a password/passcode to unlock my laptop or tablet.*"

Word/Phrase Revision. some items could not be made smartphone-specific with simple substitutions. For example, "*I do not change my passwords, unless I have to*". This was revised to the following: "*I regularly change my password for online services/accounts using my smartphone,*" where we specified the password target to avoid confusion and turned the negative statement into a positive statement. We did this since participants might be biased toward taking a defensive stance against the negative behavior.

Item Deletion. Some of the SeBIS items are not applicable to the smartphone context. For instance, the item "*When browsing websites, I mouse-over links to see where they go, before clicking them*" is not applicable on mobile devices since the pointing mechanism on smartphones is different (mouse or trackpad for desktops/laptops vs finger or stylus on mobile devices). Such items were removed from the survey.

Item Addition. Several important smartphone security behaviors were not specified or included in SeBIS. For instance, significant security mechanisms introduced by Original Equipment Manufacturers (OEMs), or by the research community, become obsolete if the user roots (or jailbreaks) their smartphone. This is an important "device securement" measurement to take. Moreover, on smartphones, user privacy is preserved through a permission system that allows users to determine what device and personal information each installed third-party app can access. This mechanism can also be compromised if users become inattentive to permission requests or if they never revoke permissions from apps [23, 64]. To address such phenomena, we added relevant smartphone-specific items into the survey.

As a result of this exercise, we developed the Smartphone-SeBIS, a comprehensive instrument consisting of 20 items targeting smartphone security behaviors (see Table 5). We administered the Smartphone-SeBIS through an online survey using Amazon MTurk, where participants were asked to respond on a 5-point Likert-type scale ranging from Never' to Always'. To mitigate the potential priming effect of social desirability, we advertised our study as an investigation into 'the use of smartphones and mental health wellness' and included several related questions in the survey questionnaire. To control for potential order effects, the survey sections were randomized. After completing the questionnaire, participants were asked to provide demographic information.

Survey demographics. We recruited a total of 100 participants. Ages of participants were between 18 to 71 (μ=36.2, σ=11.4), and 41 of them are female (41%). Thirteen percent of our participants had a high school diploma (n=13); 36% had some college or associate degree (n=36); 36% had bachelor's degree (n=36); and 15% had a graduate or professional degree (n=15). The average time to take the survey was 11.7 minutes. The participants were remunerated for their participation in the survey.

4.2 Results

The analysis shows that the internal reliability of the 20-item smartphone-SeBIS is below the recommended cutoff point by Nunnally (1978) (Cronbach's α=.67<.70) [48]. We further conducted Confirmatory Factor Analysis (CFA) to examine whether our measurement of the construct is consistent with SeBIS by the goodness-of-fit of data to the latent variable model. We used several tests to determine the goodness-of-fit of data to the model of SeBIS, including the Comparative Fit Index (CFI) and the Root Mean Square Error of Approximation (RMSEA).

According to our results, the CFI and TLI were 0.565 and 0.490, which are below the cutoff (0.90) recommended by Netemeyer et al. [47]. Furthermore, our RMSEA and SRMR were 0.127 and 0.152 respectively, which are above the recommended cutoff points (a cutoff of 0.06 for RMSEA and 0.08 for SRMR [33])). These results indicate poor goodness-of-fit of our data to smartphone-SeBIS. Put another way: *the revised four dimensions of smartphone-SeBIS might not be the best fit for assessing users' smartphone security behavior intentions.*

5 Phase-2: Developing SSBS

5.1 Survey design and item generation

To develop a new scale to measure users' smartphone security behavior intentions we employed the approach used by Egelman and Peer (2015). We first generated a list of smartphone security behaviors and collected data on Amazon MTurk. We then conducted an Exploratory Factor Analysis (EFA) to extract the effective items for assessing users' smartphone security behavior.

Item generation. According to Egelman and Peer [20], the metric of security behavior should be "applicable" to and "widely accepted" by the majority of users. Therefore, we generated a list of different smartphone security behavior based on the views of security professionals.

In conducting our study, we invited a panel of 35 subject matter experts in the field of security. The panelists consisted of faculty members, graduate and undergraduate students specializing in cyber-security, who are participating in a security focused reading seminar. These expert panelists were tasked with identifying and ranking the 10 most critical types of smartphone security behavior(Table: 9). Meanwhile, two security researchers then categorized these security behaviors

into *Technical* and *Social* behaviors. The researchers also examined public security advice for smartphone security by the United States Computer Emergency Readiness Team (US-CERT) to ensure no important behaviors were missing from the list. Five security experts went through the list to determine if any item violated the principles of applicability and acceptance. Our initial list contained 45 types of behavior. We proceeded to translate these behaviors into personal statements. Survey participants were asked to read and rate each statement on a five point scale of frequency (From 'Never' to 'Always').

Survey Demographics. We collected 487 responses via Amazon MTurk. This is a larger sample than the sample size recommended by Hair *et al.* (minimum of 5 participants per item) [30]. The average age of participants was 34.6 and 44.8% were female (41%). About 11% of our participants had high school diplomas (n=54); 29% had some college or associate degree (n=142); 49.5% had a bachelor's degree (n=241); and 10.3% had a graduate or professional degree (n=50). The average time taken to complete the survey was 6.3 minutes. Participants were paid $0.75 after completing the survey and passing the validation checks.

