Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates

Arunesh Mathur
University of Maryland
College Park, MD
amathur@umd.edu

Marshini Chetty
Princeton University
Princeton, NJ
marshini@princeton.edu

ABSTRACT

To keep mobile devices secure, experts recommend turning on auto-updates for applications, but recent research has suggested that users often avoid auto-updating because updates can lead to undesirable consequences such as user interface changes or compatibility issues. Understanding whether there are commonalities amongst users who avoid auto-updates can help us create better mobile application updating interfaces. However, little is known about how users' characteristics associate with their attitudes towards auto-updating their mobile applications, or how we can leverage these characteristics to encourage users to auto-update these applications to improve security. In this paper, by surveying Android users, we establish how users' past experiences with software updating, and users' psychometric traits differentiate those users who avoid application auto-updates from those who do them, as well as users' preferences towards auto-updating their applications. Our findings reveal that users who avoid application auto-updates are more likely to have had past negative experiences with software updating, tend to take fewer risks, and display greater proactive security awareness. Users' perceived level of trust with mobile applications also determined how comfortable they are auto-updating these applications. Based on these findings, we recommend how Android can improve the design of application update systems to encourage users to auto-update and keep their devices secure.

1. INTRODUCTION

Keeping mobile applications and platforms updated is important since these devices store sensitive data from or about users and software updates can prevent security exploits from known vulnerabilities. For instance, in 2015 alone, Symantec reported 528 new mobile vulnerabilities [1], up 214% from 2014. Furthermore, recent research has shown that mobile users are slow to apply updates: only 32% users auto-updated their applications and only 16% applied updates manually as soon as updates were released [2], and only half of all users update to a new application version within the first week after the update's release [3]. Additionally, on the Android Operating System (OS)—the mobile OS with the largest market share of mobile phones worldwide [4]—studies [5, 6] have reported multiple Secure Sockets Layer (SSL) and OpenSSL Heartbleed bug [7] vulnerabilities which could have been fixed by promptly applying application updates. For this reason, various companies [8, 1], academics [9], and even the United States-Computer Emergency Readiness Team [10] suggest that developers deploy, and users turn on automatic updates—updates that are downloaded and installed without human intervention—to ensure that their systems remain secure. Automated updates have also been shown to be effective, more so than requiring users to manually update their devices [9, 11].

However, recent research has suggested that users often turn off automatic updates since updates can disrupt settings, cause unnecessary reboots, compatibility issues, or change the user interface [12, 13]. Yet we know little about whether there are commonalities amongst those users who avoid auto-updates versus those who do auto-update, despite knowing that user characteristics can influence computer security attitudes and behaviors [14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24]. To address this gap in the literature and determine if we can leverage user characteristics and auto-updating preferences to encourage more users to auto-update their mobile applications, we posed two research questions. First, we asked whether there are underlying user characteristics that differentiate users who avoid auto-updating from those who auto-update their Android applications based on their current auto-update settings. Second, we asked how these user characteristics, including users' attitudes towards their Android applications explain users' preferences indicating whether they would like auto-updating to vary across their applications. Our goal is to inform the design of enhanced mobile application systems that increase user uptake of auto-updates on mobile devices to improve mobile security.

To answer these questions, we conducted a survey with 477 Android users on Amazon Mechanical Turk in the United States (US). Specifically, we considered how users' past experiences with software updating, users' psychometric traits—including their risk taking capacities, consideration for future consequences, propensity to engage in cognitive endeavors, and resistance to change—differentiate how users currently auto-update their Android applications. Next, we investigated how these user characteristics, including users' attitudes towards their Android applications—such as how much they trust an application—explain how comfortable users

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

are auto-updating updates across their different applications, that is, their auto-updating preferences.

In a new contribution, our results show that users who avoid auto-updating their applications on Android differ from those who auto-update in three ways:

1. First, we found a large effect indicating that users who avoid auto-updating have had previous negative experiences with updating their software—confirming the findings from previous interview studies about desktop users [12, 13]. However, unlike prior work, our findings suggest users' past negative experiences with updates may not necessarily have been on their Android devices.

2. Second, we found a medium effect indicating that users who avoid auto-updating also tend to take fewer financial investment risks. For instance, these users were less likely to invest their money in business ventures and mutual funds. In addition, we found a medium effect indicating that users who avoid auto-updating also tend to fewer ethical risks. For instance, these users were less likely to take questionable deductions on their income task returns (to receive greater returns).

3. Third, we found a small effect indicating that users who avoid auto-updating also exhibit a greater propensity to take proactive steps to maintain their online security—similar to what others have found for users who avoid auto-updating on desktops [13]. For instance, these users were more likely to verify the green HTTPS lock on websites, and verify links before clicking them.

Finally, we discovered medium effects indicating that users were less comfortable auto-updating across their Android applications if they had a previous negative experiences with software updating, whereas users were more comfortable auto-updating across their Android applications for security updates and when they perceived an application as trustworthy—similar to what others studies have reported for desktop users [25].

Based on our findings, we make four primary recommendations to improve the design of mobile application updates on Android to encourage users to auto-update. First, we suggest that an improvement to the current Android OS would be to provide users with a more accessible mechanism to rollback application updates to a prior point in time to encourage users to be more risk taking with respect to turning on auto-updates. Second, we suggest leveraging the characteristics we identified of users who avoid auto-updating, including their risk averse nature, to design nudges and messages to encourage users into auto-updating security updates. Third, we suggest that the security community study the practices of software developers, how they develop and build updates, and how these practices lead to negative experiences for end-users. Finally, we suggest that an improved Android application interface for updates could be personalized by inferring users' attitudes towards their Android applications and preferences for auto-updating those applications using our work as a starting point. Doing so, may encourage more users to auto-update their mobile applications, which in-turn will ultimately affect the security of their mobile devices. In the remainder of this paper, we discuss related work, our methods and study, our findings, discussion, and conclusions for improving mobile software update interfaces.

2. BACKGROUND AND RELATED WORK

In this section, we highlight previous research related to software updates, and place our research in context.

2.1 User Characteristics and Security

Multiple studies have investigated how users' individual differences affect their security attitudes and behaviors. One such line of work [21, 22, 23, 24] examined how demographics and users' level of technical expertise impact security decisions. For instance, Jeske *et al.* [21] suggested that the manner in which users select a wireless network may be affected by individual differences in users. These authors designed and evaluated user interfaces in a 67 participant study showing how certain interface elements (e.g., color and ordering) can be utilized to help users with low technical expertise select secure networks. Another set of researchers [24] examined the characteristics of users who succumb to phishing attacks, and found that younger users and women were more susceptible than other users. These researchers designed and evaluated educational material to help these users stay protected against phishing attacks. In another study of targeted security solutions, Garg *et al.* [22] found that using video to communicate malware and phishing threats improved older adults' ability to understand security risks with these two threats.

Another line of work [14, 15, 16, 17, 18, 19, 20] examined how differences in users' beliefs, mental models and decision making capacities impact security attitudes and behaviors. Wash [14] uncovered how users' mental models and beliefs about computer security influence the actions they take to protect themselves across two folk models of threats: hackers and viruses. The author suggested that due to the variance in users' beliefs about security threats, one-size-fits-all security interfaces such as warnings and notifications may be less impactful than those that are specifically targeted at users' beliefs. Whitty *et al.* [15] found that older people and people who self-regulated their actions and behavior—as measured by the self-monitoring personality trait—were more likely to share their passwords with others. In related work, Egelman and Peer developed [16] and validated [26] the Security Behavior Intentions Scale (SeBIS) to measure behavior intentions, and with their data, demonstrated [17] that these behavior intentions are associated with users' psychometric traits, including capacity to take risks, being inherently curious and inquisitive, and thinking about long-term implications of actions. For instance, the authors discovered that those users who take fewer risks also tend to keep their software updated to prevent potential harm from exploits. The authors suggested that segmenting users by these traits may allow designers to infer users' security intentions, and use them to tailor computer security user interfaces to help users remain secure. Similarly, in another study, Malkin *et al.* [20] developed and tested browser SSL warnings tailored to users' decision making capabilities, and found several correlations between the framing of the warnings and users' decision making capabilities. Related studies have also shown that users who take fewer risks were also less likely to plug in potentially harmful USB drives [19] and more likely to keep their systems secure [18]. Our study builds upon both lines of work on linking users' past software update experiences, their psychometric traits, and their security behavior (which is driven by underlying beliefs about security) to attitudes towards automatic application updates.

2.2 Software Updates

2.2.1 User Issues Around Software Updates

There is a growing body of work that examines in detail users' attitudes and interactions with software updates but most of this work focuses on the desktop experience of updates. One set of studies has examined how users manage their computer security, perceive software updates, and software updating behaviors. For example, Ion *et al.* [27] compared the security advice expert and non-expert users gave to others to stay secure, and found that non-experts lacked awareness about the benefits of software updates and used their judgements to avoid updates that they felt introduced bugs. Furthermore, they found that 39% of experts reported auto-updating compared to 29% of non-expert users. In another US national representative survey [28], researchers found that a large fraction of their sample updated their software with 39% reporting they update their software immediately and 41% reporting that they update their software sometime after an update is released, and only 5% reported rarely or never updating their software.

Several studies have indicated that negative experiences—such as user interface changes or compatibility issues with software—either cause users to avoid or delay software updates [25, 12, 29, 13] on desktop machines. In some cases, users avoid desktop updates because they find software updates messages confusing and unclear [30]. In other cases, studies [31, 32] show that users often delay and only perform updates on Wi-Fi networks if they have access to limited and expensive Internet data plans on both desktop and mobile.

There are at least three studies of mobile updating behaviors, specifically on the Android OS. Moller *et al.* [33] and Oltrogge *et al.* [3] found that half of the users they studied would still use a vulnerable application on their phones even seven days after the release of the update that fixed that vulnerability. Tian *et al.* [34] developed a novel updating notification that used user generated reviews to help mobile users make privacy conscious decisions about which updates to apply based on what permissions were asked for by the updates. Collectively, all of these studies illuminate that users lack awareness about the security benefits of software updates, and that users often delay or avoid updates. However, unlike our work, these studies do not focus specifically on mobile users' automatic update experiences or link auto-updating attitudes and preferences with user characteristics.

