DEVICE-SPECIFIC MENTAL MODELS OF SECURITY AND PRIVACY

by

Jacqueline White

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2024

Approved by:

Dr. Heather Richter Lipford

Dr. Cori Faklaris

Dr. David Wilson

Dr. Jiang (Linda) Xie

ABSTRACT

JACQUELINE WHITE. Device-specific mental models of security and privacy.
(Under the direction of DR. HEATHER RICHTER LIPFORD)

People adopt security technologies and make security decisions based on their perceptions of what risks they have, and what things they can do to protect their devices and their information. We refer to these perceptions as mental models. People rely on their mental models to decide how to use their computing devices and the consequences of these actions. Understanding why users make security decisions and addressing the misconceptions in their mental models, specifically regarding security risks, can help prevent security mistakes made by users and help us determine how to help users make good security decisions. This dissertation explores how users perceive security risks, why they make security-related decisions, and where they have misconceptions. In my dissertation, I examine how users' mental models of security and privacy differ by device platform, how that impacts how people use and interact with applications on each platform, and how user's mental models can be used to influence adoption of good device security practices.

In this dissertation, I present the results of three user studies exploring user mental models of security and privacy and how users need an increasing awareness of security risks and measures across all types of computing platforms in order to adopt appropriate practices to protect themselves and their information. While existing research on mental models of security and privacy has been conducted on a variety of device platforms, this work has been primarily focused on identifying mental models of security and privacy which apply to computers and smartphones, explaining how the risks users perceive with a device influence the actions they take to protect themselves from known security risks, such as viruses and data sharing.

However, there is a lack of research into the mental models of security on other

device platforms, particularly tablet-based device platforms. The overarching purpose of my studies are to determine how users' mental models of security and privacy differ by device platform and understand how the relationship between mental models and user behavior affects users' interaction with each device platform. The study of this topic addresses a phenomenon in the field, explained by Wash [50], which is that users use mental models to decide how to use their devices and the consequences of these actions. Understanding why users make security decisions and addressing the misconceptions in their mental models, specifically regarding security risks, can help prevent security mistakes made by users. These mistakes could result in data being collected without the users' awareness, or their personal information, files, money, and/or data being stolen or compromised due to risks such as virus, hackers, or phishing attacks.

The studies in this dissertation expand upon existing research by deepening the understanding of device-specific mental models and their effect on device-specific security behaviors through an interview-based study and survey-based study of security related mental models across the three primary personal computing platforms- laptops, smartphones, and tablets. Additionally, the third study in this dissertation explores the potential influence of device-specific mental models and nudges in encouraging potential adoption of security tools on other platforms based on existing adoption of the tool on a traditional computing device.

Results of the first study indicated users had the most detailed and nuanced perceptions of risk and security behaviors with laptops, while mental models of smartphones and tablets were under-developed, leading to fewer security practices. Similarly, results of the second study indicated that the mental models and perceptions in the first study existed on all three platforms, though they varied in their prevalence. Additionally, the second study indicated that while adopted security behavior(s) are generally consisted across all three platforms, regardless of the user's device-specific

mental models, their adopted security tools did differ with more tools being adopted on traditional computing devices. The results of the third study indicated that nudges may be effective in encouraging adoption of security tools on other devices, particularly with motivators and calls to action informed from existing device-specific mental models.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Mental models are "mechanisms whereby humans generate descriptions of system purpose and form, explanations of system functioning and systems states, and predictions of future system states" [49]. In other words, mental models are users' internal perceptions of how a system works, which influences their interactions with their devices and computing systems. When humans are faced with unfamiliar situations or concepts, they apply analogies to translate understanding of one domain to another [44]. Users apply mental models to any type of system and these mental models affect their behavior. For example, users' mental models of a door handle affect whether or not they attempt to push or pull the door open. When people see a door with a bar, or a flat plate, their mental model is that the door pushes open. However, when people see a door with a handle, their mental model is generally that they should pull the door open. When users encounter a system that differs from their mental model, their behavior often does not conform to expectations, resulting in errors. In the example of the door handles, when users encounter a door with a bar that they must pull open, they may first try to push the door before realizing that they door does not operate congruent to their mental model.

Mental models are developed as people interact with devices and through the mental models of others. Media stories, security training, stories from friends and family, and individual experiences of security compromises help develop mental models [44, 50]. As a result, these mental models differ by application and device. Additionally, as users interact with applications, they develop mental models about what the software is doing and can do, so services that users never encounter usually never become a part of their mental model of the application [44]. When applied to computing systems,

mental models can influence users' behavior and perceptions of risk, resulting in an influence on their computer security or data privacy mechanisms, which is the focus of this dissertation. These mental models influence users' trust and behavior when interacting with applications and how users perceive their security risk levels [35].

This perception of risk is one of the key factors that determines the measures users take to protect their security and privacy on their devices, such as the installation of security tools on their device or the adoption of good security practices. One such example would be users' mental models of security regarding the effectiveness and need for antivirus software on their device. Depending on their perceptions, users may or may not install antivirus software on each of their devices. Additionally, they may install antivirus software on one device, such as laptops, and not on others, such as a smartphone, due to perceptions such as a lack of risk from viruses on smartphones and/or the lack of effectiveness of antivirus software on smartphones. Helping users modify or expand their mental models can help users adopt better computer security practices after understanding the risks they face and how various security applications and practices can help protect them and their data [44].

In a more general sense, mental models have been used in the field of human computer interaction to improve the users' experience with applications, both from the user's standpoint and the design team's considerations. Qian et. al explains, "There are two mental models that must be distinguished: a user's mental model, which refers to what an end user believes about a system [Nielsen 2010], and a designer's mental model, which refers to the conceptualization of the current system, is mostly invented by a system's designer [Wilson and Rutherford 1989; Staggers and Norcio 1993]" [39]. Understanding how users' behavior varies by device platform has been used to inform software developers' design of devices and applications to meet the expressed preferences of users for the respective platform. For example, understanding users' existing mental models can help designers to understand the effectiveness of

design updates and modifications as well as the usability of applications [55].

Additionally, understanding users' device specific mental models of security can be used to educate them about the security and privacy risks associated with each device platform and the appropriate security mechanisms that should be utilized to protect their data and their devices. Users are generally trained in specific security practices at their workplace, however smaller educational messages could be shared with users through methods such as social media platforms, news sites, and friends and family members. Utilizing users' mental models when creating educational messages will improve the effectiveness of the messages by building upon users' existing understanding of how devices work and their perceptions of their vulnerability to security risks on each device platform. To educate users regarding security and privacy vulnerabilities, designers and educators should consider their mental models in order to build upon them and correct misconceptions [44, 51]. Speaking to these mental models will give value to why users should emulate desired security behaviors. Additionally, when educators are able to explain risks to users so that they understand them, they are more likely to modify their actions to address the security risks they face.

There are some important gaps in the current research of mental models, namely that they have been primarily studied on traditional computing devices with more recent but limited exploration into the mental models of smartphone devices. There is still a significant lack of research into the mental models of tablets, more relevantly, the security-based mental models of tablets. Additionally, there is also a lack of research into the overlap and relationship between users' device-specific mental models of security and on users' device specific behaviors. Mental models of security and privacy on smartphones and traditional computing devices have been studied on their respective platforms but not compared for commonalities and potential effects on device-specific security behaviors, except in some instances where specific applications were being explored. However, even those instances were not exploring the mental

models of security and privacy of the device platform but rather a system which is used on that platform.

Seeking to address this gap in research, this dissertation identifies the mental models of the three main device platforms- laptops/desktops, smartphones, and tablets, to compare and contrast users' existing mental models and the adopted security tools and behaviors on the different device platforms. This dissertation discusses three research studies that were conducted to identified mental models of security on these three device platforms, how they compare to each other, and the potential connection between the similarities and differences of mental models of security on different platforms and their connection to the adoption of security behaviors on each device platform. Additionally, this explores how utilizing the commonalities in and addressing misconceptions in device-specific mental models can be used to encourage the adoption of security tools and behaviors across platforms. This dissertation does not address other personal computing devices such as smartwatches and smart home devices since their function and utilization is very different compared to traditional computing devices, smartphones, and tablets and thus would have additional considerations when making a comparison.