5.2 Results

5.2.1 Exploratory Factor Analysis

Our analysis of Kaiser-Meyer-Olkin (KMO) test was 0.92 indicating the high sampling adequacy of variables, which suggest suitability for further factor analysis. Considering a large set of items, our approach was to refine our scales until the loading of each item was above 0.5 and was twice more than its loading on other components after a Varimax rotation [54]. Furthermore, we used optimal coordinates to determine the optimal number of factors, which is a non-graphical approach for factor determination [52]. The optimal coordinate is a determined point where the predicted eigenvalue is not greater than or equal to the mean eigenvalue by performing linear regression analysis of the last and $(i+1)$th eigenvalue [52]. By using optimal coordinates, we could overcome a limitation of subjective and unclear decision-making about the number of components to retain [52].

We performed three rounds of EFA to finalize our scale of smartphone security behavioral intention. In our first round of EFA, we first conducted Principal Component Analysis (PCA) and extracted five components in EFA based on optimal coordinate analysis. Next, we excluded 27 items based on the aforementioned loading criteria. In the second round of EFA, we followed the same procedure and extracted three components in EFA. 3 items were excluded from the list of items. In the third round of EFA, we also followed the same procedure performed in the last two rounds, extracted 2 components in EFA, and retained the remaining 14 items. The final set of items and their rotated factor loadings are presented in Table 3.

Analysis of the items revealed two distinct themes: *technical* approaches (*e.g.*, using a VPN and an anti-virus app) and *social* approaches (*e.g.*, verifying the source of texts before sharing and deleting suspicious communication). The *technical* items (T1...T8) describe actions that an Android user can take that are either supported by the underlying smartphone technology or can be supported by third-party add-on technology. For instance, the ability to reset the Advertising ID through the phone's Settings is an example of a feature supported by the underlying smartphone technology, while installing an anti-virus app is an example of a add-on feature by third-party. In contrast, the *social* items (S1...S8) pertain to behaviors that are socially constructed, in other words, it refers to behaviors that the user may exhibit while interacting and engaging with the technology. For example, item S2 refers to the user checking the source of an app during the process of downloading it. This is not a technical measure rather an interaction with the environment or context. Hence, our scale includes *Technical* and *Social* as two subscales.

5.2.2 Reliability of the Scale

We adopted the same approach used by Egelman and Peer [20] to examine the reliability of the scale based on three metrics. We first employed Cronbach's α, which is commonly used to assess internal consistency of a group of items. As shown in Table 3, the Cronbach's α for the full scale was 0.80. For subscales of technical and social approaches were 0.84 and 0.79 respectively. Our scale met the criteria of internal consistency that requires both full scale and all subscales to be above 0.7 [43, 49]. We subsequently leveraged the item-total correlation (ITC), which is the Pearson correlation between each item and the mean of all other items. All of our items' ITC are above the recommended threshold of 0.2 [21].

While assessing the reliability of the scale, it is also important to examine the diversity of the items of a scale and prevent the redundancy of the items [3]. Toward this end, we computed the average inter-item correlation (IIC) that not only evaluates the internal consistency but also tests the degree of redundancy of a set of items on a scale [10, 51]. The recommended correlational coefficient of IIC is between 0.20 and 0.40, which suggests that the items contain sufficient diversity of variance while they are still representative of the same construct [51]. The ITC of both our subscales fall within the range, which indicates the adequate level between consistency and diversity. Based on these three metrics, our full scale and sub-scales exhibit high reliability.

5.2.3 Convergent Validity: Correlation with SeBIS

To ensure that we assess the construct of users' security behavior, we measured the convergent validity of our scale and SeBIS. Convergent validity is a type of criterion validity that evaluates if a developed scale measures the same construct

Table 1: Pearson's Correlation between SeBIS and SSBS

	Correlation coefficient (p-value)	
SeBIS / SSBS	Technical approach	Social approach
Device securement	-.017 (p=.896)	.060 (p=.628)
Password generation	.290 (p=.018)	.229 (p=.064)
Proactive awareness	-.090 (p=.471)	.614 (p<.0001)
Update	.301 (p=.014)	.431 (p=.0003)

of the 'criterion' scale. We used SeBIS as our criterion because it is the only measure with high reliability for assessing security behavioral intentions. We collected a new dataset with 66 participants who completed both SeBIS and Smartphone Security Behavior Scale (SSBS). Then we conducted Pearson's correlation between SeBIS and SSBS. The average score of SeBIS had a significantly positive correlation with the average score of SSBS (r=.403, p=.0008). In addition, results show the positive significant correlation between the subscales of SeBIS and SSBS (see Table 1). These findings suggest that *participants who showed higher intentions in protecting their general security were also more likely to protect their smartphone security*. This confirms that our scale is measuring a similar construct with SeBIS, that of security behavior intentions.

5.2.4 Confirmatory data analysis

Our final step was to examine the goodness of fit of SSBS with the hypothesized latent components by performing Confirmatory Factor Analysis(CFA). We collected a new dataset with 358 U.S. participants from Amazon MTurk in the final round of our survey. Each participant was compensated for completing the survey. In order to mitigate the potential priming effect on participants' responses, we employed the same approach as in our phase-1 study by advertising the survey as research related to users' mobile phone usage and mental wellbeing so we included few related questions in the survey questionnaire. After completing the questionnaire, participants were asked to provide demographic information. To control for potential order effects on participants' responses, all survey sections were randomized. Additionally, we implemented a range of validity check measures to ensure data quality. These measures included the inclusion of several attention check questions throughout the survey to make sure the survey participants were attentive, restricting the survey participants to be between 18 and 65, including only 100% completed responses in our analysis, reverse coding when appropriate, and randomizing the order of survey questions to minimize any potential biases due to the ordering effects. In terms of demographics, 38% (n=136) of our participants were female and the average age of participants was 35.3 (σ=10.6). Each participant was paid $1 after completing the survey.