2.2.2 Automatic Software Updating

Several studies have shown that auto-updating is extremely effective at keeping users up to date with the latest security patches. For instance, Gkantsidis *et al.* [35] analyzed software update data from close to 300 million Microsoft Windows computers and discovered that more than 90% of all machines which had automatic updates enabled had security patches applied. Similarly, Duebendorfer and Frei *et al.* [11] collected log and update data from various Web browsers including Google Chrome, Mozilla Firefox, and Apple Safari. They found that compared to all other browsers, Google Chrome's silent update mechanism, a form of automatic updates that requires no user notification, had the most efficient patching rate: within three weeks, 97% of all active users were up-to-date on the latest version, unlike browsers with other update mechanisms such as Mozilla Firefox and Apple Safari. One other study of nearly 8.4 million hosts [9] also demonstrated that applications with auto-updating mechanisms such as Chrome reached 50% and 90% patch deployment coverage significantly faster than those that did not, such as Wireshark.

Another set of studies touches more on user experiences with automatic updates. Two studies about desktop users revealed that automatic updates can lead to varying user experiences. First, this research discovered that because automatic updates do not include users in the decision making process, users develop poor mental models of how updates on their system work [36]. As a result of these poor mental models, the authors argue that users fail to troubleshoot and manage these updates, which adversely affects the security of their systems [37]. Second, in another study, researchers found that users who desire control and make active choices in computer security and maintenance tasks turned off automatic updates, and used their own judgement to decide which updates to apply—but were sometimes less secure than those who kept auto-updating on [13]. Finally, Mathur *et al.* [25] designed a novel interface to support silent updates and found that users varied in their preferences to let applications auto-update with some preferring the convenience of auto-updates and others disliking the lack of control over what changes updates make to their systems.

While these studies collectively suggest that automatic updates are indeed effective to patch systems, users are still impacted when applications and devices auto-update. These studies also highlight several qualitative user experiences around auto-updates on desktops, but they offer no such insights into mobile users' attitudes towards auto-updating. Our study makes the following contributions to the body of work on users and updates: we provide evidence of differences between users who avoid and who do auto-update their applications on mobile devices, we show what factors explain user preferences for mobile application auto-updates, and we make recommendations for leveraging this information to design better mobile update interfaces to increase the chance of users' auto-updating to remain secure.

2.3 Android Application Updates

Given that it has the large market share of all OSes that run on mobile devices [4], we decided to study application software updating on the Android OS. Android users rely on the Google Play Store to download and update applications on their phone [38]. The Play Store contains settings that allow users to control how they receive updates to their applications. As shown in Figure 1, these settings are:

1. **Do not auto-update apps:** Applications are not auto-updated, and users receive notifications each time updates become available for their applications.
2. **Auto-update apps at any time. Data charges may apply:** Applications are auto-updated without user consent regardless of whether the user is on Wi-Fi or on mobile data.
3. **Auto-update apps over Wi-Fi only:** Applications are auto-updated without user consent but on Wi-Fi only to prevent excessive data charges.

By default, the Android OS ships with "Auto-update apps over Wi-Fi only" option enabled. In addition to these op-

tions, Android allows users to disallow auto-updating certain applications even in auto-update mode in case they wish to provide consent to updating these applications. For instance, if users wish to provide consent to update the Google Chrome application, they can retain the default auto-update setting but disable auto-updating specifically for Google Chrome. Users can also roll back application updates for certain applications and not for others. Specifically, applications that come pre-installed with the device can be rolled back only to their initial version from within the Android OS *Settings* menu [39], whereas applications downloaded from the Play Store cannot be rolled back at all.

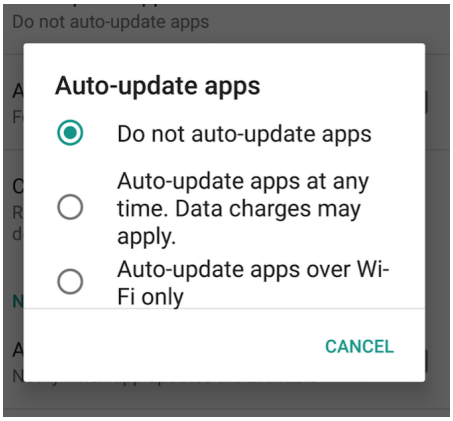


Figure 1: The Application Update Options Available in the Google Play Store on the Android OS.

If Android users disable auto-updating their applications, they see an update notification indicating the applications with available updates. Upon clicking the notification, users interact with a list of applications requiring updates. Users also see a notification—indicating the updated applications—after applications have been updated, independent of the update mechanism. All of these notifications can be activated or deactivated from the Play Store. Updates that require additional permissions for an application cannot be automated to prevent malicious applications from acquiring device permissions. However, since the introduction of Android 6.0, permissions are requested at run-time [40].

3. RESEARCH QUESTIONS

In order to design and develop better user interfaces and systems that encourage users to auto-update, we need to answer two questions. First, we need to identify what differences exist between the characteristics of those users who currently avoid auto-updating and those users who currently auto-update their mobile applications. Identifying these differences can help inform how the user interfaces of mobile devices can be improved to better incorporate these differences. Second, we need to identify—regardless of whether users currently auto-update—how these characteristics explain users' preferences indicating whether they would like auto-updating across their different applications. Establishing which factors explain these preferences can further help us identify how auto-update systems can incorporate these preferences into their design. In this section, we describe these research questions in further detail.

3.1 How are Users Who Avoid Auto-updating Different From Those Who Auto-update?

Our first research question investigated how various user characteristics differentiate those Android users who avoid auto-updating their applications from those who auto-update their applications (retaining the default option to auto-update applications in the Play Store). Previous interview-based studies have suggested that past negative experiences with software updating—such as surprise user interface changes or compatibility issues—can affect users' auto-updating behavior [12, 13] and their attitudes towards future updates [29]. Based on this observation, we formulated our first hypothesis:

• **H1**: Avoiding auto-updates will likely be associated with users who have had negative experiences with updating their software.

Previous research [17, 16] into users' psychometric traits—including risk taking capacities, consideration for future consequences, propensity to engage in cognitive endeavors—and cybersecurity behaviors has shown that they correlate with how often users' take actions and make decisions towards keeping their software updated. Unlike when users are asked to provide consent to updating each time an update is available, auto-updating is a one-time decision users make to allow their system to update itself and does not require continual consent. However because auto-updates are installed without users' consent, they may cause undesired consequences, and are likely to be avoided by those who take fewer risks. Based on this, we formulated our second hypothesis:

• **H2**: Avoiding auto-updates will likely be associated with lower risk taking behavior.

Next, leaving auto-updates on has the potential to cause undesired consequences to systems in the long-term, and are therefore likely to be avoided by those who consider the future consequences of their actions. This allowed us to formulate our third hypothesis:

• **H3**: Avoiding auto-updates will likely be associated with a higher consideration of future consequences.

When updates are automatically installed, users only grasp the changes made by the update after the update has been installed. Therefore, it is likely that those who avoid auto-updates also have a greater propensity to keep appraised of the changes updates make. This led to our fourth hypothesis:

• **H4**: Avoiding auto-updates will likely be associated with higher curiosity and inquisitiveness.

Finally, because auto-updating applies updates as soon as the updates become available and updates have the potential to bring about undesired changes and consequences, users who avoid auto-updating may also exhibit a greater resistance to change. This led to our fifth and final hypothesis:

• **H5**: Avoiding auto-updates will likely be associated with a greater resistance to change.

3.2 How Do User Characteristics Explain Users' Auto-updating Preferences?

Our second research question explored how user characteristics explain Android users' preferences towards auto-updating their mobile applications. Previous research [25] with desktop users has suggested that users vary in their preferences

towards auto-updating their applications, and that they consider a variety of factors towards deciding which application to auto-update. The study suggested that users are more comfortable auto-updating security updates compared to non-security updates and applications they trust, and that they are less comfortable auto-updating applications that are important to them, applications they use frequently, and applications they are satisfied with. While we do not claim that these are the only characteristics Android users consider, we investigate how each of they factors correlate with users' auto-updating preferences across their applications in the mobile space. Therefore, to answer our second research question, we first considered how comfortable would users be auto-updating each application if they were given the choice to selectively auto-update their applications. Following that, we investigated how users' past negative experiences with software updating, users' psychometric traits, and users' attitudes towards auto-updating their Android applications explain these preferences.

4. METHOD

To answer our research questions we conducted a survey of Android users on Amazon Mechanical Turk (AMT) between April and May 2016. In total, the survey took took approximately 15 minutes to complete. We hosted the survey on SurveyGizmo[1], and advertised it as an "Android Apps Update Survey" task on AMT. Turkers were invited to participate if they were 18 or older, their primary smartphone was an Android phone, and if they had previously used the Play Store for at least one month. We used these filters to ensure participants were familiar with the Android OS and how applications are installed and updated. To ensure response quality, we restricted the task to Turkers based in the US who had an approval rating of 95% or higher. Because we did not filter Turkers based on the number of tasks previously completed, we added three attention check questions to the survey—based on the findings of Peer *et al.* [41]—one of which specifically asked about the Android OS. We filtered all responses that failed any of the attention check questions, and compensated the Turkers with $2.50 for completing the survey. The study was approved by the Institutional Review Board of our university.

4.1 Survey Instrument

The survey instrument contained three sections in total—all of which are described below—and is available in the Appendix.

4.1.1 Section One: Psychometric Scales

To answer our first research question, investigating what differentiates those who avoid auto-updates for their applications from the other users, we employed a psychometric scale to measure the corresponding psychometric trait for each hypotheses listed in Section 3. The statements of each scale and the order of the scales themselves were randomized to avoid any bias, and therefore each scale appeared in a page by itself in the survey. Specifically, we used the following psychometric scales, which have been used by Egelman and Peer [16, 17] and other studies in the past [18, 19, 24]:

Risk Taking: For hypothesis **H2**, we employed the Domain Specific Risk Taking scale (DoSpeRT) [42] to measure people's risk taking propensity. The DoSpeRT scale measures risk taking across the following dimensions: Ethical (e.g., passing off somebody else's work as your own), Financial/Investment (e.g., investing 10% of your annual income in a moderate growth mutual fund), Financial/Gambling (e.g., betting a day's income at the horse races), Social (e.g., admitting that your tastes are different from those of a friend), Recreational (e.g., bungee jumping off a tall bridge), and Health & Safety (e.g., engaging in unprotected sex). The score for each sub-scale lies between 1 (Extremely Unlikely) and 7 (Extremely Likely).

Future Consequences: For hypothesis **H3**, we employed the Consideration for Future Consequences scale (CFC) [43], which measures how much people consider the long-term consequences of their actions and decisions (e.g., my behavior is generally influenced by future consequences). The score for this scale lies between 1 (Extremely Uncharacteristic of Me) and 7 (Extremely Characteristic of Me).