1.0.1 Research Questions

The guiding research questions are as follows:

- RQ1: What are mental models of security on various device platforms and how are they similar or different?
- RQ2: How do the perceptions of risk and security mitigation strategies relate to each other?
- RQ3: How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform?

- RQ4: How can you increase awareness of risk and effective security mechanisms on different platforms based on the perceptions on an existing platform?

1.0.2 Thesis

Mental models of security and perceptions of risk vary by device platform, which correlates with users adopting both similar and different security behaviors on each device platform. Mental models of security from one platform can be used to inform perceptions of risk and mitigation strategies as well as practiced security behaviors on another device platform.

1.0.3 Contributions

This dissertation is composed of three studies that identified users' existing device-specific mental models and tried to understand how those mental models might be playing a role in influencing security behaviors. The first study identified five novel mental models of security which exist for laptops/desktops, smartphones, and tablets. Additionally, it identified supporting perceptions of security and privacy for each of those mental models and variances in prevalence of those perceptions across the device platforms. The first study also identified some device specific behaviors which seemed to correspond to a device-specific prevalent perception of security, such as the increased reliance on security tools on laptops with the increased perception on laptops/desktops that application-based security tools are needed to protect the device. While mental models of security have been explored on devices, there is little exploration into the commonalities and differences in mental models across devices, especially mental models of security which have varying influence on security behaviors depending on the platform.

The research questions for Study 1 are:

- RQ1.1: What are users' mental models of security on laptop/desktops, smartphones, and tablets?

- RQ1.2: What are the similarities and differences in perceptions of security risks across the three platforms?

- RQ1.3: What are the similarities and differences in security behaviors on the three platforms, and what do these behaviors indicate about the mental models users have for each platform?

Study 2 investigated whether the mental models of security and supporting perceptions identified in Study 1 could be generalized and were still present in a larger population. Furthermore, Study 2 identified device-specific similarities and differences in the perceptions of security identified in Study 1 were also present in a larger population. Study 2 also identified 8 supporting perceptions which had statistically significant variation across the different platforms. Additionally, Study 2 attempted to correlate the existence of a mental model on a device with users' stated adopted security tools and behaviors. However, any potential correlation was not found to be statistically significant. For this study, we also selected the six factors which appear the most frequently and consistently across various behavior prediction models- cues to action, perceived severity, benefit of action, cost of action, self-efficacy, and ease of use [21, 16, 12, 38, 17, 42]. These factors were evaluated for device-specific similarities and differences which might provide context or outside motivations for device-specific security behaviors.

The research questions for Study 2 are:

- RQ2.1: What are the similarities and differences in mental models of security by device platform?

- RQ2.2: What are the similarities and differences in the factors influencing security behavior on different device platforms?

- RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms?

Study 3 provided a method of addressing a gap in users security awareness observed in Study 1. Specifically, it was noted in Study 1 that participants have a lack of awareness regarding potential security risks, particularly on smartphones and tablets, and the appropriate measures to address those risks. However, it was also observed that users have more developed awareness of risks and security mechanisms on laptops. As a result, this study designed two nudges which were effective in prompting user-stated intent to install antivirus software on a smartphone through a notification in existing antivirus software on laptops. Additionally, this study identified user stated motivations for installing existing utilized security mechanisms on one platform, specifically laptops, on other platforms, specifically smartphones. Some of these motivations were rooted in two of the mental models of security identified in Study 1, indicating the potential effectiveness of these mental models in prompting desired security behaviors. Lastly, this study identified user stated guidelines for designing effective nudges which will communicate the necessary information to encourage installation of the mobile version of the antivirus software.

The research questions for Study 3 are:

- RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform?
- RQ3.2: What are the user suggested design guidelines for such a notification to encourage attention and adoption?

Overall, this dissertation identified and explored the similarities and differences of users' mental models of security and privacy for laptops/desktops, smartphones, and tablets and their influence on users' security behaviors. These contributions are summarized in Figure 1.1.

In this dissertation, five mental models of security were identified with multiple supporting perceptions each. While these mental models of security and perceptions

Research Question	Relevant Study Research Questions	Contributions/Findings	Relevant Sections
RQ1: What are mental models of security on various device platforms and how are they similar or different?	• RQ1.1: What are users' mental models of security on laptop/desktops, smartphones, and tablets? • RQ1.2: What are the similarities and differences in perceptions of security risks across the three platforms? • RQ2.1: What are the similarities and differences in mental models of security by device platform?	Identification of 5 mental models of security with supporting perceptions	Section 3.4.3
		Identification of variances in prevalance of these mental models and perceptions of security on different device platforms	Section 3.4.3 Section 4.3.2
		Identification of similarities in prevalance of these mental models and perceptions of security on different device platforms	Section 3.4.3 Section 4.3.2
		Partially support the alternate hypothesis HA 2.1: There are statistically significant variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.	Section 4.3.2
RQ2: How do the perceptions of risk and security mitigation strategies relate to each other?	• RQ1.3: What are the similarities and differences in security behaviors on the three platforms, and what do these behaviors indicate about the mental models users have for each platform? • RQ2.2: What are the similarities and differences in the factors influencing security behavior on different device platforms? • RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms?	Identification of device-specific similarities and differences in security tool adoption	Section 3.4.5 Section 4.3.3
		Identification of device-specific similarities in security behavior adoption	Section 3.4.5 Section 4.3.4
		Identification of the four most common factors influencing security tool adoption across all three device platforms	Section 4.3.3
		Identification of the five most common factors influencing security behavior adoption across all three device platforms	Section 4.3.4
RQ3: How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform?	• RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms? • RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform?	Designed two nudges to encourage adoption of antivirus software on another device	Section 5.2.2 Section 5.3.4
		Identified user stated motivations for adopting security behaviors on another platform based on two previously identified mental models of security (RQ1)	Section 5.3.2
		Partially support the alternate hypothesis HA 2.2: There is a correlation between some of the device-specific mental models and the adoption of security behaviors on each device platform.	Section 4.3.5
RQ4: How can you increase awareness of risk and effective security mechanisms on different platforms based on the perceptions on an existing platform?	• RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform? • RQ3.2: What are the user suggested design guidelines for such a notification to encourage attention and adoption?	Designed two nudges to encourage adoption of antivirus software on another device	Section 5.2.2 Section 5.3.4
		Identified user stated guidelines for designing effective nudges to increase awareness of risk and security behaviors on other platforms from a different device	Section 5.3.3
		Identified user stated motivations for adopting security behaviors on another platform based on two previously identified mental models of security (RQ1)	Section 5.3.2

Figure 1.1: Summary of dissertation findings and contributions.

generally exist on all three device platforms, their prevalence and influence on security mechanism and behavior adoption differed. As a result, the mental models of security identified in Study 1 and supported in Study 2 provide a start for understanding the differing levels of awareness and perceptions of security and privacy on each device platform influence not only what applications are used on the device, but also the security mechanisms used, or not used, to protect the device. Finally, the nudges designed in Study 3 provide a potentially effective method of utilizing device-specific mental models of security to encourage desired device-specific security behaviors.

CHAPTER 2: RELATED WORK

Mental models are internal models that users create to reason about and understand concepts in the world. Originally a common term in cognitive science, computer science researchers have been studying the mental models of non-expert users to learn how to improve communication with them, how to educate users about proper security and privacy practices, and how to improve interfaces [6]. These mental models describe how a user thinks about a problem or how they think things work. However, mental models of digital technologies can be more challenging to form and use than mental models of the physical world.

As Blythe and Camp explain, "When reasoning about simple physical domains these models typically match the structure of the domain and humans' reason about future events through simulation. When they are applied to more complex domains, such as when making decisions about medical treatments or computer security, these models are more likely to be incorrect or incomplete, bearing a looser relation to the structure of the real-world situation, much of which may be unknown to the human reasoner" [6]. As a result, users are more likely to develop misconceptions in their mental models of complex domains, such as device security and privacy. Regardless of these potential misconceptions, mental models are used by users to decide which actions to take and to understand the possible consequences of these actions [50]. Thus, a major focus of studying mental models within computing, and in particular, computer security, is identifying the misconceptions and incorrect assumptions that people have in order to address them and help them to understand the potential security and privacy consequences of their behaviors, particularly security behaviors.