The reliability of full SSBS was 0.79, 0.81 for the *Technical* subscale, and 0.85 for the *Social* subscale. We conducted PCA with a Varimax rotation and extracted two components. The results show that all items were loaded on the same unique component as found in the previous EFA. We conducted CFA to examine the goodness-of-fit of the two-component model for users' smartphone security behavior intentions. We used the same approach employed in the Phase-1 study, by performing multiple test to determine the goodness of fit of our data to the model, including Comparative Fit Index (CFI), the Tucker-Lewis Index (TLI), the Root Mean Square Error of Approximation (RMSEA), and the Standardized Root Mean Square Residual (SRMR). Based on the analysis, the CFI and TLI were 0.954 and 0.942, which are above the cutoff (0.90) recommended by Netemeyer et al. [47]. Additionally, the RMSEA and SRMR were 0.054 and 0.059 respectively. Both scores are below the cutoff points recommended by [33]. Our results show a well goodness-of-fit of our data to our hypothesized two-component model. We also performed Pearson's correlation between the two subscales and found no significant correlations. Please see Table 2 for the details of CFA results.

6 Discussion & Future Work

6.1 Applications and Role of the SSBS

In this study, we determined that the psychological construct of smartphone security behavior differs from general security behavior measured by SeBIS [20]. Driven by this finding, we used a series of factor analyses to create a Smartphone Security Behavior Scale (SSBS) with 14 questions that loads onto two factors: a technical approach (using technical strategies to protect smartphones) and a social approach (being contextually aware and cautious while using their smartphones). Our scale exhibited satisfactory psychometric properties: the full scale and both the subscales have high internal consistency, all items map uniquely on one single component, and no correlation exists between the subscales while establishing convergent validity between SSBS and SeBIS. These indicate that SSBS is a well-established psychological construct and measurement. Furthermore, we distinguished a psychological construct of smartphone security behavior from a general security behavior measured by SeBIS [20]. This finding also corroborates that users have different security and privacy concerns and behaviors toward smartphone and laptop [9].

Using SSBS to measure Smartphone Security Behavior Intentions. Our new scale of smartphone security behavior intentions can be employed for various purposes. The most obvious utilization is for measuring smartphone end-users' security behavior intentions. While SeBIS has been shown to predict secure locking behavior on smartphones, some of its wording is outdated [22] as well some of its items are irrelevant to smartphone security actions. By contrast, SSBS items are specific to current smartphone functionality and

Table 2: SSBS Average variance extracted for CFA factor

	Standardized loading	R^2
Technical		
I reset my Advertising ID on my smartphone.	.715	.511
I hide device in my smartphone's bluetooth settings.	.641	.411
I change my passcode/PIN for my smartphone's screen lock at a regular basis.	.792	.627
I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).	.595	.354
I use an adblocker on my smartphone.	.529	.280
I use an anti-virus app.	.536	.287
I use a Virtual Private Network (VPN) app while connected to a public network.	.577	.333
I turn off WiFi on my smartphone when not actively using it.	.372	.139
Social		
I care about the source of the app when performing financial and/or shopping tasks on that app.	.770	.593
When downloading an app, I check that the app is from the official/expected source.	.785	.616
Before downloading a smartphone app I ensure the download is from official application stores (e.g. Apple App Store, GooglePlay, Amazon Appstore).	.799	.639
I verify the recipient/sender before sharing text messages or other information using smartphone apps.	.651	.423
I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.	.651	.424
I pay attention to the pop-ups on my smartphone when connecting it to another device (e.g. laptop, desktop).	.578	.334

SSBS reduces the number of items in the scale. This makes SSBS valuable in environments at risk that exhibit high use of smartphone technology.

Our scale has numerous potential applications across a variety of contexts. For instance, in a healthcare setting, a doctor who wishes to utilize health-related apps for treatment or self-management may use our scale to determine whether her patients require educational interventions before using the app. In a workplace setting, employers can use our scale to evaluate the risk of accidental insider threats arising from employees' use of smartphones and implement interventions to promote more secure behavior. In an educational context, schools can deploy our scale to assess the smartphone security behavior of both teachers and students as they embrace the use of smartphones for online education. Schools may also use our scale to gauge the vulnerability of their students and faculty to potential cyberthreats through smartphones, such as cyberbullying and stalking. Additionally, enterprises can leverage our scale to design personalized and subject-based cybersecurity educational programs for training and onboarding their employees.

Moreover, researchers may utilize SSBS to investigate how behavior intentions change among different cultures and languages (similar to Sharif et al. [55] for SeBIS), or over time with educational or motivational interventions. For instance, researchers who are interested in smartphone malware prevention may use SSBS to explore the effect of smartphone security behavior intentions to vulnerability exploits.

Role of SSBS in modeling Smartphone Security Behavior. Davis et al. [24] in their *Theory of Reasoned Action*, postulated that behavior intention is an antecedent to behavior. SSBS can thus add to the predictive value of a computational model of smartphone security behavior targeting early interventions that seek to prevent security breaches stemming from smartphone attack entry-points.