Cognitive Endeavors: For hypothesis **H4**, we employed the Need for Cognition scale (NFC) [44], which measures how much people consider and indulge in thought and curiosity provoking endeavors (e.g., when I make a decision, I think about how it might affect me in the future). The score for this scale lies between 1 (Extremely Uncharacteristic of Me) and 5 (Extremely Characteristic of Me).

Resistance to Change: For hypothesis **H5**, we employed the Resistance to Change scale (RTC) [45], which measures how averse users are to change across the following dimensions: Short-term Focus (the extent to which individuals are distracted by the short-term inconveniences associated with change; e.g., often, I feel a bit uncomfortable even about changes that may potentially improve my life), Emotional Reaction (the amount of stress and uneasiness induced by change; e.g., when I am informed of a change of plans, I tense up a bit), Routine Seeking (inclination to adopt routines; e.g., whenever my life forms a stable routine, I look for ways to change it), and Cognitive Rigidity (frequency and ease with which individuals change their minds; e.g., my views are very consistent over time). The score for each sub-scale lies between 1 (Strongly Disagree) and 6 (Strongly Agree).

In addition, we also included the SeBIS scale to determine whether users who avoid auto-updating and do auto-update their applications differed in their security behavior intentions. That is, we wanted to determine if applying auto-updates is associated with a tendency to indulge in "good" security behaviors? We did so to determine whether users who intend to behave securely also consider auto-updating a "good" security practice. The SeBIS scale measures users' security behavior intentions across four dimensions: Password Generation (do users create strong passwords?; e.g., when I create a new online account, I try to use a password that goes beyond the site's minimum requirements), Proactive Awareness (do users take proactive steps towards their security?; e.g., when browsing websites, I mouseover links to see where they go, before clicking them), Device Updating (do users update their software and devices regularly?; e.g., when I'm prompted about a software update, I install it right away), and Device Securement (do users protect their devices with passwords and pins?; e.g., I use a PIN or passcode to unlock my mobile phone). The score for each sub-scale lies between 1 (Never) and 5 (Always).

[1]http://surveygizmo.com

4.1.2 Section Two: Android Application Update Settings and Auto-Update Preferences

Section Two of the survey collected data about participants' mobile application update settings and their preferences towards auto-updating their applications on Android. To understand how users currently auto-update their applications, we collected users' Android application update settings—as described in Section 2.3—in the Play Store. Rather than asking participants directly about whether they auto-updated applications on their devices, we elicited their auto-update settings in the Play Store using detailed labelled instructions to increase the validity of the self-reported data. More specifically, we asked users to report two settings: the first question asked participants to report their application update settings from the Play Store—one of the options in Figure 1—and the second question followed up with an image displaying how an application could be disallowed from auto-updating, asking participants if they ever disallowed auto-updates for any application. The second question appeared only if participants reported auto-updating in the first question.

To answer our second research question and elicit users' auto-updating preferences for mobile applications, we asked the participants to select the applications installed on their phones from a visual grid containing the most installed Android applications of all time [46]—all 95 of them—since more users are likely to encounter these applications. To eliminate any biases, the order of the applications in the grid was randomized for each participant. For each application, participants then rated their level of comfort with automating security and non-security updates (UpdateType)—assuming no data charges applied—on a scale of Uncomfortable (0) to Comfortable (100) using visual slider. Participants then answered, for each application, how trustworthy they felt the application was (Trust), how important the application was to them (Importance), how frequently they used the application (Use Frequency), and how satisfied they were with the application (Satisfied)—all on a scale of 1 (Lowest) to 5 (Highest). To limit the number of applications participants answered these questions about and prevent fatigue, we randomly drew a maximum of 10 applications from the ones participants reported they had on their phone. We designed the survey to elicit preferences in this manner—for each application—to gather how participants varied in their responses. To prevent ordering bias, we randomized how participants observed Sections One and Two of the survey.

4.1.3 Section Three: Past Update Experiences

Finally, in Section Three of the survey, we asked participants whether they had previously had a negative experience with software updates i.e., if they had regretted updating any device or software—not just their mobile devices. If participants answered "Yes", we listed the common negative experiences users reported with software updating from the literature at the time [13, 29, 25] for participants to select or to enter their own experiences. This section of the survey always appeared right before the end of the survey—to avoid any priming effects of asking participants to report their preferences towards auto-updating in Section Two. The survey ended with demographic questions asking about age, gender, income and occupation.

4.2 Survey Pilot and Deployment

After constructing the survey, we piloted it with a six participant convenience sample drawn from within our institution. During the pilot, we employed cognitive interviews [47], a commonly used technique in survey research, where participants are asked to "think-aloud" when attempting the survey questions. These are conducted to ensure the survey questions convey their intended meanings and measure the construct the researcher intends to measure. During the interviews, participants were asked to describe, in their own words, what the purpose of each question was, and whether they experienced any difficulty in answering them; we also specifically focused on the instructions to report the auto-update settings to ensure they were easy to follow through. Subsequently, we used these results to refine and revise a few questions. These interviews lasted for about 30 minutes. Participants were not reimbursed for their time.

4.3 Limitations of Self-Reported Data

We asked participants to self-report their Android application update settings in the survey, and therefore this data on settings could be subject to error. To limit this error, we asked participants to follow a set of well-labelled instructions to find and report the current settings on their phones instead of asking them directly about how they updated their applications. However, it is still possible that participants may have responded by recollecting or guessing their update settings as opposed to actually checking their devices. We did consider asking participants to upload a screenshot of the update settings page from the Google Play Store application but we chose not to do so since this would require participants to upload a screenshot from their mobile device to the device they were using to taking the survey, which may have been different. This additional step would have been prohibitively time consuming and cumbersome, and likely to have introduced a bias of its own. Future research could identify ways to collect this information directly from users' devices to increase the accuracy of the settings data.

4.4 Participants

The survey received 525 responses in total from AMT, out of which 48 responses (9.1%) failed at least one attention check question and were subsequently discarded, leaving 477 valid responses. Table 1 summarizes the survey participants' demographics. The survey participants were predominantly between 18–34 years old, with more males than females (62.3% vs 37.1% respectively). Nearly 90% of the survey participants had either a college or bachelor's degree, and earned a median annual income between $35,000 and $49,999. 33% of the survey participants reported that they avoided auto-updating their applications, i.e., they chose the "Do not auto-update apps" option described in Section 2.3 in the Play Store. Only close to 10% of the participants reported that they restricted auto-updating for at least one application using the feature described in Section 2.3.

4.5 Data Analysis

4.5.1 Reliability and Dimensionality of the Scales

Before proceeding towards building statistical models for our data, we analyzed all the psychometric data in terms of *Reliability* and *Dimensionality* [48]. Both these techniques are used in developing and constructing scales, but are also used to evaluate data that results from using scales in order to confirm the gathered data's validity. A scale's *Dimensionality* measures the number of underlying factors it measures

Demographic	Survey Participants
Age	
18–34	69.2%
35–54	28.9%
>55	1.9%
Gender	
Male	62.3%
Female	37.1%
Other	0.6%
Education	
Some College	45.4%
Bachelor's	45.6%
Master's	8.4%
Other	0.6%

Table 1: Demographic Information of the Participants.

(one, for uni-dimensional, or many, for multi-dimensional scales) and the nature of these factors (correlated or uncorrelated). In our analysis, for each psychometric scale described in Section 3, we conducted a confirmatory factor analysis using Principal Component Analysis (PCA) [49]—applying the rotation method used originally by the authors' of the psychometric scales—to confirm the theoretical structure and underlying factors of the scales. A scale's *Reliability* measures how consistent the scale is when administered repeatedly. We measured reliability using Cronbach's alpha (α) for which, a value of 0.7 of greater is considered acceptable, while a value greater than 0.8 is considered good [50].

Starting with the DoSpeRT scale, a PCA with oblimin rotation revealed the original factor structure of the scale and when taken together, the factors explained 56% of the variance in the data. We extracted these factors and computed their reliability: Ethical ($\alpha = 0.71$), Health/Safety ($\alpha = 0.72$), Financial/Investment ($\alpha = 0.79$), Financial/Gambling ($\alpha = 0.90$), Recreational ($\alpha = 0.82$), and Social ($\alpha = 0.78$).

Next, with the RTC scale, a PCA with oblique rotation revealed the original factor structure of the scale and when taken together, the factors explained 63% of the variance in the data. We extracted these factors and computed their reliability: Emotional Reaction ($\alpha = 0.88$), Short-term Focus ($\alpha = 0.84$), Routine Seeking ($\alpha = 0.81$), and Cognitive Rigidity ($\alpha = 0.70$). Next, we examined the uni-dimensional CFC and the NFC scales. Both these scales revealed high reliability: ($\alpha = 0.9$) and ($\alpha = 0.95$) respectively.

Finally, with SeBIS, a PCA with varimax rotation revealed the original factor structure of the scale and when taken together, the factors explained 59% of the variance in the data. We extracted these factors and computed their reliability: Proactive Awareness ($\alpha = 0.72$), Password Generation ($\alpha = 0.78$), Device Securement ($\alpha = 0.80$), and Device Updating ($\alpha = 0.70$). Therefore, we found sufficient evidence to prove that our data was both reliable and valid.

4.5.2 Logistic Regression: Analyzing Auto-updating Differences

To answer our first research question—investigating the differences that exist between those Android users who currently avoid auto-updating and those who auto-updates their applications—we constructed a logistic regression model [51] using the glm() from the "stats" package in R. Logistic regression is a regression model where the dependent variable is categorical and binary. In our case, the binary outcome is whether participants avoided auto-updating or did auto-update their applications. Because of the low number of participants who restricted auto-updating only for some applications (10%; Section 4.4), we only considered participants' settings from the Play Store (Figure 1) as they reported in Section Two of the survey. We regressed this update choice ("Avoided Auto-updating" = 1 vs "Auto-updated" = 0) on the psychometrics (DoSpeRT, RTC, CFC, NFC), the covariates (SeBIS, age, gender, education), and the presence of a previous negative experience with updating software (Neg. Experience). We coded all those who answered "I don't remember" to having had a previous software updating negative experience as the absence of one. To reduce the number of levels in education, we transformed it into a continuous variable using the following scheme: No High School:1, (High School Graduate, Some College):2, (Bachelor's Degree, Associate's Degree):3, (Master's Degree, Doctoral Degree, Professional Degree):4.