Mental models have been studied in a variety of fields within the broad umbrella

of human-computer interaction. Some of these fields include computer accessibility, such as how to help blind users effectively use the Internet, computer usage for users of different ages, and trust in AI tools [1, 13, 34]. Despite the broad applicability of mental models to various fields, the general purpose of studying mental models is to understand both how users think and behave for goals such as improving interface design and communication of computer concepts, such as good cybersecurity practices [44, 55].

In general, learning about mental models can help software developers design more effective software to prevent common security mistakes and improve the usability of the software. Understanding how users make security decisions and the security problems that result from these decisions or why they choose to ignore suggested security advice can help developers design software targeted towards preventing security problems that result from common security mistakes and misconceptions made by users [50]. Additionally, understanding user's mental models helps designers to build more effective interfaces that are tailored to how users understand how technology operates [2, 22]. Mental models also improve communication with users by allowing experts or instructors to utilize scenarios and terminology that is familiar to users or already understood by users [6].

Incorrect mental models lead to poor decision making or poor computer security practices. One example of this is that users usually have a general understanding of concepts, such as that viruses cause harm to their computer and that they can use an anti-virus to help protect their computer and their data. However, they do not fully understand the full risks of viruses, and therefore do not utilize anti-virus software to its full, or recommended, protective and preventive capabilities [50]. However, even if users have incorrect mental models of security threats or computer systems, or mental models that are not technically correct, their mental models can still result in good security practices if they are properly developed and can allow users to make better

security decisions than would be made without a mental model [6, 51].

As Wash and Rader explain, "to change people's mental models, we need to do two things: 1) Identify how people form these mental models, and how we can influence them. 2) Identify which models are associated with what security behaviors, so we know which models we want home computer users to possess" [51]. When users ignore security advice, it is often for logical reasons, such as the high cost of users' time and effort offsetting the benefits of the security measure [51]. Additionally, users form mental models and adopt security behaviors based on the stories they hear from other people. Understanding the impact of stories and the resulting sharing of knowledge and behaviors is integral in guiding users to alter their mental models and behaviors to be more secure [51].

When educating users who have no pre-existing mental model, designers should strive to build the correct mental model by retaining their listener's attention and addressing their pre-existing assumptions and knowledge of the topic. Traditional training methods, such as having an expert teach a group of home computer users, will not work here, both because these methods are intractable and expensive, and because previous work suggests that mental models are best transmitted through stories from friends and other "people like me." A cost-effective method of improving home security therefore is to get home computer users to train each other and spread good mental models amongst themselves [51].

When educating users who have developed a mental model of a topic, but it is limited, designers should attempt to build on their current mental model by pulling from what they already know and providing additional links, examples, or explanations to expand their understanding and elaborate on their current mental model with additional correct information. Supporting this new information with current correct information, not only supports their current mental model but also smooths the integration and development of their mental model by allowing the individuals own

beliefs to support their education [49].

A related topic to mental models is risk communication - the way in which potential risks are provided to users. Risk communication helps to build mental models, often through the use of metaphors. Camp outlined a set of common metaphors used to understand and communicate computer security risk. These 5 models are physical security, medical, criminal, warfare, and market [4, 11, 49]. Each model can be used to communicate or understand a different area of risk. For example, the medical model of risk communication can be used to understand and communicate the risk posed by computer viruses or malicious code by explaining the effect and behavior of this code as an infectious disease [4]. However, even within these 5 categories of risk models in computer security, there is discrepancy noted in how users conceptualize and verbalize the differences in these mental models based on their level of expertise [4]. One primary example can be illustrated by users' understanding of passwords. Experts tend to understand and verbalize passwords using a criminal risk model by comparing them to credit card numbers that can be stolen. Comparatively, non-expert users tended to understand passwords using a physical risk model by comparing them to a key that can be lost [4].

Mental models have been studied in the context of various domains and systems, however, the primary domain of mental models referenced in this dissertation are those of security and privacy. Privacy has a number of definitions but can be thought of as control over access to information [5, 31, 35] whereas security is the enforcement of that access to information. While these two are defined differently, many users take a holistic view of security and privacy and conflate the two and think of them together. For example, users may think of encryption, a security technology, as being something that protects the privacy of their information and describe a range of privacy and security perceptions when discussing the use of encryption. Thus, the two words, and accompanying contexts will be regularly used together within this dissertation.

2.1 Common Mental Models in Computer Security

Mental models are specific to the user and to the privacy or security issues they involve. Additionally, mental models likely differ across different cultures. Most research has currently been conducted on Western adult audiences and is therefore not all that diverse. However, there are a few additional audiences that have been studied, such as children [31] and home computer users in Germany [28]. These various audiences show that mental models do occasionally differ based on various factors, such as culture and age, however, there are still similarities and common mental models within broad populations [28, 50].

For example, Kauer et. al replicated a study in Germany that was originally done by Wash in the United States on home computer users. Kauer et. al found very similar results as Wash, with 11 mental models of computer security that included all 8 from Wash with minor differences. This study shows that while there are differences in mental models of security across different cultures, there are also similarities. These mental models, along with other common mental models and categories that exist in literature, can be grouped into four main categories- mental models of people who cause or conduct security or privacy problems, mental models of software problems, people's actions and behaviors regarding their own security and data privacy, and a common perception that users are not at risk.

2.1.1 Mental Models of People who Present Security Risks

The first category of mental models are the mental models users have regarding the people who cause or conduct security or privacy attacks. Many of the mental models in this category involve hackers as general perpetrators of crime, though with various motivations, who are responsible for doing bad things on the internet [50]. The first of the hacker-centric mental models is that of "Hackers are digital graffiti artists" [28, 31, 50]. Individuals with this mental model view hackers as people who

want to prove they can execute the crime, but they do not cause serious harm to individuals or society.

The second hacker-centric mental model views hackers as contractors who support criminals. Individuals with this mental model think of hackers similarly to those with the previously mentioned mental model, however the purpose of these hackers is to steal personal and financial information. Individuals with this mental model view hackers as interested in financial gain, and thus focus on being aware of where they make purchases or provide personal information [50].

The third hacker-centric mental model is that hackers are burglars who break into computers for criminal purposes. Similar to the previous mental model, individuals think these hackers are motivated by financial gain. However, individuals with this mindset view hackers as more focused on identity theft rather than stealing large datasets with personal or financial information. Individuals with this mental model do take steps to prevent themselves from being victims, however they do not have a good model of how hackers choose victims and simply see the choices as opportunistic. The fourth hacker-centric mental model is that "Hackers are governmental officials" [28]. Individuals with this mental model view the government as hackers who gain information, but only when there is suspicion of crime.

Researchers have also uncovered other mental models related to people who conduct attacks, which are more specific to certain kinds of risks. These include perceptions that "Stalkers get information online but can also continue their activities offline", "Spammers advertise by means of unsolicited messaging which is perceived as a type of denial-of-service attack", and that "Marketers invade individual privacy by surreptitiously collecting information about activities, purchasing patterns, etc." [28]

2.1.2 Mental Models of Software

Another set of common mental models explains the cause of software problems. Often, these software problems are thought to be the result of viruses. The first of

these virus-centric mental models understand that viruses are bad, but users only have a high-level understanding of what they do and the issues they pose to privacy and security. Users with these mental models generally believe that they are "immune" to getting viruses for various reasons such as their behavior or the type of machine they use, and thus do not need to take any precautions to protect themselves, such as downloading anti-virus software [50].

The second virus-centric model is that viruses cause mischief. With this mental model, individuals believe viruses cause annoying problems that occur with their devices but they are not very aware of how viruses are created [50]. Users with this mental model believe they are vulnerable to viruses when they click on infect links or visit infected sites. As such, they try to avoid visiting what they consider "bad parts of the Internet" as well as clicking on sketchy looking links [50].

The third virus-centric mental model is that viruses support crime. With this mental model, individuals believe viruses are used to steal personal and/or financial information. They view viruses as being passive on their computers as they collect information only and are thus hard to detect. As such, users with this mental model keep their anti-viruses up-to-date and run frequent scans to uncover the otherwise undetectable viruses. However, since they do not believe the viruses can harm the computer, they don't perform backups of their systems [50].

The last virus-centric model is that viruses are buggy software. This mental model sees viruses as software that is intentionally sent to computers to cause them to exhibit problematic behavior such as crashing or not starting. As such, users with this mental model do not see the need for anti-virus software that removes viruses as they believe it is more important to avoid getting the virus in the first place by not downloading infected applications or clicking on infected email attachments [50].