Theory of Reasoned Action. The Theory of Reasoned Action also posits that security behavior intention is a function of behavioral (attitudes) and normative beliefs. These beliefs influence intentions through attitudes and/or subjective norms. The *Theory of Planned Behavior* further argues that beliefs are not purely volitional but related to acquired resources and opportunities for performing the given behavior. Studies and ensuing causal models on what and to what extent factors (beliefs) affect smartphone security behavior intentions and behavior can further enhance an SSBS-based framework. Lastly, SSBS can contribute together with SEBIS [20] and SA-6 [22] into a more general framework modeling behavior

Table 3: Factor loadings and reliability statistics of finalized scale

ID	Item	Technical	Social	Inter-total correlation
T1	I reset my Advertising ID on my smartphone.	.787		0.52
T2	I hide device in my smartphone's bluetooth settings.	.639		0.47
T3	I change my passcode/PIN for my smartphone's screen lock at a regular basis.	.629		0.51
T4	I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).	.621		0.55
T5	I use an adblocker on my smartphone.	.614		0.51
T6	I use an anti-virus app.	.612		0.53
T7	I use a Virtual Private Network (VPN) app while connected to a public network.	.604		0.42
T8	I turn off WiFi on my smartphone when not actively using it.	.544		0.47
S1	I care about the source of the app when performing financial and/or shopping tasks on that app.		.723	0.24
S2	When downloading an app, I check that the app is from the official/expected source.		.677	0.36
S3	Before downloading a smartphone app I ensure the download is from official application stores.		.677	0.21
S4	I verify the recipient/sender before sharing text messages or other information using smartphone apps.		.609	0.41
S5	I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.		.552	0.25
S6	I pay attention to the pop-ups on my smartphone when connecting it to another device (e.g. laptop, desktop).		.526	0.39
2*	**Cronbach's alpha**	0.84	0.79	
	Inter-item correlation	0.40	0.39	

across different device types.

6.2 Limitations and Future Work

Scale Development Methodology. Our scale development process relies on security experts for generating the questionnaire items. There are other methods that can be used to incorporate expert opinions such as focus groups or Delphi studies [14]. Focus groups suffer from biases extending from individuals dominating the group opinion, which Delphi studies eliminate by collecting anonymized responses from experts through questionnaires, a process repeated for multiple rounds until consensus is reached. However, there is no element of discussion involved in Delphi, which runs the risk of vanishing opinion semantics. Additionally, the methodological process of a Delphi study is not well-established with numerous works illustrating Delphi variations with unclear reliability results. Instead, we adapted the same approach used by Egelman and Peer [20] and followed the 4-step scale development process proposed by Netemeyer et al. [47]. This approach has already been applied in the context of security behavior intentions to yield good reliability and predictive ability [19, 20].

Construct Validity. We performed established tests and demonstrated the reliability of SSBS and its goodness of fit with its two components. However, to better understand smartphone security behavior intentions, future work could further explore the convergence of SSBS with other related variables and its divergence from variables unrelated to security. We approached the problem primarily from a security standpoint, with privacy considerations only being secondary. More work is needed to understand socio-technical smartphone privacy behaviors.

Predicting Actual Behavior from Intentions. Lastly, intentions do not always result in behavior actions. The TRA and TPB theories come with limitations that SSBS inherits. For example, the TPB does not address the timeframe between a behavioral intention and an ensuing action and how this relationship can change over time. Moreover, the effects of other variables such as fear and threat of past experiences can further influence intentions. More work is needed to analyze how such factors influence the predictive power of SSBS. We plan to examine whether SSBS can predict relevant behavior actions and factors that affect that relationship in future work. Lastly, our findings indicate that a direct translation of SeBIS to the smartphone domain exhibits a poor goodness of fit. However, this should not be interpreted as SeBIS not being useful in measuring smartphone security intentions. In fact, Egelman, Harbach, and Peer found that SeBIS can predict smartphone secure screen locking behavior [19]. Our findings support the need for a new specialized measure if smartphone-specific wording is preferred or necessitated by the application context.

Comprehensiveness of Scale. While we followed an established psychometric process to operationalize smartphone security intentions, the comprehensiveness of the resulting scale should be further evaluated. This can be conducted through questionnaires with smartphone security experts to reveal whether the items can comprehensively cover the entire or a large portion of the spectrum of security behavior intentions. Such a study could reveal important items that have not been considered in our study.

Our paper also only focused on understanding the security facets of the smartphone; this work can be used as motivation for understanding privacy behavior. Lastly, studies with users could further establish user comprehension of the items' wording.

Demographic Characterization. Like the majority of psychometric measurements, SSBS is based on self-reports. To reduce potential social desirability bias, we took several precautionary procedures: being careful about wording questions in a non-judgmental way, making the surveys anonymous, and keeping the purpose of each survey vague. For data cleaning, we excluded unattended responses [53]. Moreover, our results

might not generalize since our sample is based entirely on US-based Amazon Mechanical Turk workers. Further studies are needed to support our findings across different cultures, languages, and social norms.