4.5.3 Linear Mixed Effects Model: Analyzing Auto-updating Preferences

To answer our second research question—analyzing how users characteristics explain users' preferences towards auto-updating their mobile applications—we first compiled, for each participant, two scores indicating *how comfortable* they were, one each for security and non-security updates (Update Type), across the data for each application they rated. This lead to a total of $N = 7952$ pairs of (participant, application) with responses to each of the factors we considered in Section 4.1.2. Overall, participants answered the questions about their update preferences for 8.5 applications on average (median = 10). Following that, we constructed a linear mixed-effects regression model [52] using the lmer() from the "lme4" package in R. These models are extensions of the linear regression model in which the predictors contain random effects in addition to the usual fixed effects. Since each participant only answered questions about a subset of the applications—a maximum of 10—we considered a partially crossed random effects model, where the dependent variable was the comfort score, and amongst the predictors, the various user characteristics (Past software updating experience, Psychometric data, SeBIS scores, UpdateType, Trust, Use Frequency, Importance, Satisfied) were the fixed effects, and the subjects and applications were random effects. We also added the demographic variables: age, gender and education, which was coded as before.

5. FINDINGS

Overall, our study showed that users who avoid auto-updates for applications on Android differ from those who auto-update by three characteristics. First, these users have usually had a previous negative experience updating their software—confirming the findings of previous studies for desktop users [12, 13]. However, our study newly suggests that these negative experiences may have occurred on devices other than participants' Android phones, such as their desktops and laptops. Second, these users tend to take fewer financial investment risks (e.g., lower chance to invest money in business ventures and mutual funds) and fewer ethical risks (e.g., lower chance to take questionable deductions on their income task returns). Third, these users exhibit

a greater propensity to take proactive steps to maintain their online security—similar to what others have found for desktop users [13]. Overall, across their applications, our participants were less comfortable auto-updating if they had a previous negative updating experience, but more comfortable auto-updating security updates over non-security updates, and applications they deemed trustworthy.

5.1 Differentiating Users Who Avoid Auto updating From Those Who Auto-Update

In our first research question, we asked how those users who avoid auto-updates differ from those who auto-update their applications on Android based on their current reported auto-update settings. The result of the logistic regression model regressing users' update choice on the various psychometric scales, users' past experiences with software updating, and their demographics is shown in Table 2. A likelihood ratio test [53] between the null model and the model with all the predictors revealed an effect size of 0.089 ($p < 0.0001$), and the Nagelkerke R^2 [54] of the model was 0.15—both indicating a good fit for the model.

5.1.1 Past Negative Software Updating Experience

In the survey, nearly 40% of the participants reported having had a previous negative experience with updating their software across their devices. Broken down by whether participants auto-updated their applications, 34.9% of those who auto-updated and 56.8% of those who avoided auto-updating their applications had a previous negative experience with updating their software.

Our results indicate support for hypothesis **H1**, that avoiding auto-updates is associated with past negative experiences with software updates. As seen in Table 2, we observed a significant and large effect size for the coefficient of Negative Experience ($e^{\beta} = 2.81$, $p < 0.0001$, C.I. = [1.75, 4.56]). Given the positive coefficient, we conclude that having had a previous negative experience with software updating is associated with avoiding auto-updates for applications on Android. It is important to note here that we asked for participants' negative experiences across their devices—not just their Android phones—and this may indicate a tendency for these experiences to affect updating behaviors on devices other than the one they had the negative experience on.

The participants reported a variety of negative experiences with software updating—similar to the reasons reported in previous studies [29, 12, 13, 25]—such as updates caused the software to be buggy, updates made the user interface of the software uncomfortable to use, and updates took a long time to install. Table 3 lists a summary of the negative experiences reported by the survey participants along with the frequency of their appearance. Those participants who chose to elaborate on their negative updating experiences (4.6%) stated:

- How their computers crashed: e.g., P34 *"Windows 10, or garbage time, breaks pretty much every time it updates."*
- How their devices were incompatible with the update: e.g., P145 *"The update I downloaded made other apps buggy."*
- How the update changed and toggled their application settings: e.g., P298 *"The update deleted my password and I could not get it back and it would not let me know what it was. This happened with iTunes and is why I now have Android and not Apple products of any kind. I also lost all the music I had purchased."*

5.1.2 Risk Averse Behavior Intentions

Our results indicated support for hypothesis **H2**, that avoiding auto-updates for applications is associated with lower risk taking behavior, specifically in two domains. First, we found a significant and medium effect size indicating that those who avoid auto-updating their applications also tended to take fewer financial investment risks as indicated by the DoSpeRT-Investment ($e^{\beta} = 0.79$, $p < 0.01$, C.I. = [0.66, 0.94]) coefficient in Table 2. This means that these users were less likely to invest any money into mutual funds, new business ventures, or speculative stocks. Second, we found a significant and medium effect size indicating that those who avoid auto-updating their applications also tended to take fewer ethical risks as indicated by the DoSpeRT-Ethical ($e^{\beta} = 0.75$, $p < 0.01$, C.I. = [0.62, 0.91]) coefficient in Table 2. This means that these users were less likely to indulge in affairs with married men/women or keep a lost wallet containing money for themselves. We found no differences in the remaining DoSpeRT domains (Health/Safety, Gambling, Recreational, Social), suggesting that these factors might not differentiate those users who avoid auto-updating from those who auto-update their applications on Android.

At this point, it is worth considering why we found differences particularly in the investment and ethical domains and not the others. We conjecture that because low scores on both the DoSpeRT-Ethical and Investment sub-scales indicate taking responsibility and being in control, they differentiate those users who avoid auto-updating—users with lower scores on these scales—as these users may also express a sense of responsibility over controlling the changes updates make to their devices. These differences may have been less apparent in the DoSpeRT-Gambling sub-scale as gambling and betting are more generally considered risky activities. Furthermore, we conjecture that while both the DoSpeRT-Recreational and Social sub-scales indicate a similar sense of taking responsibility, the associated risks involve references to social activities—that is, interactions with others and in groups—and may therefore, have been less apparent in decisions that affects only the self. Other research [17] has shown that both these sub-scales may be more predictive of users' privacy expectations.

It is also worth pointing out a subtle difference between our result and the results of Egelman and Peer [16] with regards to software updating and risk taking. In their study, Egelman and Peer observed that risk taking was inversely correlated with how often users took actions to update their software (as measured by the SeBIS-Device Updating sub-scale), i.e., low risk taking individuals were more likely to update their software. On the other hand, our results demonstrate that low risk taking individuals were less likely to auto-update—despite the fact that auto-updating should, at least in theory, keep software updated sooner and faster. We believe that this difference is associated with the underlying risks. That is, when users are asked to take actions and make decisions about updating their software, low risk taking individuals are likely to update often because these users are concerned about the risks of not updating (i.e., potential exploits and

Predictor	Estimate	Std. Error	Odds Ratio	Odds Ratio 95% C.I.	p-value
(Intercept)	0.19	1.35	1.21	[0.09, 17.20]	0.89
CFC	−0.33	0.21	0.72	[0.48, 1.09]	0.12
NFC	0.02	0.16	1.02	[0.75, 1.39]	0.92
DoSpeRT-Ethical	−0.29	0.10	0.75	[0.62, 0.91]	**< 0.01**
DoSpeRT-Social	−0.10	0.12	0.90	[0.72, 1.14]	0.39
DoSpeRT-Health/Safety	−0.18	0.14	0.84	[0.64, 1.09]	0.19
DoSpeRT-Recreational	0.17	0.11	1.19	[0.96, 1.48]	0.11
DoSpeRT-Investment	−0.24	0.09	0.79	[0.66, 0.94]	**< 0.01**
DoSpeRT-Gambling	0.08	0.11	1.08	[0.86, 1.34]	0.48
RTC-Emotional Reaction	−0.04	0.18	0.96	[0.69, 1.33]	0.79
RTC-Routine Seeking	−0.03	0.18	0.97	[0.68, 1.38]	0.85
RTC-Cognitive Rigidity	−0.01	0.14	0.99	[0.75, 1.32]	0.95
RTC-Short term Focus	0.17	0.18	1.19	[0.83, 1.70]	0.35
Neg. Experience [Yes]	1.03	0.24	2.81	[1.75, 4.56]	**< 0.0001**
SeBIS-Proactive Awareness	0.35	0.17	1.42	[1.01, 2.01]	**0.04**
SeBIS-Password Generation	0.08	0.16	1.08	[0.79, 1.48]	0.63
SeBIS-Device Updating	−0.13	0.16	0.88	[0.65, 1.19]	0.41
SeBIS-Device Securement	0.10	0.11	1.11	[0.89, 1.39]	0.37
Age	−0.01	0.02	0.99	[0.96, 1.01]	0.33
Education	−0.12	0.19	0.89	[0.61, 1.29]	0.54
Gender [Male]	0.08	0.26	1.09	[0.65, 1.83]	0.74
Model Fit Likelihood Ratio Test: Deviance = 45.99, $p < 0.0001$					
Model Likelihood Ratio Effect Size: 0.089					

Table 2: Results of the Logistic Regression Modeling the Outcome ("Avoided Auto-updating") on the Various Predictors. 95% C.I. is the 95% Confidence Interval. Bolded p-values are Significant at the 0.05 Level.

Negative Experience	Frequency
Version prior to update worked better	36.4%
The update introduced new bugs	34.3%
The update modified the user interface	27.6%
The update took a long time to install	11.3%
The update used up a lot of data	10.7%

Table 3: Negative Experiences with Software Updating Reported by the Survey Participants.

harm). However, with respect to auto-updating, low risk taking individuals are likely to turn off automatic updates because these users are concerned about the risks of auto-updating (i.e., undesirable and negative consequences).

5.1.3 Greater Proactive Security Awareness

Our results also indicated a significant and small effect size indicating that users who avoided auto-updating their applications also exhibited a greater propensity to take proactive steps to maintain their online security; the coefficient of SeBIS-Proactive Awareness ($\beta = 1.42$, $p = 0.04$, C.I. = [1.01, 2.01]). This means that these users were more likely to verify links before opening them, ensure the green HTTPS lock was visible before submitting information, and fix security problems by themselves rather than depending on others. This result supports the findings of Forget *et al.* [13] who, in a study with 15 desktop users, observed that those users who desired control and assumed responsibility in maintaining the security of their computers took proactive security steps (e.g. periodic virus checks), and also sometimes turned off automatic updates.

On the other hand, we observed no such differences between those users who avoided auto-updates and those users who auto-updated their applications with regards to their intentions to behave securely based on the Password Generation, Device Updating, or Device Securement sub-scales—suggesting that the security intentions of users who avoid auto-updates and do auto-update may not be different.