2.1.3 Mental Models of User Behavior

Researchers have also examined mental models that describe how users perceive the actions that they can take to protect themselves. This research explored how users interact with systems or programs, such as encryption and popup blockers to protect their privacy while they interact with their devices. However, this category is different from the following category in that it focuses on what users personally do to protect themselves, which does sometimes mean they don't take any other action or precaution other than the built-in system protections and adopting a precautionary approach to clicking on links or bypassing security warnings [23, 41]. Most of the perceptions examined are very specific to a particular technology or platform. Thus, specific mental models and perceptions of user behaviors are detailed in the following section on specific security-related domains.

2.1.4 Risk Exemption Mental Models

Finally, much research has identified why individuals believe they are not at risk for a variety of reasons. One of the frequently discussed mental models is that "Hackers are criminals who target big fish" [28, 41, 50]. Individuals with this mental model do not believe they are at risk of privacy breaches because they are not rich or important enough for hackers to take the time to target their information. Another similar mental model is that "Hackers are stakeholders with individual and opportunistic purposes" [28]. Individuals with this mental model also believe they are not at risk, but they think it is because hackers are more interested in targets that will garner a larger media coverage.

Another commonly reported perception is that an individual's privacy is not at risk because their information is not sensitive or cannot be used against them [22, 23, 41, 53]. Because individuals with these mental models do not think they are at risk, they often do not take any, or sufficient measures, to protect themselves and their data.

2.2 Mental Models of Systems

Mental models describe how users' think systems work, and thus specific mental models are particular to the type of system. Mental models of different systems explain how users' understand concepts such as how information travels between people on various systems [27, 53], how certain security protections work [22, 53] or how data is stored and collected by devices [45, 56]. While these mental models are often used to understand various systems and technical concepts, including how they work and the role they play in protecting users' privacy, these mental models can also be used to explain why users believe they are at risk for security or privacy breaches.

One example that has been studied is users' perceptions of multi factor authentication. Identified mental models are influenced by experience, dividing the mental models into expert and non-expert mental models. For example, studies have determined that experts treat multi-factor authentication as additional verification whereas non-experts treat multi-factor authentication as a security service [11]. One key difference between these two mental models is that non-expert users aren't clear how multi-factor authentication protects them, only that it does [11]. The section below explains some of the common mental models for well-known systems including the internet, encryption, and smart home devices.

2.2.1 Mental Models of Encryption

Users have mental models about everything. One common domain where this has been studied is encryption. Encryption has been understood to add a layer of security and confidentiality to messages and information, however it is also associated with a usability burden which often affects users' willingness to utilized encryption or gives them the impression that encryption is excessive except for the most important of secrets [22].

Encryption is used in a variety of applications, such as https, secure messaging, and

mobile devices [2, 53]. Regardless of how encryption is used, users tend to have the general perception of encryption as some sort of algorithm that is used for security and privacy purposes [2, 53]. Building upon that perception of what encryption is and what its purpose is, users have a variety of mental models regarding how encryption works. The most basic mental model is that encryption is used to regulate access and acts as a type of barrier in credential-based access control [53]. Users then build on this perception with the additional understanding that encryption is a process which transforms data rather than acts as a wall. However, even with this additional understanding of what encryption does, users with this mental model do not understand how it works [53].

More advanced mental models have a foundational understanding of how encryption works, namely that it transforms data during the process [53]. While the understanding of how this transformation occurs varies in both the type of operation(s) performed and the difficulty, this understanding of a clear process by which the original data is transformed into the encrypted output distinguishes users with these mental models from those with the previously discussed mental models.

Users use methods they view as secure to share sensitive information. However, depending on their mental model of encryption, they may rely on less secure methods of communication since they do not perceive encryption as being sufficient to protect their information [2]. Additionally, usability issues with encryption software influences users' willingness to implement encryption [2, 23]. As such, understanding user's perceptions of encryption can inform the design of encryption systems so that users are reassured of the effectiveness of encryption and the ease of use to implement encryption as an additional protection, particularly for sensitive information [2].

2.2.2 Mental Models of the Internet

Another security-related domain that has been investigated is the internet and how users think it works. In this domain, there are 2 specific mental models, as discussed

by Kang, et al, in their study of 28 technical and nontechnical participants [27]. The first of these is a simple understanding of the Internet. Users with this mental model understood the Internet as a somewhat simple system whose purpose is to receive and send out data. The participants with this mental model used metaphors to describe how they understood the Internet such as cloud, main hub, or library. Participants who exhibited this side of this mental model only had awareness of organizations and services they frequently interacted with, such as Google or financial services. They also tended to use made up terminology and lacked awareness of the underlying connections and layers that make up the Internet.

The other mental model users exhibited was that of an articulated technical model of the internet. Users with a strong technical background did not have such a simple understanding of the Internet and how it works. Instead, they viewed the Internet as a complex system with many pieces of hardware and connections as well as multiple layers at times. These participants were able to use accurate and detailed terms to describe the Internet and these layers as well as were aware of more organizations and services than the participants with a simpler mental model.

However, regardless of their mental model, users understood that the Internet connects computers and supports communications. Additionally, although it was not directly asked about, many participants expressed awareness or concerns about security and privacy on the Internet [27]. In their comments, participants indicated they have varying awareness and attention to security and privacy, specifically in 4 main areas: concern about private vs. public spaces, protection mechanisms, trust, and the perception of security on mobile phones vs. computers. The first three topics are explained further below, however the last topic will be discussed more in a later section.

In addition to their perception of how the internet works, participants in the study also had perceptions on how data was managed on the Internet. Many participants

understood that their data went to the servers of the company that was providing the service [27]. However, they were not sure if the information was stored permanently, especially in cases when the original website that collected the data was deleted. Additionally, many participants understood there were partnerships between companies, though they were not aware of who their data was sold to. Their awareness of these partnerships was the result of seeing personalized advertisements and services as well as articles they read discussing these partnerships.

Regardless of who they thought had the data, the participants had a generally broad list of entities they thought could see their data on the Internet. The general list of entities in decreasing order of frequency mentioned included the companies that host the website, third parties, the government, hackers (such as man in the middle attacks), other people, and Internet service providers [27]. One key difference between the two mental models was that the articulated technical model expressed awareness of more threats than participants with a simple model.

Many participants stated they were aware of various protective measures for protecting their data on the Internet, however many of them did not use them. Kang et al discovered four primary reasons that users did not use protective measures on the internet. First, the participants were not worried about their information being accessed or monitored. Second, participants thought the protective measures would interfere with the effectiveness or convenience of the services they use. Third, the poor usability of privacy protection tools or software directly influenced users' willingness to use protection measures. Lastly, participants expressed a feeling of helplessness or lack of procedural knowledge that caused them to not implement protection measures.

While these reasons were not directly correlated to one of the two identified Internet mental models, they do correlate to some of the mental models discussed previously. For example, users who are not worried about their information being accessed or monitored may also have the "big fish mental model" which is the perception that

users are not at risk because there are other targets of more value that will be targeted instead of the user. This supports the conclusion that users possess multiple mental models, and these mental models directly influence their understanding of how services work and the security risks they face as well as how they respond to any perceived risks.

2.2.3 Mental Models of Smart Home Devices

Smart home devices are a change from traditional computing devices, in that there are many more of them, each collecting and utilizing different kinds of information that is collected in a person's home. This raises a number of additional privacy and security concerns. Thus, a number of researchers have examined user's perceptions of how smart home devices should be used and their concerns about their data privacy such as how the data is stored and how the data is used [56, 57].

Two foundational smart home mental models resemble the previously discussed mental models of the Internet. The first model is a service-oriented mental model of smart home devices. Users with this mental model have a general understanding of how the smart home devices communicate with each other within the home network, but that understanding is limited to the interaction between the smart home controller, such as Google Home, and the other smart home devices, such as lights [45].

The second mental model is an advanced mental model of smart home devices. Users with this mental model have a more complex understanding of how communication works between smart home devices than users with the first mental model, particularly that other devices and components, such as routers and ethernet cords are involved in the communication between devices. Additionally, users with this mental model often set up their devices themselves and even customized their settings [45].