Average Variance Extracted(AVE). R^2 represents the proportion of variance in each item that is explained by the factor, and a desirable value for R^2 is at least 0.30. As shown in Table 2, the last technical item (T8) had a low R^2 value of 0.139, indicating that it did not capture the behavior well. This could be due to the users' uncertainty about how disconnecting from a WiFi network could enhance security, rather than using a VPN when connected to an insecure network. To calculate AVE, which is the average of R^2 values of items, a value of 0.50 or higher is recommended. If excluding T8 from the calculation, the AVE for Technical items was 0.401, which was slightly below the suggested threshold, while the AVE for Social items was 0.505, which met the criterion. The Technical scale has its merit and potential, as it is based on a rigorous literature review and empirical data collection, and it reflects some aspects of users' technical self-efficacy that are relevant for smartphone usable security behaviors. However, we also acknowledge the limitation of the low Technical AVE value and propose this as a challenge for future research in developing and validating a technical smartphone scale. We encourage future researchers to use our results as a reference point for addressing this limitation.

7 Conclusion

In this study, we found that smartphone security behavior differs from general security behavior. We thus carried out a series of factor analyses to create a Smartphone Security Behavior (Intentions) Scale (SSBS) with 14 questions that load onto two factors: technical (using technical strategies to protect smartphones) and social (being contextually cautious while using smartphones). Our scale exhibited satisfactory psychometric properties: the full scale and both the subscales have high internal consistency, all items map uniquely on one single component, and no correlation exists between the subscales. We established convergent validity between SSBS and an existent well-established security behavior measurement, SeBIS. These results support demonstrate SSBS can be a valuable specialized instrument in our arsenal for better understanding human smartphone security behavior, especially for security researchers and HCI designers that hope to preserve such cybersecurity becomes even more prevalent. Nevertheless, we recognize that the technical factor of the scale has a moderate fit and could be improved by further refinement. This is a limitation of our study that we plan to address in future work.

Acknowledgments

This work was supported in part by NSF CNS 19-55228 (SPLICE). The views expressed are those of the authors only.

References

[1] Icek Ajzen et al. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991.

[2] Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, and M Ali Babar. Security awareness of end-users of mobile health applications: an empirical study. In *MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 125–136, 2020.

[3] Mary J Allen and Wendy M Yen. *Introduction to measurement theory*. Waveland Press, 2001.

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796. ACM, 2015.

[5] Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. What the app is that? deception and countermeasures in the android user interface. In *2015 IEEE Symposium on Security and Privacy*, pages 931–948. IEEE, 2015.

[6] Andrew bunnie Huang. Betrusted: Improving security through physical partitioning. *IEEE Pervasive Computing*, 19(02):13–20, 2020.

[7] Bobby J Calder, Lynn W Phillips, and Alice M Tybout. The concept of external validity. *Journal of consumer research*, 9(3):240–244, 1982.

[8] Pew Research Center. Mobile fact sheet. https://www.pewinternet.org/fact-sheet/mobile/, June 2022.

[9] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security*, page 1. ACM, 2012.

[10] Ronald Jay Cohen and Mark E Swerdlik. *Psychological testing and assessment 6E*. New York: McGraw Hill, 2005.

[11] Ronald Jay Cohen, Mark E Swerdlik, and Suzanne M Phillips. *Psychological testing and assessment: An introduction to tests and measurement*. Mayfield Publishing Co, 1996.

[12] Jose M Cortina. What is coefficient alpha? an examination of theory and applications. *Journal of applied psychology*, 78(1):98, 1993.

[13] Lee J Cronbach. Coefficient alpha and the internal structure of tests. *psychometrika*, 16(3):297–334, 1951.

[14] Norman Dalkey and Olaf Helmer. An experimental application of the delphi method to the use of experts. *Management science*, 9(3):458–467, 1963.

[15] Amit Das and Habib Ullah Khan. Security behaviors of smartphone users. *Information & Computer Security*, 24(1):116–134, 2016.

[16] Jamie Davies. *Infographic: What do we actually use our smartphones for?*, July 2017. http://telecoms.com/483334/infographic-what-do-we-actually-use-our-smartphones-for.

[17] Fred D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[18] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. User acceptance of computer technology: A comparison of two theoretical models. *Management science*, 35(8):982–1003, 1989.

[19] Serge Egelman, Marian Harbach, and Eyal Peer. Behavior ever follows intention?: A validation of the security behavior intentions scale (sebis). In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 5257–5261. ACM, 2016.

[20] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2873–2882. ACM, 2015.

[21] Brian S Everitt and Anders Skrondal. *The Cambridge dictionary of statistics*. New York University, 2010.

[22] Cori Faklaris, Laura A Dabbish, and Jason I Hong. A self-report measure of end-user security attitudes (sa-6). In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[23] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*, page 3. ACM, 2012.

[24] Martin Fishbein. A theory of reasoned action: some applications and implications. 1979.

[25] Drew Fisher, Leah Dorner, and David Wagner. Short paper: location privacy: user behavior in the field. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, pages 51–56. ACM, 2012.

[26] Yanick Fratantonio, Chenxiong Qian, Simon P Chung, and Wenke Lee. Cloak and dagger: from two permissions to complete control of the ui feedback loop. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 1041–1057. IEEE, 2017.

[27] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. Users' expectations about and use of smartphone privacy and security settings. In *CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2022.

[28] Hugo Gascon, Sebastian Uellenbeck, Christopher Wolf, and Konrad Rieck. Continuous authentication on mobile devices by analysis of typing motion behavior. *Sicherheit 2014–Sicherheit, Schutz und Zuverlässigkeit*, 2014.

[29] Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. Gazeroomlock: Using gaze and head-pose to improve the usability and observation resistance of 3d passwords in virtual reality. In *International Conference on Augmented Reality, Virtual Reality and Computer Graphics*, pages 61–81. Springer, 2020.