Overall, in our regression model we found evidence to support hypothesis **H1**, auto-updating is associated with previous negative experiences, and hypothesis **H2** that auto-updating applications on Android is associated with taking fewer risks. However, we found no evidence to support hypothesis **H3**, **H4**, **H5**, suggesting that auto-updating may not be associated with consideration of future consequences, curiosity and inquisitiveness, or resistance to change respectively.

5.2 Users' Auto-Updating Preferences

In our second research question, we asked how user characteristics explain users' preferences for how they would like to auto-update across their applications on Android. In the survey, participants rated *how comfortable* they were auto-updating security and non-security updates for the applications they selected. The result of the linear mixed effect regression is shown in Table 4; we only report the significant fixed effects. The $R^2_{LMM_m}$ measure [55] considering only the fixed effects in the model was 0.25—indicating a medium to large effect size. As well, the variance ($\sigma^2 = 432.42$) due to the Participant random effect was much greater than the variance ($\sigma^2 = 5.40$) due to the Application random effect, indicating that differences in preferences towards auto-updating were much greater across participants but fairly consistent across applications.

Fixed Effects	Estimate	Std. Error	Est 95% C.I.	p-value
Neg. Experience [Yes]	−7.39	2.14	[−11.49, −3.29]	< 0.001
SeBIS-Proactive Awareness	−3.84	1.47	[−6.67, −1.02]	< 0.01
UpdateType [Security]	6.76	0.37	[6.03, 7.49]	< 0.0001
Trust	7.29	0.34	[6.61, 7.96]	< 0.0001
Importance	2.24	0.25	[1.76, 2.73]	< 0.0001
Satisfied	2.96	0.32	[2.32, 3.58]	< 0.0001
Model $R^2_{LMM_m}$ Measure: 0.25				

Table 4: Results of the Linear Mixed Effect Model for the Auto-updating Preferences. Participant and Application were Included as Random Effects. 95% C.I. is the 95% Confidence Interval. Only the Significant Fixed Effects are Shown.

Previous Negative Updating Experience: We observed that having had a previous negative experience with software updating affected how comfortable users were towards auto-updating their applications. In our model, we observed a significant and medium effect size for the coefficient of Negative Experience ($\beta = -7.39$, $C.I. = [-11.49, -3.29], p < 0.001$), indicating that once users have a negative experience with updating their software, they become less comfortable auto-updating their applications.

Perceived Trust in the Application: Android applications' perceived trustworthiness played an important part in users' decision making towards auto-updating them. In our model, we observed a significant and medium effect size for the coefficient of Trust ($\beta = 7.29$, $C.I. = [6.61, 7.96], p < 0.0001$), indicating that the more trustworthy users considered an application, the more comfortable they were auto-updating it.

Security Updates vs Non-security Updates: We also observed that the type of update played an important part in whether users would let it apply automatically. In our model, we observed a significant and medium effect size for the coefficient of security updates ($\beta = 6.76$, $C.I. = [6.03, 7.49], p < 0.0001$), indicating that users were more comfortable auto-updating security updates over non-security updates.

Greater Security Awareness: We observed that those users who displayed a higher proactive awareness towards managing their security were less comfortable towards auto-updating their applications. In our model, we observed a significant but small effect size for the coefficient of SeBIS-Proactive Awareness ($\beta = -3.84$, $C.I. = [-6.67, -1.02], p < 0.01$), indicating that users who exhibited greater propensity to engage in proactive security behavior were less comfortable auto-updating their applications.

Perceived Satisfaction with the Application: Android applications' perceived satisfactory performance played a less important part in users' decision making towards auto-updating. In our model, we observed a significant but small effect size for the coefficient of Satisfied ($\beta = 2.96$, $C.I. = [2.32, 3.58], p < 0.0001$), indicating that the more satisfied users were with an application, the more comfortable they were auto-updating it.

Perceived Importance of the Application: Android applications' perceived importance to users also played an important part in users' decision making towards auto-updating them. In our model, we observed a significant but small effect size for the the coefficient of Importance ($\beta = 2.24$, $C.I. = [1.76, 2.73], p < 0.0001$), indicating that the more important users considered an application, the more comfortable they were auto-updating it.

While drawing comparisons with the results for desktop users in [25] is difficult since the previous study included a small sample size, we point out how our results differ. Our results suggest that like desktop users, mobile users are more comfortable auto-updating applications they trust, and more comfortable auto-updating security updates over non-security updates. While desktop users are less comfortable auto-updating applications they are satisfied with and are important to them, both factors have only a small influence on how comfortable mobile users' feel towards auto-updating their applications. Finally, unlike desktop users who were less comfortable auto-updating applications they frequently used, we observed no differences with Android users. It may be possible that we observed no difference because we considered the most popular Android applications which could be used more frequently overall.

6. DISCUSSION

In the following section, we outline the implications of our findings for improving the design of Android OS update system, and encouraging users who avoid auto-updating mobile applications to auto-update security updates.

6.1 Improve Auto-update User Interfaces

To help mobile users keep their applications updated, we suggest that mobile update systems make application software update rollbacks more accessible, and include nudges to encourage users to auto-update security updates.

6.1.1 Make Update Rollbacks Accessible

Our first recommendation stems from our finding that avoiding auto-updating mobile applications on Android is associated with having had a previous negative experience with updating. Therefore, we recommend that one improvement to the current Android OS, or mobile application update systems more generally, would be to provide users with the ability to rollback updates for all applications to a previous point in time to help users who dislike changes made by updates to a particular application to rollback those changes. Presently, updates for applications that are installed from the Play Store cannot be rolled back; update rollbacks are only allowed for applications that come pre-installed with the device (as described in Section 2.3). However, because the implications of update rollbacks may be potentially harmful—as security updates may be rolled back as well—this change

may require a mobile OS to restrict update rollback for applications that do not contain recent security updates. Such a system would also rely on informing users about potential feature losses to help them understand what rolling back updates would entail. Overall, this would potentially increase end-users' confidence in auto-updating security updates.

6.1.2 Design Nudges for Auto-Updating

Our second recommendation stems from our findings that users who avoid auto-updating mobile applications on Android also tend to take fewer investment risks and fewer ethical risks. We suggest that these characteristics can be used to design "nudges" to persuade users to auto-update security updates, since our findings suggest that overall, users are more comfortable automating security updates. Nudges entail the use of behavioral economics to encourage users into making certain decisions [56]. Numerous studies have experimented with nudging to affect behavior change in domains ranging from health [57, 58, 59] to retirement savings policies [60, 61]. In the privacy and security community, recent studies have created nudges for users to make stronger passwords using password meters [62], and others have nudged users into reducing regrets during online social network use [63].

Specifically, we envision nudges to encourage users to auto-update security updates that leverage the vast literature on "Framing Effects" [64]—a cognitive bias in which people react to choices based on how these choices are framed (such as loss vs gains). For instance, because users who avoid auto-updating application updates on Android also take fewer ethical risks as measured by the DoSpeRT-Ethical scale, one nudge could highlight the ethical risk and responsibility associated with not auto-updating security updates, e.g., *"Switching auto-updates on for security updates will protect you, and others like you from suffering the consequences of someone exploiting your device"*. Similarly, because the same users also take fewer investment risks, as measured by the DoSpeRT-Investment scale, another nudge could highlight the financial and investment risk associated with not auto-updating security updates: *"Not switching auto-updates on for security updates increases the chances of someone gaining access to your bank account or stealing your credit card information"*. Both these nudges, using the risk taking traits resulting from our findings, emphasize the potential losses—an attacker exploiting your device, or accessing your credit card information—that may result from not auto-updating security updates.

Such nudges could also emphasize that negative experiences such as changes to the user interface or data loss, will be minimized since these are primarily security updates. If the Android OS implements a mechanism to rollback updates, as we touched upon in Section 6.1.1, these nudges could also remind users about the application update rollback setting and emphasize that users can un-install updates at any time if they dislike the changes caused post update. These nudges could be presented to users at different times. For instance, these nudges could be presented to users who avoid auto-updates when they attempt to switch off auto-updates, or soon after they manually install an update for an application. Future research could test the effectiveness of these nudges and messages by means of various controlled experiments.

In addition to nudges, security education experts can leverage the same ethical and investment risk taking trait differences between users who avoid auto-updating and those who do not in order to design better security education campaigns and security advice for end-users. For instance, the ethical risk taking could be used to highlight that *"Users have a responsibility to auto-update their systems and keep their organization and fellow users safe"*, and changes in user behavior could be measured pre- and post-training.

Of course, allowing auto-updates for security updates only will entail providing software developers with the incentives, education, and necessary infrastructure to decouple mobile application security updates, whenever possible, from all other kinds of updates. On Android, enabling this functionality would also require a redesign of the application update interface. As Figure 1 shows, the Android OS currently has provisions for users to either auto-update all their applications, disallow auto-update for certain applications (through the applications' page on the Play Store), or auto-update none of their applications. However, there is no provision for users to automate certain kinds of updates over others. In contrast, the Apple Mac OS X system allows users to selectively automate security OS updates while restricting updates of all other types [65]. The Android OS could extend this concept to the Play Store, providing users with another option to automate only security updates.

6.2 Examine Update Development Practices

Our third recommendation stems again from our finding that mobile users who avoid application auto-updates have had a previous negative experience with software updating. We suggest that the burden of updating applications and device should not solely rely on end-users, and echoing the call of others [66], we hope that the security community go beyond studying the updating behaviors of end-users and also investigate how software developers decide to develop, build, and test software updates in the first place. Like end-users, software developers make trade-offs when deciding what content to add or remove via an update, or what security changes to push to end-users. These trade-offs maybe influenced by a variety of factors, including their attitudes, motivations, and the feedback they receive from their end-users. Future research could identify how software developers propagate application changes to their end-users, what specific changes lead to negative experiences for end-users, and ways to minimize these downsides as part of the update development process. For instance, when developers add or remove features from a particular application, how do they consider these changes will impact those users with the current version of the application, and how do developers decide what information to provide to users to inform them about the changes made by updates?

6.3 Personalize Mobile Auto-update Systems

Our fourth recommendation stems from our finding that overall, mobile users' perceived level of trust with applications, and the type of update (security over non-security updates) is positively and strongly correlated with how comfortable they felt auto-updating their applications. Because users' auto-updating preferences contain some nuances, we argue that a one-size-fits-all update system may be less optimal, and work against the preferences of those users who avoid auto-updating. While the Play Store does provide users with the ability to restrict auto-updates for certain applications—

as described in Section 2.3—the choice to do so lies with the end users, and can ultimately be an effort requiring task because a user can have 95 different applications installed on average [67]. Indeed, in our data only 10% of our participants actually used this feature.