In general, users with the second mental model were more informed of the complexity of data flows between devices and servers in the cloud [45]. However, the degree to which they understand how their data is stored does vary based on their mental model.

While users generally had a good conception of much of the information that devices collect, they were generally uncertain about how their data is stored, used, and shared.

Users expressed three primary uses for the data collected by their smart home devices beyond the functioning of the device- personalized advertising, product improvement, and market needs research [45]. Also, they expressed understanding that several entities had access to their data, primarily the manufacturer of the device, third parties or advertisers, parent companies, subsidiaries or affiliates of the manufacturer, hackers, legal organizations, the manufacturer of the app used to control the smart home device, and other people who have accounts on the device [25, 27]. Their trust in the company that provides the device and services as well as whether the device records audio and video and their perception that smart home devices are for convenience influences their data privacy concerns, as their focus on the use of the product and the benefits of using the device outweighs their concerns of privacy [56].

2.3 Mental Models by Device Platform

The mental models discussed in the previous section provided an overview of some of the common types of mental models and examples of specific mental models in these categories as well as a more in-depth look at the mental models of a few specific domains. Most of these mental models were determined using evaluations of perceptions of risk on and usage of desktops or laptops. However, there are additional device platforms which have different purposes and functions, and thus likely different mental models. The three platforms discussed below are laptop/desktops, smartphones, and tablets. These three were chosen for comparison purposes due to the differing ways users utilize these devices while the capabilities are relatively similar. Other devices, such as smartwatches and smart home devices, will not be considered in this section as their function and utilization by users is very different from these three device types.

2.3.1 Laptop and Desktop Mental Models

One of the main domains privacy and security mental models are studied is that of laptop and desktop mental models. The mental models in the previous section above were primarily studied in this domain, and thus describe laptop and desktop mental models. One of the foundational works in security mental models is Rick Wash's 2010 folk models study, which examined common perceptions, and mis-perceptions, of security within a culture [50]. This study identified eight common folk models of home computer security, which were divided into two broad categories regarding viruses and hackers. Each of these folk models is summarized in Figure 2.1. Virus models varied regarding how people thought they caused problems, such in within buggy software or through causing mischief on someone's computer. Hacker models differed in who people thought were causing attacks and why, from teenagers looking to cause mischief, to criminals, to those only targeting "big fish".

As detailed in the previous sections, user's mental models of laptop and desktop vulnerability and purpose tend to include a wide range of mental models due to the varying capabilities of laptops and desktops. However, these mental models do seem to be centered on what could be considered more traditional understandings of computers and vulnerabilities. For example, many of them understood vulnerabilities as coming from hackers or viruses, with users having varying mental models as to their risk level. Additionally, regarding actual software and functional mental models, users tend to either have more simplistic models where they have very general understanding of what the service being provided should do, or a more complex understanding of exactly what the service does and how.

2.3.2 Smartphone Mental Models

Smartphones have a different capabilities and functions compared to laptops and desktops and thus have different mental models associated with their functions and

Folk Model	Summary
Viruses are bad software	General understanding that viruses are bad and should be avoided.
Viruses are buggy software	Viruses are buggy software which cause the worst types of bugs.
Viruses cause mischief	Viruses are created to be annoying and often caught from the "shady" part of the internet.
Viruses support crime	Viruses steal personal information, are stealth, and spread automatically.
Hackers are digital graffiti artists	Hackers are teenage boys showing off for friends but not causing serious harm.
Hackers are burglars	Hackers are looking for personal information in your computer for identity theft but do not cause other types of harm.
Hackers target big fish	Hackers are professional criminals who target rich and important people for information.
Hackers are contractors who support organized crime	Hackers are contract criminals who support organized crime by targeting large databases rather than individual people.

Figure 2.1: List of folk models identified by Rick Wash [50].

their risks. For example, one of the key functions of smartphones is their use of pre-granted permissions to operate apps. However, smartphone users have a number of mental models, some of which are very similar, or identical, to the most common laptop/desktop mental models previously described. The first category of mental models belongs to the category of users who believe they are not at risk. Two mental models in this category specific to smartphone users are "I have nothing to hide" and "I am too unimportant" [30]. Users with the first mental model believe that they are not at risk even if their data is collected, because they do nothing illegal or that they would wish to hide. However, these users do not recognize the other risks that could be associated with their data being collected, such as targeted spear phishing attacks [30]. Similarly, users with the second mental model believe that with data being collected at such a large scale, they are not interesting amongst the crowd of other users and thus not at risk [30]. Another mental model that falls into this category is

"If the company is trustworthy, then it is safe to provide my data to them" [30]. Just like users with the previous two mental models, users with this mental model do not feel they are at risk because they trust the company to protect their data. However, companies can also be victims of hackers, not just individuals.

Another category of mental models belonging to smartphone users involves how users think systems work. Similar to this category of mental models for laptops/desktops, users with these mental models have various understandings of how their phones actually function, and consequently, varying levels of understanding of the resulting privacy vulnerabilities associated with using smartphones. Three examples of this category are the mental models "If my smartphone is secured, my privacy is ensured as well", "Apps from app stores are secure by default", and "Only the data that is input explicitly can be leaked" [30]. As evidenced by these mental models, many users associate smartphones with being relatively secure and their data on smartphones with being relatively safe. However, as is the case of all three of the aforementioned mental models, personal data, both direct input or data stored on the phone, can still be collected by apps and shared with other companies [30].

The last common mental model category shared by smartphone users is that of actions users taken to protect themselves. As previously discussed, there are privacy vulnerabilities associated with using smartphones, one key one being the utilization of private data by apps to complete basic functions. However, smartphone users seem to adopt the mental model that they are unable to do anything to prevent apps and services from accessing their private data [30]. However, there are steps users can take to manage their risk, such as uninstalling unused apps or moving their private data, such as images, to other devices so that apps are only able to access less private data [30].

One of the key attributes of smartphones is users primarily interact with applications and services through singular apps. In other words, instead of accessing Amazon

through a Web browser, users would likely use the Amazon app as its interface is designed to be user friendly on the smaller device screen. When users first download apps for use, they are often asked to grant apps access to permissions needed to utilize the app services. Asking users to accept these permissions when first running or installing the app, can cause them to make incorrect inferences about how and when the app accesses these permissions [52].

However, similar to the mental models users have of computer services, users have also developed perceptions of risk for apps, specifically their access to permissions and data in regard to privacy and security. For example, depending on when and how apps asks for accesses to permissions, users can gain the understanding that granting permission only applies to this instance or that the permission is only for the action they are trying to complete rather than the application as a whole [52].

The most commonly researched mental models thus far have to do with users' perceptions of the risk of smartphone app usage. And while this application does focus on one of the key attributes of smartphones, it leaves the question of how users actually perceive smartphones as a whole and the privacy risks associated with using smartphones compared to laptops/desktops. As users are able to perform similar functions on smartphones, this raises the question of whether or not users perceive the same risks with smartphones as they do laptops/desktops for the same actions and services, and whether their behaviors put them more at risk.

2.3.3 Tablet Mental Models

Currently, there exists little research into mental models specific to tablets. In this review of existing mental model research, all the existing research into privacy and security mental models read was conducted on either smartphones or laptops and desktops. However, tablets are a unique combination of both smartphones and laptops/desktop devices as they have both the portability and app capability of smartphones, but they also have the larger screen size and higher functionality that is

common for laptops and desktops. This raises the question, are users' mental models of tablets a combination of their mental models of laptops/desktops and smartphones, or are they a unique adaption of existing models that users created to understand the functionality and vulnerabilities of tablets?

2.4 Conclusion

Understanding users' mental models provides guidance towards identifying and understanding users' needs for reducing their security and privacy risks. One of the most prevalent user mental models across various domains is that users are not at risk for a variety of reasons. This leads to reduced motivation to practice effective privacy and security behaviors as users do not understand a need for these practices which outweighs the inconvenience of implementing good privacy and security behaviors.

While there exists prior research of mental models, most of this research has been focused on specific device usage, specifically laptops, desktops, and smartphones, or specific system usage on a device. Additionally, there is currently a lack of research on the privacy and security mental models of tablets. While these devices can be used similar to smartphones and laptops, they still have unique concerns and mental models due to their unique design that is a cross between the more portable smartphone and the more heavily functional laptop.