[30] Joseph F Hair, William C Black, Barry J Babin, and Rolph E Anderson. *Multivariate data analysis: Pearson new international edition*. Pearson Higher Ed, 2013.

[31] Marian Harbach, Alexander De Luca, and Serge Egelman. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4806–4817. ACM, 2016.

[32] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 213–230, 2014.

[33] Li-tze Hu and Peter M Bentler. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1):1–55, 1999.

[34] Beth H Jones and Amita Goyal Chin. On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time. *International*

Journal of Information Management, 35(5):561–571, 2015.

[35] Joon-Myung Kang, Sin-seok Seo, and James Won-Ki Hong. Usage pattern analysis of smartphones. In *2011 13th Asia-Pacific Network Operations and Management Symposium*, pages 1–8. IEEE, 2011.

[36] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3393–3402. ACM, 2013.

[37] Murat Koyuncu and Tolga Pusatli. Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, 2019, 2019.

[38] Shakuntala P Kulkarni and Sachin Bojewar. Vulnerabilities of smart phones. *International Research Journal of Engineering and Technology*, 2(9):2422–2426, 2015.

[39] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. When csi meets public wifi: Inferring your mobile phone password via wifi signals. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1068–1079. ACM, 2016.

[40] Rui Li, Wenrui Diao, Zhou Li, Jianqi Du, and Shanqing Guo. Android custom permissions demystified: From privilege escalation to design shortcomings. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 70–86. IEEE, 2021.

[41] Huigang Liang and Yajiong Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7):394–413, 2010.

[42] Thomas J Madden, Pamela Scholder Ellen, and Icek Ajzen. A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin*, 18(1):3–9, 1992.

[43] Robert K McKinley, Terjinder Manku-Scott, Adrian M Hastings, David P French, and Richard Baker. Reliability and validity of a new measure of patient satisfaction with out of hours primary medical care in the united kingdom: development of a patient questionnaire. *Bmj*, 314(7075):193, 1997.

[44] Joel Michell. Is psychometrics pathological science? *Measurement*, 6(1-2):7–24, 2008.

[45] Kireet Muppavaram, Meda Sreenivasa Rao, Kaavya Rekanar, and R Sarath Babu. How safe is your mobile app? mobile app attacks and defense. In *Proceedings of the Second International Conference on Computational Intelligence and Informatics*, pages 199–207. Springer, 2018.

[46] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security*, 34:47–66, 2013.

[47] Richard G Netemeyer, William O Bearden, and Subhash Sharma. *Scaling procedures: Issues and applications*. Sage Publications, 2003.

[48] Jum C. Nunnally. *Psychometric theory / Jum C. Nunnally*. McGraw-Hill New York, 2d ed. edition, 1978.

[49] Jum C Nunnally and Ira Bernstein. *Psychometric theory 3E*. Tata McGraw-Hill Education, 1994.

[50] oberlo.com. How many people have smartphones in 2020?, 2020. https://www.oberlo.com/statistics/how-many-people-have-smartphones.

[51] Ralph L Piedmont. Inter-item correlations. *Encyclopedia of quality of life and well-being research*, pages 3303–3304, 2014.

[52] Gilles Raîche, Theodore A Walls, David Magis, Martin Riopel, and Jean-Guy Blais. Non-graphical solutions for cattell's scree test. *Methodology*, 2013.

[53] Elissa M Redmiles, Sean Kross, Alisha Pradhan, and Michelle L Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk and web panels to the us. Technical report, 2017.

[54] Gerard Saucier. Mini-markers: A brief version of goldberg's unipolar big-five markers. *Journal of personality assessment*, 63(3):506–516, 1994.

[55] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214. ACM, 2017.

[56] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. Can systems explain permissions better? understanding users' misperceptions under smartphone runtime permission model. In *USENIX Security Symposium*, pages 751–768, 2021.

[57] Sooel Son, Daehyeok Kim, and Vitaly Shmatikov. What mobile ads know about mobile users. In *NDSS*, 2016.

[58] Mohsen Tavakol and Reg Dennick. Making sense of cronbach's alpha. *International journal of medical education*, 2:53, 2011.

[59] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. "security begins at home": Determinants of home computer and mobile device security behavior. *computers & security*, 70:376–391, 2017.

[60] Güliz Seray Tuncay, Soteris Demetriou, Karan Ganju, and Carl A Gunter. Resolving the predicament of android custom permissions. In *Proceedings of Network and Distributed System Security (NDSS) Symposium*, 2018.

[61] Güliz Seray Tuncay, Jingyu Qian, and Carl A Gunter. See no evil: phishing for permissions with false transparency. In *Proceedings of the 29th USENIX Conference on Security Symposium*, pages 415–432, 2020.

[62] Silas Formunyuy Verkijika. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77:860–870, 2018.

[63] Jice Wang, Yue Xiao, Xueqiang Wang, Yuhong Nan, Luyi Xing, Xiaojing Liao, JinWei Dong, Nicolas Serrano, Haoran Lu, XiaoFeng Wang, et al. Understanding malicious cross-library data harvesting on android. In *USENIX Security Symposium*, pages 4133–4150, 2021.

[64] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. Android permissions remystified: A field study on contextual integrity. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 499–514, 2015.

[65] Luyi Xing, Xiaorui Pan, Rui Wang, Kan Yuan, and XiaoFeng Wang. Upgrading your android, elevating my malware: Privilege escalation through mobile os updating. In *2014 IEEE symposium on security and privacy*, pages 393–408. IEEE, 2014.