Therefore, we propose that mobile update systems need to be more personalized and learn from users and their actions, and accordingly decide which applications to auto-update and which others to not—selectively involving users only when necessary. Our findings provide a starting point for personalization based on the user characteristics and preferences we identified for users auto-updating their mobile applications. For instance, since users in our study were more comfortable auto-updating applications they trusted, future systems could explore and uncover proxies for trust, and use that to drive auto-update decisions. Some proxies of trust might include dimensions such as whether a user provides a high rating, or a positive comment for a particular application, or has downloaded multiple applications from the same application developer.

These proxies could allow the system to help suggest or even decide when to automatically install updates for any particular application depending on the user's preference for consent to update. As another example, the system could automatically install all updates for applications that users might generally trust, such as emergency applications. Of course, such a system would require great transparency, and be able to inform users about *what* actions it has taken and *how* it arrived at the decision of taking those actions.

7. LIMITATIONS

Our study has several limitations. First, our results correlating user characteristics and their choice of automating updates is limited to how applications are updated on the Android platform, and therefore limited in how far they can be generalized to non-application updates (such as OS updates). Second, as noted in Section 4.3, our survey collected users' self-reported update settings, and these settings may be subject to error. Third, the applications users reported having installed on their phones could be subject to recall bias, and are only limited to the ones we presented as part of the survey. However, providing a list of all applications was impractical, and we had to pare it to the most popular applications. Fourth, as a result of choosing the AMT platform, our results are limited in their generalizability to other Android users. However, while the psychometric scales have been used outside of AMT before, the SeBIS scale has only been tested and validated on AMT, which made it a reasonable platform to run our study. Furthermore, the AMT population, while limited in its diversity, has been shown to be fairly similar to participants from university campuses and other online participant pools [68, 69]. Despite these limitations, our study provides insight into users preferences towards auto-updating mobile applications.

8. CONCLUSION AND FUTURE WORK

We conducted a survey to understand how user characteristics affect attitudes towards mobile application updates on Android. We found that three characteristics differentiated those users who avoid auto-updates from those who auto-update their mobile applications. These characteristics are past experiences with software updating, propensity to engage in risk taking behavior, and displaying greater proactive awareness about their online security.

We also found that previous negative experiences made users less comfortable with auto-updating their applications. However, users were more comfortable with the idea of auto-updating security updates and applications they deemed more trustworthy. Based on these findings, we made four recommendations for improving security on Android by encouraging users to switch on auto-updates via making application update rollbacks more accessible, nudging users to auto-update, studying software developers and their update development practices, and using our findings as a starting point for personalizing mobile update systems.

Future work could examine how users' attitudes towards auto-updating vary on other platforms and devices, and more directly observe or infer how users update as opposed to using self-reported user data. Future work could also examine how our results generalize beyond the AMT platform by repeating our survey on a more representative sample of Android users. Finally, future work could use controlled experiments to present users with different versions of the nudges we proposed, and measure whether or not users are moved to switch on auto-updates after being exposed to these kinds of nudges. Another potential area for future inquiry would be to build on our findings to help create both user and application profiles for personalizing auto-updates in mobile OS update systems.

Lastly, auto-updating applications on a mobile also poses an interesting dichotomy: while on one hand auto-updates may bring enhanced security and protection, on the other hand these updates can also be abused by malicious software developers. These malicious developers might want to use this channel to collect more data about users that might be of high value to advertisers, or inject advertisement libraries. A final suggestion for future research is to consider this dichotomy in greater detail, and devise ways so that software updates are vetted before they can be automated.

9. ACKNOWLEDGEMENTS

We thank Yasemin Acar for shepherding the paper, and the anonymous reviewers for their helpful comments. We also thank Michelle Mazurek, Jessica Vitak, Marian Harbach, Nathan Malkin, and Elissa Redmiles for feedback on earlier drafts of the paper. Our research is based upon work supported by the Maryland Procurement Office under contract H98230-14-C-0137. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Maryland Procurement Office.

10. REFERENCES

[1] Symantec. Internet Security Threat Report. `https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf`, April 2016.

[2] Kenneth Olmstead and Aaron Smith. Americans and Cybersecurity. `http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/`, January 2017.

[3] Marten Oltrogge, Yasemin Acar, Sergej Dechand, Matthew Smith, and Sascha Fahl. To pin or not to pin—helping app developers bullet proof their tls connections. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 239–254, Washington,

D.C., 2015. USENIX Association.

[4] Net Applications Inc. Mobile/Tablet Operating System Market Share. https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1, August 2016.

[5] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. Why Eve and Mallory Love Android: An Analysis of Android SSL (in)Security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 50–61, New York, NY, USA, 2012. ACM.

[6] Vishwanath Raman Adrian Mettler, Yulong Zhang. SSL Vulnerabilities: Who Listens When Android Applications Talk? https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-\applications-talk.html, August 2014.

[7] Williams Pelegrin. These android, ios, and wp8 apps are affected by the heartbleed bug. http://www.digitaltrends.com/mobile/heartbleed-bug-apps-affected-list/, April 2014.

[8] Cisco. Cisco Annual Security Report. https://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf, 2015.

[9] Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, and Tudor Dumitras. The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 692–708, Piscataway, NJ, USA, May 2015. IEEE.

[10] US-CERT. Before You Connect a New Computer to the Internet. https://www.us-cert.gov/ncas/tips/ST15-003, December 2015.

[11] Thomas Duebendorfer and Stefan Frei. Why silent updates boost security. *TIK, ETH Zurich, Tech. Rep*, 302, 2009.

[12] Kami Vaniea and Yasmeen Rashidi. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 3215–3226, New York, NY, USA, 2016. ACM.

[13] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, Denver, CO, June 2016. USENIX Association.

[14] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, Ottawa, 2015. USENIX Association.

[15] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, 2015.

[16] 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*, CHI '15, pages 2873–2882, New York, NY, USA, 2015. ACM.

[17] Serge Egelman and Eyal Peer. The Myth of the Average User: Improving Privacy and Security Systems Through Individualization. In *Proceedings of the 2015 New Security Paradigms Workshop*, NSPW '15, pages 16–28, New York, NY, USA, 2015. ACM.

[18] Juan Herrero, Alberto Urueña, Andrea Torres, and Antonio Hidalgo. My computer is infected: the role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm. *Journal of Risk Research*, pages 1–14, 2016.

[19] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey. Users really do plug in usb drives they find. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 306–319, May 2016.

[20] Nathan Malkin, Arunesh Mathur, Marian Harbach, and Serge Egelman. Personalized security messaging: Nudges for compliance with browser warnings. In *2nd European Workshop on Usable Security*. Internet Society, 2017.

[21] Pam Briggs Debora Jeske, Lynne Coventry and Aad van Moorsel. Nudging whom how: IT proficiency, impulse control and secure behaviour. *Networks*, 49:18, 2014.

[22] Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. *Risk Communication Design: Video vs. Text*, pages 279–298. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[23] Timothy Kelley, L. Jean Camp, Suzanne Lien, and Douglas Stebila. Self-identified Experts Lost on the Interwebs: The Importance of Treating All Results As Learning Experiences. In *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results*, LASER '12, pages 47–54, New York, NY, USA, 2012. ACM.

[24] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 373–382, New York, NY, USA, 2010. ACM.

[25] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. "They Keep Coming Back Like Zombies": Improving Software Updating Interfaces. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 43–58, Denver, CO, June 2016. USENIX Association.

[26] 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*, CHI '16, pages 5257–5261, New York, NY, USA, 2016. ACM.

[27] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages

327–346, Ottawa, July 2015. USENIX Association.

[28] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 666–677, New York, NY, USA, 2016. ACM.

[29] Kami E. Vaniea, Emilee Rader, and Rick Wash. Betrayed by Updates: How Negative Experiences Affect Future Security. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 2671–2674, New York, NY, USA, 2014. ACM.

[30] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A Study of Users' Experiences and Beliefs about Software Update Messages. *Computers in Human Behavior*, 51, Part A:504 – 519, 2015.

[31] Marshini Chetty, Richard Banks, A.J. Brush, Jonathan Donner, and Rebecca Grinter. You're Capped: Understanding the Effects of Bandwidth Caps on Broadband Use in the Home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 3021–3030, New York, NY, USA, 2012. ACM.

[32] Arunesh Mathur, Brent Schlotfeldt, and Marshini Chetty. A Mixed-methods Study of Mobile Users' Data Usage Practices in South Africa. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '15, pages 1209–1220, New York, NY, USA, 2015. ACM.

[33] Andreas Moller, Stefan Diewald, Luis Roalter, Technische Universitat Muchen, Florian Michahelles, and Matthias Kranz. Update Behavior in App Markets and Security Implications: A Case Study in Google Play. In *In Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI*, pages 3–6, 2012.

[34] Yuan Tian, Bin Liu, Weisi Dai, Blase Ur, Patrick Tague, and Lorrie Faith Cranor. Supporting privacy-conscious app update decisions with user reviews. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '15, pages 51–61, New York, NY, USA, 2015. ACM.

[35] Christos Gkantsidis, Thomas Karagiannis, and Milan VojnoviC. Planet Scale Software Updates. *SIGCOMM Comput. Commun. Rev.*, 36(4):423–434, August 2006.

[36] Rick Wash, Emilee Rader, Kami Vaniea, and Michelle Rizor. Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences. In *Tenth Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 89–104, Menlo Park, 2014. USENIX Association.

[37] W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. Security Automation Considered Harmful? In *Proceedings of the 2007 Workshop on New Security Paradigms*, NSPW '07, pages 33–42, New York, NY, USA, 2008. ACM.

[38] Google. Update Downloaded Apps. `https://support.google.com/googleplay/answer/113412?hl=en`, September 2016.

[39] Rollback or Uninstall Updates on Android App. `https://www.updateallapps.com/rollback-uninstall-updates-android-app/`, June 2016.

[40] Google. Working with System Permissions. `https://developer.android.com/training/permissions/index.html`, 2016.

[41] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods*, 46(4):1023–1031, 2014.

[42] Ann-Renée Blais and Elke U Weber. A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, 1(1), 2006.

[43] Jeff Joireman, Monte J Shaffer, Daniel Balliet, and Alan Strathman. Promotion orientation explains why future-oriented people exercise and eat healthy evidence from the two-factor consideration of future consequences-14 scale. *Personality and Social Psychology Bulletin*, 38(10):1272–1287, 2012.