There is also a lack of research on how the mental models of all three devices overlap or differ. While the same applications can be used across all three platforms, we are unable to understand whether users would use the same apps on all three devices without further research into whether these devices are perceived to all have the same level of security and privacy vulnerabilities as well as how those perceptions of these vulnerabilities influences application usage and security mechanism adoption. Thus, this dissertation addresses these gaps in existing research by identifying users' device specific mental models of security, the similarities and differences in these mental models, and the differences in users' security behavior on each device. Additionally,

this dissertation provided two nudges to enhance user security and privacy utilizing the differences in device-specific perceptions of security to prompt desired security behavior adoption.

As such, the guiding research questions for this dissertation are as follows:

- RQ1: What are mental models of security on various device platforms and how are they similar or different?
- RQ2: How do the perceptions of risk and security mitigation strategies relate to each other?
- RQ3: How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform?
- RQ4: How can you increase awareness of risk and effective security mechanisms on different platforms based on the perceptions on an existing platform?

CHAPTER 3: STUDY 1: DEVICE-SPECIFIC MENTAL MODELS OF SECURITY AND PRIVACY

3.1 Introduction

Several prior studies of general security mental models of computing devices have focused around traditional personal computers, identifying that users are primarily concerned with risks of hackers and viruses, with varied levels of understanding. However, users are increasingly using other platforms, such as smartphones and tablets, to access the Internet and perform a variety of digital activities. There have been few studies examining how user mental models are similar or differ across these various platforms, and the impact of those perceptions on the security-related behaviors that users engage in on those platforms.

This chapter is a study of the mental models of security of three different general computing platforms - namely laptops/desktops, smartphones, and tablets. Our aim is to examine the security mental models that are unique to a device platform, as well as perceptions that are shared across all three platforms, and how users' mental models of a device influence their behavior on that device. This study addresses RQ1: What are mental models of security on various device platforms and how are they similar or different, and RQ2: How do the perceptions of risk and security mitigation strategies relate to each other of this dissertation.

Our research questions are as follows for this study:

- RQ1.1: What are users' mental models of security on laptop/desktops, smartphones, and tablets?
- RQ1.2: What are the similarities and differences in perceptions of security risks

across the three platforms?

- RQ1.3: What are the similarities and differences in security behaviors on the three platforms, and what do these behaviors indicate about the mental models users have for each platform?

We conducted a semi-structured interview of 27 undergraduate and graduate students, asking questions about how they use their devices and the security concerns they have regarding these devices. Our results make the following contributions:

1. We provide continued evidence of prior virus and hacking-oriented mental models of security, as well as evidence of adaptions to these mental models.

2. We identify a broader and deeper awareness of security risks and mitigation methods on laptops/desktops as compared to smartphones and tablets.

3. We describe the mental models that are common across platforms regarding platform security, security tools, and risky behaviors, as well as the unique perceptions that support those models on each platform.

3.2 Methodology

Traditional and mobile devices now have the capacity to support many of our everyday digital activities, with both overlapping and different risks based on the platform and how devices are used. While prior studies have examined mental models on laptops/desktops and smartphones separately, none have examined these platforms together to identify how these perceptions are similar or differ, and the impact that may have on security behaviors. Thus, we designed this study to identify these similarities and differences, across all 3 of the common computing platforms. We patterned this study after some of the prior work, [50], with a semi-structured interview study with users who owned at least 2 different devices. Some of the interview questions were based off some of the virus and hacker questions from Wash's 2010 study and the

codebook incorporated the mental models identified by Wash when found. The study was approved by our university IRB. We queried participants on how and why they used different devices, as well as asking specifically about security perceptions and behaviors for each kind of device. Below we detail the interview, our participants, and study analysis methods.

3.2.1 Interview

Participants received a consent form and demographics survey via email, to complete prior to the interview session. Interviews were then conducted via a Google Meet phone number, were audio recorded for transcription, and generally lasted 30 minutes.

Question Category	Question
Background and Inclusionary Criteria	Do you own at least two devices, if so, what? What personal technology devices, such as smartphones or laptops, do you use on a regular basis?
Scenario Based	Which device(s) would you use for [banking transactions, bill payment, online shopping, social media]? Why would you use this/these devices? Why would you not use [device(s)]?
Device-Specific Device Usage	What types of applications do you [primarily use, or would not use] on [device]? Have you ever had security or privacy problems with [device] or the applications used on it? If yes, can you describe what happened? How did you know it was a [virus/hacker/identity theft/other type of concern]? How was it detected? How did you fix it? Do you know where it came from/how you got it? Do you know who did it?* What types of security/privacy issues are you concerned about happening on [device]? Are you worried about [viruses/hackers] on [device]?* If yes, what are you worried [viruses/hackers] will do? What do you do to protect yourself?* If no, why not? What security/privacy measures do you have on [device]?
General/ Hypothetical Device Usage	What types of applications do/would you use/not use on [device platform 3]? Do/Would you have any security/privacy concerns with [device platform 3]? What security/privacy measures do/would you use on [device platform 3]?

Figure 3.1: Complete list of interview questions asked in Study 1.

The full list of interview questions is shown in Figure 3.1. The participants were first asked basic questions to identify the types of devices they own, with the intention of categorizing these devices as a smartphone, laptop/desktop, or tablet, based on the user's definition of that device's type. For example, if the participant owned a chrome book, it would be their own classification of that device as a laptop or a tablet

that would determine its device classification. They were then asked scenario-based questions regarding which devices they would use for some potentially security-sensitive situations, namely banking, bill payment, online shopping, and social media.

The participants were then asked more specific questions about two different devices they own, such as their smartphone and tablet, to determine the specific risks they associate with each device as well as how they use each device. All participants indicated they owned a laptop or desktop, and a smartphone. Thus, for participants who regularly reported using a tablet, we focused on that device as one of their two. This resulted in 22 participants discussing traditional computing devices, 25 participants discussing smartphones, and 7 participants discussing tablets for this portion of the interview. To help determine some of their perceived risks, participants were asked four questions regarding viruses and hackers which were adapted from Wash's 2010 folk model study [50].

Due to the repetitive nature of the questions asked, as needed for comparison of perceptions and behavior between the devices, the detailed questions were only asked for two devices. Thus, we then asked several higher level questions for the third device, with detailed follow-up questions only if the participant indicated experience with a security vulnerability or the usage of a security mechanism. In the case of participants who did not own the third device, a tablet in all cases, they were asked to answer this section as if they hypothetically owned a tablet. In this case, while participants were describing hypothetical concerns or security behaviors with the device, the perceptions influencing these concerns and behaviors were still formed the same way as their mental models for other devices- through experience, stories, and education. As such, their responses reflect their real concerns and security behaviors based on their current mental models of the device.

3.2.2 Participants

Participants were recruited through a Facebook post on the researcher's personal account, and an email announcement sent to students at our university by the university's research organization. Participants were then encouraged to share the information with others who might be interested and asked to do so at the end of the interview. To participate in the study, participants had to be older than 18 years old and own at least two devices from the list of laptop/desktop, smartphone, and tablet. Shown in Figure 3.2, 27 participants were recruited through snowballing and the university listserv, 17 of which indicated they are a student. All but 1 of the remaining participants indicated they had a college degree. Additionally, all but 1 of the participants were between 18-34 years old, with 20 of the participants being between 18-24 years old and 19 of the participants indicating they were female. Using a scale of 1-5, 17 participants indicated they were very comfortable (5) with technology and all participants indicated they were at least moderately comfortable (3) with using technology.

3.2.3 Analysis

After being transcribed, the interviews were coded using Corbin and Strauss' grounded theory method to identify the emergent themes [8]. Using this approach, a three-phase coding strategy was applied to the transcripts - open, axial, and selective coding. In the open coding stage, two coders worked separately to code two of the longest transcripts. They then compared, combined, and refined their codebooks. While most of the codes in this stage were a result of the discovered themes, both coders noted the presence of some of Wash's 2010 folk models [50], resulting in their inclusion into the codebook. During the axial coding stage, the coders applied this initial codebook to 7 additional transcripts.