[66] Wu Zhou, Yajin Zhou, Xuxian Jiang, and Peng Ning. Detecting repackaged smartphone applications in third-party android marketplaces. In *Proceedings of the second ACM conference on Data and Application Security and Privacy*, pages 317–326. ACM, 2012.

Appendices

8 Translating SeBIS to the smartphone domain

Smartphone-SeBIS is based on the four dimensions of SeBIS: device securement, password management, proactive awareness, and update (Table 4). We generated items by revising SeBIS's through *word/phrase substitution*, *word/phrase revision*, *item deletion*, *item addition*. The resulting scale is depicted in Table 5.

9 Common Method Bias Test

To test if the Common Method Bias (CMB) (7)existed in the mode, we adopted the Harman Single Factor approach. We conducted exploratory factor analysis where all variables are loaded onto one factor. According to the result, the Harman Single Factor technique estimates the common method variance to be 26.85% which is below the commonly accepted threshold of 50%; this suggests that common method bias might not be a problem in the study.

Table 4: Items for the **original** Security Behavior Intentions Scale (SeBIS) and associated sub-scales.

Dimension	**Item**
Device Securement	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
	I use a password/passcode to unlock my laptop or tablet.
	I manually lock my computer screen when I step away from it.
	I use a PIN or passcode to unlock my mobile phone.
Password Generation	I do not change my passwords, unless I have to.
	I use different passwords for different accounts that I have.
	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
	I do not include special characters in my password if it's not required.
Proactive Awareness	When someone sends me a link, I open it without first verifying where it goes.
	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).
	When browsing websites, I mouseover links to see where they go, before clicking them.
	If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
Updating	When I'm prompted about a software update, I install it right away.
	I try to make sure that the programs I use are up-to-date.
	I verify that my anti-virus software has been regularly updating itself.

Table 5: Preliminary set of survey items developed based on SeBIS (*smartphone-SeBIS*)

Dim..	ID	Item	μ	σ
Device Securement	DS1	I use biometrics (fingerprint, face recognition) to unlock my smartphone.	2.41	1.6
	DS2	I enable encrypted storage on my smartphone.	2.41	1.44
	DS3	I use a rooted/jailbroken phone (r).	1.45	1.07
	DS4	I turn on the "lost my device" feature on my smartphone.	2.5	1.6
	DS5	I use a password/passcode to unlock my smartphone.	3.76	1.51
Password management	PM1	I regularly change my password for online services/accounts using my smartphone.	2.36	1.13
	PM2	I share my smartphone's passcode/PIN with other(s). (r)	1.51	0.99
	PM3	I use password manager app to manage my passwords on my smartphone.	1.88	1.31
Proactive awareness	PA1	When downloading an app, I check that the app is from the official/expected source.	3.95	0.99
	PA2	Before downloading a smartphone app I ensure the download is from official application stores (e.g. Apple App Store, GooglePlay, Amazon Appstore)	4.13	1.14
	PA3	I reset my Advertising ID on my smartphone.	1.6	1.02
	PA4	I manually revoke permissions from apps.	3	1.09
	PA5	I grant smartphone apps the permissions they request. (r)	3.2	0.85
	PA6	I disable geotagging of images captured by smartphone's camera app.	3.23	1.48
	PA7	I check which apps are running in the background.	3.33	1.14
	PA8	I check my smartphone's privacy settings.	3.31	1.17
	PA9	When receiving a link from an unknown source via SMS, I click the link immediately. (r)	1.67	1.04
Update	UP1	When I'm prompted about a software update on my smartphone, I install it right away.	3.3	1.13
	UP2	I make sure that the smartphone applications I use are up-to-date.	3.61	0.92

Table 6: Developed smartphone security behavior measurement

Research	Smartphone Security Behavior Measurement	Scale
Das and Khan [2016]	1. I lock my smartphone with a PIN or password. 2. I update my software when new versions are released. 3. I have installed a mobile anti-virus program. 4. I encrypt confidential information (e.g., passwords, bank details, . . .) on my smartphone. 5. I avoid storing confidential information (e.g., passwords, bank details, . . .) on my smartphone. 6. I review security features of apps before installing them on my smartphone.	6-point scale
Jones and Chin [2015]	1. Have you set the idle timeout (so that the screen goes dark) to a shorter time than the factor default? 2. To wake up after idle, is a password or other code required on your smartphone? 3. Do you disable Bluetooth when it's not in use? 4. Do you disable GPS (navigation) when you are not using it? 5. When you use your phone to connect to Wi-Fi wireless networks, do you only connect to encrypted password-protected networks? 6. Select one answer regarding anti0virus software: "Anti-virus software has been downloaded and installed on my phone and I use it. . . " 7. Select one answer regarding encryption software: "Encryption software has been downloaded and installed on my phone and I use it. . . "	5-point categorial scale (Frequently, Sometimes, Rarely/Never, Software not installed, Don't know)
Thompson et al. [2017]	1. I have installed security software on my device 2. I have recent backups of my device 3. I have enabled automatic updating of my computer software 4. I use security software (anti-virus/anti malware) 5. My device is secured by a password.	7-point Likert scale (Strongly Disagree-Strongly Agree)
Verkijika [2018]	1. I have installed security software on my device 2. I have recent backups of my device 3. I have enabled automatic updating of my computer software 4. I regularly use security software (anti-virus/anti malware) on my smartphone. 5. My smartphone is secured by a password or another authentication method (e.g., fingerprint).	5-point Likert scale (Strongly Disagree-Strongly Agree)