[44] Richard E Petty, John T Cacioppo, and Chuan Feng Kao. The efficient assessment of need for cognition. *Journal of Personality Assessment*, 48(3):306–307, 1984.

[45] Shaul Oreg. Resistance to change: developing an individual differences measure. *Journal of applied psychology*, 88(4):680, 2003.

[46] Wikipedia. List of Most Downloaded Android Applications. `https://en.wikipedia.org/wiki/List_of_most_downloaded_Android_applications`, 2016.

[47] Seymour Sudman, Norman M Bradburn, and Norbert Schwarz. *Thinking about answers: The application of cognitive processes to survey methodology.* Jossey-Bass, 1996.

[48] Mike Furr. *Scale construction and psychometrics for social and personality psychology.* SAGE Publications Ltd, 2011.

[49] Harold Hotelling. Analysis of a complex of statistical variables into principal components. *Journal of educational psychology*, 24(6):417, 1933.

[50] Rosemary R Gliem and Joseph A Gliem. Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, 2003.

[51] David W Hosmer Jr, Stanley Lemeshow, and Rodney X Sturdivant. *Applied logistic regression*, volume 398. John Wiley & Sons, 2013.

[52] Douglas Bates, Martin Mächler, Ben Bolker, and Steve Walker. Fitting linear mixed-effects models using lme4. *arXiv preprint arXiv:1406.5823*, 2014.

[53] Scott Menard. Coefficients of determination for multiple logistic regression analysis. *The American Statistician*, 54(1):17–24, 2000.

[54] Nico JD Nagelkerke. A note on a general definition of the coefficient of determination. *Biometrika*, 78(3):691–692, 1991.

[55] Shinichi Nakagawa and Holger Schielzeth. A general and simple method for obtaining R2 from generalized linear mixed-effects models. *Methods in Ecology and Evolution*, 4(2):133–142, 2013.

[56] H Thaler Richard and R Sunstein Cass. Nudge: Improving decisions about health, wealth, and happiness, 2008.

[57] Eric J Johnson and Daniel G Goldstein. Defaults and donation decisions. *Transplantation*, 78(12):1713–1716, 2004.

[58] Julie S. Downs, George Loewenstein, and Jessica Wisdom. Strategies for Promoting Healthier Food Choices. *American Economic Review*, 99(2):159–64, May 2009.

[59] Scott D. Halpern, Peter A. Ubel, and David A. Asch. Harnessing the Power of Default Options to Improve Health Care. *New England Journal of Medicine*, 357(13):1340–1344, 2007. PMID: 17898105.

[60] Brigitte C Madrian and Dennis F Shea. The power of suggestion: Inertia in 401 (k) participation and savings behavior. *The Quarterly Journal of Economics*, 116(4):1149–1187, 2001.

[61] James J Choi, David Laibson, Brigitte C Madrian, Andrew Metrick, et al. Saving for retirement on the path of least resistance. *Rodney L White Center For Financial Research - Working Papers* -, 9, 2005.

[62] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 2379–2388, New York, NY, USA, 2013. ACM.

[63] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2367–2376, New York, NY, USA, 2014. ACM.

[64] Irwin P Levin, Sandra L Schneider, and Gary J Gaeth. All frames are not created equal: A typology and critical analysis of framing effects. *Organizational behavior and human decision processes*, 76(2):149–188, 1998.

[65] Apple. Mac App Store: Automatic security updates. `https://support.apple.com/en-us/HT204536`, September 2016.

[66] Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *Cybersecurity Development (SecDev), IEEE*, pages 3–8. IEEE, 2016.

[67] Paul Sawers. Android users have an average of 95 apps installed on their phones, according to yahoo aviate data. `https://thenextweb.com/apps/2014/08/26/android-users-average-95-apps-installed\-phones-according-yahoo-aviate-data/`, August 2014.

[68] Daniel J Simons and Christopher F Chabris. Common (mis) beliefs about memory: A replication and comparison of telephone and mechanical turk survey methods. *PloS one*, 7(12):e51876, 2012.

[69] Christoph Bartneck, Andreas Duenser, Elena Moltchanova, and Karolina Zawieska. Comparing the similarity of responses received from studies in amazon's mechanical turk to studies conducted online and with direct recruitment. *PloS one*, 10(4):e0121595, 2015.

APPENDIX

A. PART ONE: PSYCHOMETRIC SCALES

1. Domain Specific Risk Taking (DoSpeRT) scale [42] (Ethical = E, Financial/Investment = F/I, Financial / Gambling = F/G, Health/Safety = HS, Social = S, Recreational = R) [Scoring: 1 (Extremely Unlikely) and 7 (Extremely Likely)]
   - Admitting that your tastes are different from those of a friend. (S)
   - Disagreeing with an authority figure on a major issue. (S)
   - Choosing a career that you truly enjoy over a more secure one. (S)
   - Speaking your mind about an unpopular issue in a meeting at work. (S)
   - Moving to a city far away from your extended family. (S)
   - Starting a new career in your mid-thirties. (S)
   - Going camping in the wilderness. (R)
   - Taking a skydiving class. (R)
   - Bungee jumping off a tall bridge. (R)
   - Piloting a small plane. (R)
   - Going down a ski run that is beyond your ability. (R)
   - Going whitewater rafting at high water in the spring. (R)
   - Betting a day's income at the horse races. (F/G)
   - Betting a day's income at a high-stake poker game. (F/G)
   - Betting a day's income on the outcome of a sporting event. (F/G)
   - Investing 10% of your annual income in a moderate growth mutual fund. (F/I)
   - Investing 5% of your annual income in a very speculative stock. (F/I)
   - Investing 10% of your annual income in a new business venture. (F/I)
   - Drinking heavily at a social function. (HS)
   - Sunbathing without sunscreen. (HS)
   - Riding a motorcycle without a helmet. (HS)
   - Driving or riding a car without wearing a seat belt. (HS)
   - Walking home alone at night in an unsafe area of town. (HS)
   - Engaging in unprotected sex. (HS)
   - Taking some questionable deductions on your income tax return. (E)
   - Having an affair with a married man/woman. (E)
   - Passing off somebody else's work as your own. (E)
   - Revealing a friend's secret to someone else. (E)
   - Not returning a wallet you found that contains $200. (E)
   - Leaving your young children alone at home while running an errand. (E)

2. Consideration for Future Consequences (CFC) scale [43] [Scoring: 1 (Extremely Uncharacteristic of Me) and 7 (Extremely Characteristic of Me)]
    - I consider how things might be in the future, and try to influence those things with my day to day behavior.
    - Often I engage in a particular behavior in order to achieve outcomes that may not result for many years.
    - I only act to satisfy immediate concerns, figuring the future will take care of itself.
    - My behavior is only influenced by the immediate (i.e., a matter of days or weeks) outcomes of my actions.
    - My convenience is a big factor in the decisions I make or the actions I take.
    - I am willing to sacrifice my immediate happiness or well-being in order to achieve future outcomes.
    - I think it is important to take warnings about negative outcomes seriously even if the negative outcome will not occur for many years.
    - I think it is more important to perform a behavior with important distant consequences than a behavior with less important immediate consequences.
    - I generally ignore warnings about possible future problems because I think the problems will be resolved before they reach crisis level.
    - I think that sacrificing now is usually unnecessary since future outcomes can be dealt with at a later time.
    - I only act to satisfy immediate concerns, figuring that I will take care of future problems that may occur at a later date.
    - Since my day-to-day work has specific outcomes, it is more important to me than behavior that has distant outcomes.
    - When I make a decision, I think about how it might affect me in the future.
    - My behavior is generally influenced by future consequences.
3. Need for Cognition (NFC) scale [44] [Scoring: 1 (Extremely Uncharacteristic of Me) and 5 (Extremely Characteristic of Me)]
    - I would prefer complex to simple problems.
    - I like to have the responsibility of handling a situation that requires a lot of thinking.
    - Thinking is not my idea of fun.
    - I would rather do something that requires little thought than something that is sure to challenge my thinking abilities.
    - I try to anticipate and avoid situations where there is a likely chance I will have to think in depth about something.
    - I find satisfaction in deliberating hard and for long hours.
    - I only think as hard as I have to.
    - I prefer to think about small daily projects to long term ones.
    - I like tasks that require little thought once I've learned them.
    - The idea of relying on thought to make my way to the top appeals to me.
    - I really enjoy a task that involves coming up with new solutions to problems.
    - Learning new ways to think doesn't excite me very much.
    - I prefer my life to be filled with puzzles I must solve.
    - The notion of thinking abstractly is appealing to me.
    - I would prefer a task that is intellectual, difficult, and important to one that is somewhat important but does not require much thought.
    - I feel relief rather than satisfaction after completing a task that requires a lot of mental effort.
    - It's enough for me that something gets the job done; I don't care how or why it works.
    - I usually end up deliberating about issues even when they do not affect me personally.
4. Resistance to Change (RTC) scale [45] (RS = Routine Seeking, ER = Emotional Reaction, SF = Short-term Focus, CR = Cognitive Rigidity) [Scoring: 1 (Strongly Disagree) and 6 (Strongly Agree)]
    - I generally consider changes to be a negative thing. (RS)
    - I'll take a routine day over a day full of unexpected events any time. (RS)
    - I like to do the same old things rather than try new and different ones. (RS)
    - Whenever my life forms a stable routine, I look for ways to change it. (RS)
    - I'd rather be bored than surprised. (RS)
    - If I were to be informed that there's going to be a significant change regarding the way things are done at work, I would probably feel stressed. (ER)
    - When I am informed of a change of plans, I tense up a bit. (ER)
    - When things don't go according to plans, it stresses me out. (ER)
    - If one of my bosses changed the performance evaluation criteria, it would probably make me feel uncomfortable even if I thought I'd do just as well without having to do any extra work. (ER)
    - Changing plans seems like a real hassle to me. (SF)
    - Often, I feel a bit uncomfortable even about changes that may potentially improve my life. (SF)
    - When someone pressures me to change something, I tend to resist it even if I think the change may ultimately benefit me. (SF)
    - I sometimes find myself avoiding changes that I know will be good for me. (SF)
    - I often change my mind. (CR)
    - I don't change my mind easily. (CR)
    - Once I've come to a conclusion, I'm not likely to change my mind. (CR)
    - My views are very consistent over time. (CR)