Afterwards, both codebooks were again compared, combined, and refined. As a result

ID	Education	Race	Gender	Age	Profession	Technology
P1	Some college	Asian	Female	18-24	Student	5
P2	Some college	Asian	Female	18-24	Student	5
P3	Some college	Asian	Female	18-24	Student	3
P4	Bachelor's degree	Asian	Female	18-24	Computer Programmer	5
P5	Bachelor's degree	Black or African American	Female	18-24	Concierge	5
P6	Associate degree	American Indian or Alaska Native	Female	18-24	N/A	5
P7	Associate degree	White	Female	18-24	Student	3
P8	Associate degree	White	Female	35-54	Student	4
P9	Some college	Black or African American	Female	18-24	Nonprofit	3
P10	Some college	White	Male	18-24	Student	5
P11	Bachelor's degree	White	Female	25-34	Nanny	5
P12	Doctoral degree	White	Male	25-34	Student	5
P13	Bachelor's degree	Black or African American	Male	18-24	Business	4
P14	Bachelor's degree	Black or African American	Female	18-24	Sports Nutrition Assistant	4
P15	Bachelor's degree	Asian	Female	25-34	Student	5
P16	Some college	Asian	Female	18-24	Student	5
P17	Some college	Black or African American	Female	18-24	N/A	5
P18	Master's degree	Asian	Male	25-34	Student	5
P19	Associate degree	White	Female	18-24	High School Math Teacher	3
P20	Some college	White	Male	18-24	Student	5
P21	Associate degree	Black or African American	Gender Variant/ Non-conforming	18-24	Unemployed	4
P22	Some college	Black or African American	Female	18-24	Student	3
P23	Some college	Black or African American	Female	18-24	Student	5
P24	Master's degree	Black or African American	Female	25-34	Student	5
P25	Bachelor's degree	White	Female	18-24	Student	3
P26	Master's degree	Black or African American	Female	25-34	Healthcare	5
P27	Bachelor's degree	Asian	Male	18-24	Student	5

Figure 3.2: Demographics of participants from Study 1.

of this iteration, a codebook with 126 codes was created and grouped into categories. The two coders agreed that the codes should be grouped by three overarching categories-

behavior, concerns, and mental models. Within these categories, the codes were further grouped by device platform. As a result, the same code-naming scheme could be used for each device platform, increasing the ability to recognize the similarities and differences between the mental models and perceptions for each device.

Finally, the codebook was used to code the remaining transcripts by the primary researcher during the selective coding process. During this stage, the codes were then split into themes. These themes summarized the main idea of the supporting codes for the establishment of theories and conclusions based on observations of these themes and the comparison of them across devices and categories.

3.3 Limitations

This study has limitations typical of qualitative interview studies, with a small sample size and demographics that are not representative of a more general population. Being that this study was conducted with university students, the population is well-educated and has a heavy interaction with laptops and desktops. Furthermore, participants had more limited usage of tablets than the other two platforms, with many of the tablet discussions being about hypothetical usage or past tablet usage, which may have limited the perceptions reported with tablets. However, clear commonalities and patterns in perceptions and mental models did occur across the devices, indicating saturation did occur in the responses.

3.4 Results

Below we describe the themes that emerged from our interview analysis. We first discuss several general factors as well as the overall expression of folk models throughout the interviews. We then discuss the perceptions on each platform separately, before highlighting the role that trust and confidence played in users' choices in security behaviors.

When reporting the number of participants who had the relevant mental model for

a device, letters are used to represent each device category. Specifically, "l" is used when reporting the number of participants for laptops/desktops, "s" is used when reporting the number of participants for smartphones, and "t" is used when reporting the number of participants for tablets. We indicate numbers to describe prevalence of a particular theme within our participants, which do not generalize beyond our population. Additionally, grouping terms are used when describing such trends. A "couple" is used when speaking of 1-2 participants, "few" is used when describing 3-5 participants, "some" is used to describe 6-10 participants, "many" is used when describing 11-20 participants, and "most" is used when describing over 20 participants.

3.4.1 Factors of Device Choice

We started the interview asking how and for what activities participants used their different devices. Participants reported that they used their smartphones for the widest range of activities, followed by laptops which were used primarily for more formal or complex tasks (l=9, s=0, t=0). As explained by P22, *"there's nothing that I wouldn't necessarily not use on my phone... I feel like that's also the case because I had my phone first, so because that was the first thing I had, I automatically put everything on it".* Variations of these sentiments were expressed by the other participants, with the caveat that more functionally intensive activities, such as document editing, were done primarily on the laptop. To further characterize their device usage and preferences, we also asked which they would use to do a select few online activities with potential privacy or security concerns, specifically banking transactions, paying bills, shopping online, and social media. Device usage varied largely by individual based on their preferences, the specific tasks they were performing, and the context in which they were performing the tasks.

We asked participants why they chose certain devices for different activities to understand their perceptions of the different capabilities offered by the platforms. As expected, the two most prevalent factors impacting participants' decisions of device

usage were functional considerations of using the device (l=24, s=22, t=13) and the context in which they were in (l=8, s=25, t=5). For example, when P2 explained the reasoning behind why they use their laptop for online shopping, they focused on how convenient and easy the laptop is to use compared to their phone because it saves their credit card information: *"It's just harder for me to use my phone for shopping because I would have to physically get out my card and everything like that. Whereas on my laptop, it's already saved."*

App compatibility and functionality played a large role in influencing users' device preferences, particularly for social media (l=6, s=16, t=3). Many users indicated they would prefer to use a smartphone for social media due to the compatibility and functionality available for those apps on these devices compared to desktops. P4 explained for social media use they mostly use *"...my phone, because a lot of the social media apps were made for smartphones, like Instagram and TikTok. And if you even use the website they will send you to the app. So mostly my phone."*

The context of the user also influenced device choice, choosing the device they could use in certain locations (such as away from home) or alongside other activities. P11 explains how context can influence device choice:

> *"I use anything that's readily available at the time. If I'm shopping for something, usually it's something I'm looking for throughout the day. So, usually that's easier to be on my smartphone as I'm going from place to place, as I don't always have my laptop with me, but if I have my laptop with me, I'll use that to look at something on the side. If I decide not to buy it at the time, I might come back to my apartment and then complete the transaction there."*

Security and privacy did arise in discussing device choice, generally as a tertiary concern (l=2, s=2, t=2). Participants often mentioned that they were not concerned with the activities they performed, such as online shopping or banking, on their different

devices. A couple discussed an activity they might avoid due to some concerns, such as shopping at unfamiliar websites, that might influence how they performed that activity. So while security was not frequently a factor in what participants were willing to use on their devices, their choices in how they used those devices still have implications for their security risks and behaviors. For example, P11 explains how security concerns can become a factor in device choice:

> *"If it's anything beyond day-to-day shopping where it's more formal purchases, I usually just do that on my computer, my desktop computer, just because I know, once again, it's a comfort thing, I guess. But I don't have any specific concerns about online banking or online shopping. Obviously, I worry about website security. So, I usually try and stay away from if a website's questionable in terms of shopping on there, but for places where I frequent Amazon and things, I'll do that anywhere."*

Section 3.4.1 Key Takeaways: Most influential factors influencing device usage were functionality and context.

3.4.2 Evolution of Folk Models

As part of our analysis, we looked for evidence of each of the 8 folks models identified in Wash's study [50]. No participants discussed two of them - "Hackers are contractors" and "Hackers are graffiti artists." The remaining two hacker-based folk models were discussed across all the devices. Hackers are burglars was the most commonly identified folk model (l=13, s=9, t=3) while only a few participants on each device mentioned that hackers targeted big fish (l=4, s=1, t=2).

All four of the virus-centric folk models were found in the laptop interviews, with "Viruses are buggy software" being the most prevalent (l=10), followed closely by "Viruses support crime" (l=7), "Viruses are bad" (l=5), and "Viruses cause mischief" (l=4). For example, P10 expressed a perception of viruses as buggy software when he explained what they thought caused their laptop to operate differently than normal:

"I don't think it's a hack or anything like that, more like a virus or something more related to that, started acting a little more glitchy."

While virus models were regularly present in discussions regarding laptop risks, they were much less frequent in smartphones and tablets. Viruses are buggy software (s=3) and viruses support crime (s=1) were the only ones mentioned with smartphones, while tablet discussions mentioned viruses support crime (t=2), viruses are bad (t=1) and viruses cause mischief (t=1). These differences in the folk models expressed by participants when talking about different platforms indicate a reduced awareness of risks on smartphones and tablets. One common perception of participants was that they were not at risk of viruses or hackers on their smartphone, due to a variety of reasons, and thus did not need to be concerned or conduct any preventative security behaviors beyond the default, factory provided, measures.