Table 7: Common Method Bias Test

Dimensions	Eigenvalue	Proportion (%)	Cumulative (%)
1	3.759	26.851	26.851
2	3.348	23.916	50.767
3	1.046	7.471	58.238
4	0.812	5.805	64.044
5	0.716	5.114	69.158
6	0.628	4.489	73.648
7	0.592	4.235	77.883
8	0.568	4.061	81.945
9	0.532	3.801	85.745
10	0.483	3.451	89.197
11	0.443	3.169	92.367
12	0.386	2.759	95.127
13	0.358	2.557	97.684
14	0.324	2.315	100.000

Table 8: Correlation between SSBS Technical (**T**) and Social (**S**) Scales

	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**
T1	1.000	.455	.594	.401	.327	.339	.460	.270	-.196	-.108	-.159	-.047	-.065	-.002
T2		1.000	.486	.405	.342	.286	.401	.344	.009	.024	.007	.118	.083	.112
T3			1.000	.484	.393	.432	.445	.282	-.017	.018	-.011	.106	.036	.102
T4				1.000	.302	.363	.282	.239	.004	.078	.062	.100	.141	.103
T5					1.000	.472	.352	.098	.045	.029	.001	.119	.066	.002
T6						1.000	.243	.169	.017	.043	.020	.120	.141	.029
T7							1.000	.199	-.033	.087	.033	.051	.037	.072
T8								1.000	.009	.053	.053	.083	.041	.122
S1									1.000	.612	.616	.473	.537	.420
S2										1.000	.629	.498	.515	.444
S3											1.000	.545	.484	.475
S4												1.000	.423	.401
S5													1.000	.381
S6														1.000

Table 9: List of Original Items of smartphone security behaviors generated by security professionals

ID	Item	μ	σ
A1	I turn off WiFi on my smartphone when not actively using it.	2.88	1.38
A2	I perform banking transactions/operations on my smartphone while connected to a public network.	3.62	1.35
A3	I connect to public WiFi using my smartphone.	2.92	1.78
A4	I use a Virtual Private Network (VPN) app while connected to a public network.	2.43	1.38
A5	When downloading an app, I check that the app is from the official/expected source.	3.92	1.07
A6	Before downloading a smartphone app I ensure the download is from official application stores (e.g. Apple App Store, GooglePlay, Amazon Appstore)	4.04	1.08
A7	I manually revoke permissions from apps.	3.15	1.11
A8	I grant smartphone apps the permissions they request.	2.56	0.89
A9	I disable geotagging of images captured by smartphone's camera app.	3.17	1.39
A10	I check which apps are running in the background.	3.59	1
A11	I delete apps I don't frequently use.	3.88	0.97
A12	I enable two-step authentication when offered by an app.	3.45	1.15
A13	I reset my Advertising ID on my smartphone.	2.32	1.36
A14	I check my smartphone's privacy settings.	3.5	1.06
A15	I turn off location services on my smartphone when I am not actively using them	3.41	1.28
A16	I turn off bluetooth (NFC, wifi) on my smartphone when I am not actively using it	3.67	1.32
A17	I use an anti-virus app	2.72	1.53
A18	I store proprietary business information on my smartphone.	3.7	1.33
A19	I store personal health information on my smartphone.	3.52	1.39
A20	I verify the recipient/sender before sharing text messages or other information using smartphone apps	3.71	1.14
A21	I use an adblocker on my smartphone.	2.84	1.48
A22	I pay attention to the pop-ups on my smartphone when connecting it to another device (e.g. laptop, desktop).	3.83	1.07
A23	I care about the source of the app when performing financial and/or shopping tasks on that app	4.05	0.98
A24	I back-up my smartphone's contacts, photos and videos on another device/cloud	3.44	1.23
A25	I delete any online communications (i.e., texts, emails, social media posts) that look suspicious	3.92	1.11
A26	I get permissions from my friends before sharing them on a photo or video online	3.48	1.24
A27	I check the latest news updates regarding my smartphone and apps	3.36	1.09
A28	I use private browsing on my smartphone.	3.06	1.16
A29	I use biometrics (fingerprint, face recognition) to unlock my smartphone.	3.07	1.61
A30	I enable encrypted storage (or phone memory) on my smartphone.	2.87	1.48
A31	I use a rooted/jailbroken phone.	1.97	1.35
A32	I turn on the "lost my device" feature on my smartphone.	2.89	1.53
A33	I use a password/passcode to unlock my smartphone.	3.87	1.27
A34	I hide device in my smartphone's bluetooth settings.	2.63	1.43
A35	I use a privacy screen on my smartphone	2.58	1.51
A36	I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).	2.89	1.25
A37	I change my password for online services/accounts using my smartphone.	2.89	1.24
A38	I share my smartphone's passcode/PIN with other(s).	4	1.27
A39	I use password manager app to manage my passwords on my smartphone.	2.55	1.48
A40	I store passwords and usernames on my smartphone.	3.32	1.41
A41	I change my passcode/PIN for my smartphone's screen lock at a regular basis.	2.7	1.31
A42	I use different passwords for different accounts that I have on my smartphone.	3.68	1.14
A43	When I'm prompted about a software update on my smartphone, I install it as soon as I can	3.53	1.09
A44	I make sure that the programs smartphone applications I use are up-to-date.	3.79	1.05
A45	Before downloading a smartphone app I read its privacy policy to ensure my information is handled securely	2.96	1.33