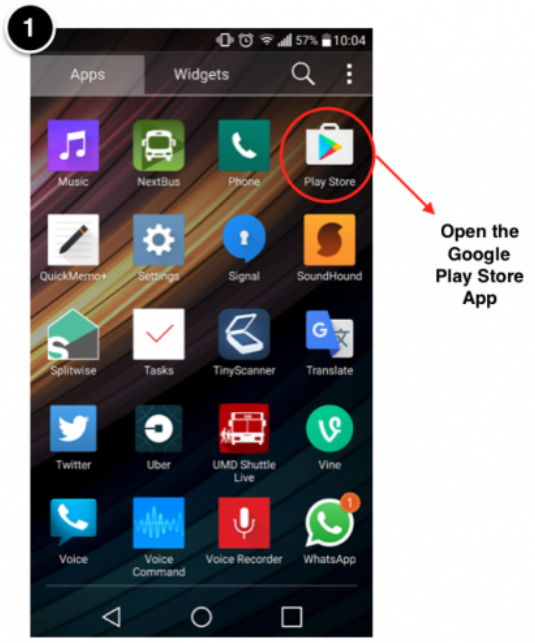
5. Security Behavior Intentions (SeBIS) scale [16] (DU = Device Updating, DS = Device Securement, PG = Password Generation, PA = Proactive Awareness) [Scoring: 1 (Never) and 5 (Always)]

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

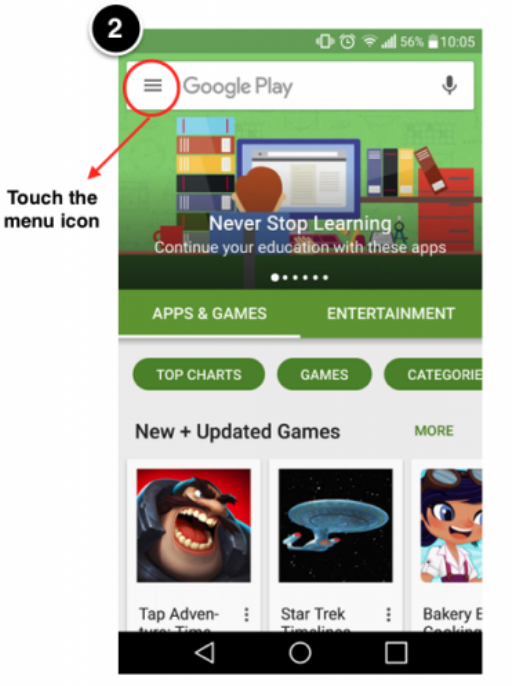
B. PART TWO: ANDROID APPLICATION UPDATE SETTINGS AND AUTO-UPDATING PREFERENCES

1. Please report the following update settings for your Android device by following the instructions in the images below.

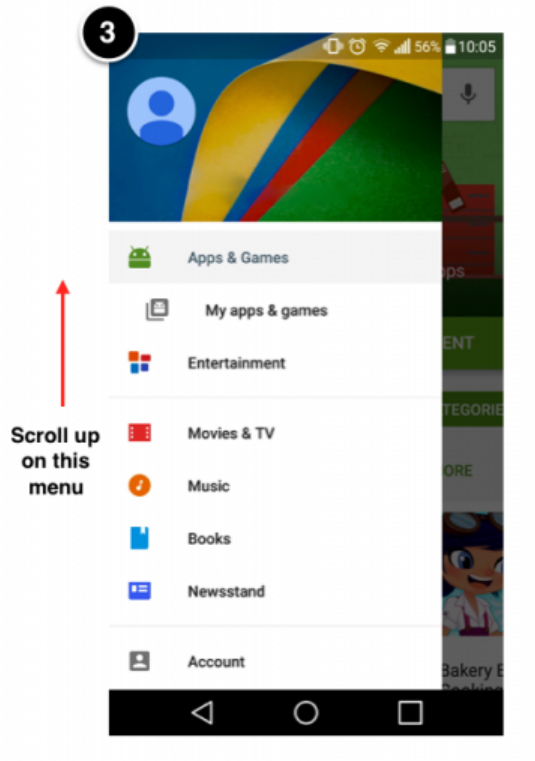
1.



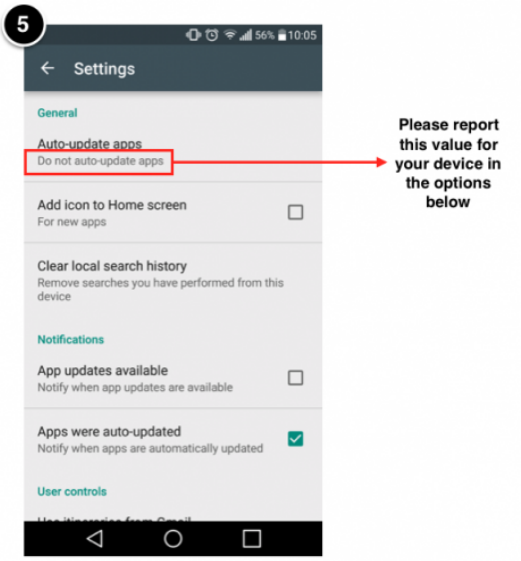
2.



3.



5.

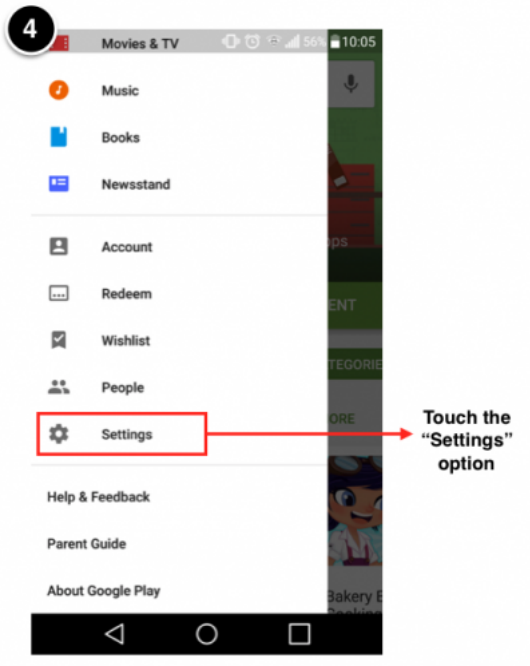


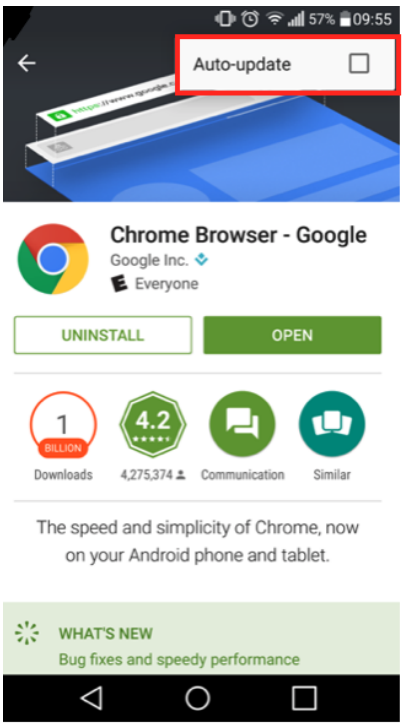
Please report the text in image (5) for your device:

1. Do not auto-update apps.
2. Auto-update apps at any time. Data charges may apply.
3. Auto-update apps over Wi-Fi only.
4. I don't know

2. The Google Play Store allows certain apps to be updated manually. For example, the following images describe how by deselecting the Auto-update checkbox, the Google Chrome app will no longer be auto-updated. [Only shown if the answer to the previous questions is (b) or (c)]

4.

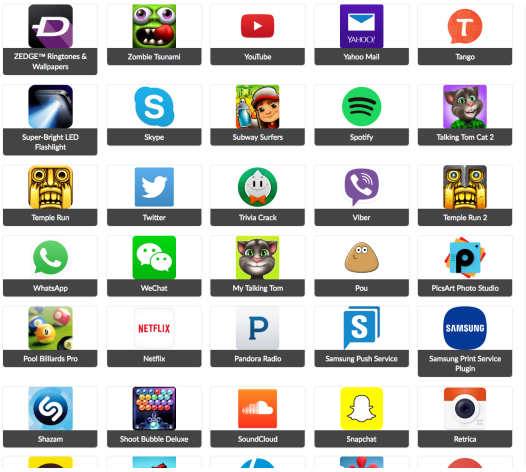




Do you manually update certain apps in the manner shown above?

1. I do not manually update any of my apps in this manner
2. I manually update some of my apps in this manner
3. I manually update most of my apps in this manner
4. I don't know

3. The following is a list of the most downloaded Android apps from the Google Play Store. From this list, please select ALL the ones you have installed on your Android phone. List taken from [46].



For a maximum of 10 randomly selected applications from the previous question:

1. Assuming no data charges apply, how comfortable are you setting security updates to automatically download and install for the following apps? [0 - 100]
2. Assuming no data charges apply, how comfortable are you setting NON security updates to automatically download and install for the following apps? [0 - 100]
3. How frequently do you use the following apps? [Several times a day (5) - Less often (1)]
4. How trustworthy do you feel are the following apps? [Not at all trustworthy (1) - Extremely trustworthy (5)]
5. How satisfied are you with using the following apps? [Not at all satisfied (1) - Extremely satisfied (5)]
6. How important are the following apps to you? [Not at all important (1) - Extremely important (5)]

C. PART THREE: PAST UPDATE EXPERIENCES

1. Have you ever regretted or had a negative experience updating any software across your devices?
   (a) Yes
   (b) No
   (c) I don't remember
2. The following are some reasons why people regret installing updates. Please check all the reasons that have caused you to regret updating your software. [Only shown if the answer to the previous questions is "Yes"]
   (a) The update introduced new bugs in the software.
   (b) The update changed the user interface.
   (c) The update used up a lot of data.
   (d) The update took more time to install than I expected it to take.
   (e) The old version of the software worked better than the updated one.
   (f) Other - Write In

D. DEMOGRAPHICS

1. What is your age? [Write In]
2. What is your annual household income?
   (a) Less than $25,000
   (b) $25,000 to $34,999
   (c) $35,000 to $49,999
   (d) $50,000 to $74,999
   (e) $75,000 to $99,999
   (f) $100,000 to $124,999
   (g) $125,000 to $149,999
   (h) $150,000 or more
   (i) Prefer not to answer
3. What is the highest education level you have completed?
   (a) No High School
   (b) High School Graduate
   (c) Some College
   (d) Bachelor's Degree
   (e) Associate's Degree
   (f) Master's Degree
   (g) Doctoral Degree
   (h) Professional Degree (e.g., MBA, J.D.)
   (i) Prefer not to answer
4. What gender do you most closely identify with?
   (a) Male
   (b) Female
   (c) Other
   (d) Prefer not to answer