When examining the details of the folk models expressed by participants, we also saw additional nuances in those perceptions that were not mentioned in the original study. First, regarding the hackers are burglars folk models, the primary understanding of users was that hackers were still after money or bank accounts. However, some participants also expressed that there are other resources that hackers could want as well (l=9, s=6, t=3). As described by P18, he was worried that hackers would *"try to access my files, in the form of, as I said, books, applications, photos, videos"*. Thus, there is some evidence that users understand that other resources have value to attackers, not just those that are clearly related to money.

Participants also expressed additional details regarding how viruses support crime in that risks, such as viruses, can come from downloading (l=20, s=7, t=3). Many participants had the perception that viruses came from *"possibly visiting sites that are kind of sketchy, or haphazardly downloading an app that could be like a tracker."* (P20). This demonstrates the evolution of users' understanding of potentially risky behavior, even if that understanding is still not entirely accurate or complete.

We identified two additional hacker-related mental models in our interviews. The first is that "Hackers attack networks" (l=2, s=3). Users with the mental model have the understanding that hackers attack the WiFi networks or the cellular network to gain access to all accounts and devices shared on that network. However, users with this mental model do not have a clear understanding of how this occurs, just that it means they should be careful of using public WiFi: *"What I heard of, sometimes when they share public WiFi, they also share what they can see on your phone. I'm not sure how exactly it works"* (P16)

The other new mental model was found exclusively during discussions about smartphone concerns and risks - "Hackers attack social media" (s=4). Participants with this mental model have an understanding that hackers can use social media to hack their devices, largely because of personal experience with these kinds of attacks. P22 explains it as *"The links, they're normally on social media. It would be an advertisement or something like that. Then I would just click it and then go from there."*.

Section 3.4.2 Key Takeaways: Two new folk models identified, **viruses support crime** and **hackers are burglars**. Two evolved folk models identified, **viruses come from downloading** and **hackers want other resources**.

3.4.3 Device Specific Mental Models

We now detail the specific perceptions participants raised when discussing their concerns and behaviors on the three different platforms.

We discovered five common mental models across all three device platforms, each with several supporting perceptions that form each mental model, summarized in Figure 3.3 above. While these mental models and perceptions are categorized the same way across the different device platforms, their effect on security behaviors and the primary supporting perceptions did differ by device platform at times. Each mental model and perception is described below, along with their frequency on each device

Mental Model	Supporting Perceptions	Example
Platform is secure	• Device platform is secure • Tablets are similar to smartphones • Smartphones are more secure • Company is trustworthy thus secure • Risk come from user error • Physical security of device influences risk	• "I feel like I think I heard somewhere that it's really hard for phones to get viruses or to get hacked and stuff like that, and it's personally never happened to me or anyone that I know about, so I assume that that's probably got some truth to it." P3 • "Windows of late is relatively more secure, but Linux has a history of being secure, so if I do online banking, if I'm using my laptop, it would be through a Linux operating system." P18
Applications are secure	• App is secure • Trustworthy apps reduce risk • Third party apps are risky	• "...on my laptop, whenever I'm surfing the internet and keying in information on my laptop, I feel as though I'm just more at risk, versus the app itself." P22
Security tools are used to mitigate risk	• Smartphones are less vulnerable to hackers and viruses • Security tools help protect devices • Sufficient security tools are based on risk • Security is not a priority due to cost	• "I actually install an antivirus, actually. The Norton security AntiVirus. I just installed that so that I don't get any virus or it prompts me if someone is trying to include my information." P26 • "[...] for most of my things I would prefer to be really secure, I do have face ID or a passcode to let you in them." P24
Web browsing and downloading is risky	• Good web browsing practices help mitigate risk • Web browsing and downloading is risky • Web-based security tools protect from internet-based risks	• "I don't go to any third party sites. And as I said, I use an ad blocker. So mainly you go to the third party sites by clicking an ad or something, when we try to access a webpage. UBlock prevents such issues, and also I had installed an antivirus. So I ensure I don't access those websites" P26
Limited risk due to usage	• Limited usage of device limits risk • Stopping the task/device stops risk	• "If I just had recreational things, I wouldn't be concerned about anything being hacked into, because nothing on there would be really meaningful to me. It could easily be recovered." P19

Figure 3.3: Identified mental models and supporting perceptions.

platform. In instances where participants did not described evidence of a perception on a particular device platform, that platform will be missing from the list.

Participants expressed a greater breadth of mental models and perceptions regarding laptops/desktops, which indicated a greater understanding of the possible security risks with using these machines. One reason may be that participants reported a number of past security problems when discussing laptops, such as experiences they had with phishing and scam emails (l=22), and less experience with security problems on smartphones or tablets.

3.4.3.1 Platform is Secure

The first common mental model was that the device platform itself was secure (l=19, s=21, t=9). As part of this mental model, participants generally perceived their laptop or desktop to be secure because of factors such as the operating system, the type of device they owned, or the manufacturer of their device. For example, a few participants perceived they were safe due to having a machine manufactured by Apple (l=4, s=11, t=9). With this perception, users believed their device was secure because of the built-in protections provided on Apple devices or the perception that Apple devices were impervious to risks. However, this perception was not limited to Apple devices. As P18 explains, *"Windows of late is relatively more secure, but Linux has a history of being secure"*.

As part of this perception, users believed their devices to be secure due to built in protections and perceptions of trust in the companies' reputation for protecting their information. Interestingly, one impact of this perception on security behavior is that some participants thought because laptops are secure, the main security issues they encounter are due to user error rather than security risks like viruses (l=6, s=2). Participant 14 explains, *"No issues other than me causing them myself, like if I forgot a password or something and I tried to login too many times and I got locked out of my account..."*.

As part of this model, there was a common perception that smartphones are more secure than laptops and desktops (l=5, s=5). P22 sums up these perceptions by

explaining *"If anything, when it comes to security, I would actually think that my laptop is less secure"*. Another perception that made up this mental model was that tablets are similar to smartphones, and thus have the same vulnerabilities and protections as a smartphone (t=10). A few participants also perceived the physical security of their device as a key factor in maintaining device security and, as a result, placed an emphasis on having their device in hand or nearby as a method to mitigate those risks (s=4, t=3). P24 explains, *"Because with my phone it's constantly on me and my laptop is always in my book bag. But with the tablet, I just think about them laying out more and how it's a lot easier for anyone to pick them up versus a phone."* Thus, participants indicated that they are careful what applications they have on their tablet because it is, or could be, more easily accessed by other people.

3.4.3.2 Applications are Secure

In addition to the mental model that their devices were secure, some participants had the mental model that the applications they were using were secure or had built in security features that were sufficient for mitigating risk. As part of this mental model, participants expressed a belief that certain apps were secure (l=1, s=7, t=1). In some cases, this perception of security caused them to do certain activities on their phones, such as shopping on Amazon, due to their perception that the Amazon app is more secure than the website. Another perception they had was that the software or service was responsible for managing security. Those with this perception sometimes chose to trust the application to secure their information, either on a website or device application, rather than their device. In this instance, they view the company as having more trustworthy and stronger security measures than their device. As P16 explains, *"In terms of websites, I feel like the companies make it secure enough. Computers, I feel like it's a little bit less secure. I don't completely trust my computer completely."* However, these perceptions also caused participants to not use additional security measures at times as they trusted the companies that provided

the application to protect their information and devices. As P9 explains *"Different apps have different passwords, of course, and those are what I really focus on because if the app has a password to it, then I'm more comfortable not really getting anything else for privacy reasons."* As a result, participants' trust in organizations to provide security within applications is important because some participants rely on and trust an application to utilize good security practices, resulting in them not using additional security measures to protect their data or device.

Another perception participants had was that downloading apps can be risky (l=2, s=4, t=1) and thus apps should only be downloaded from trustworthy sources rather than third party sources. Additionally, unlike with laptops, there was also an added perception that using trustworthy applications reduces the possibility of risk on the smartphone. As P12 explains, "I try to use trusted applications as much as I can, but there is always this, *"Why I'm giving this? If I install a new application, why I'm giving access to this or that, to my photos, or to the mic?" But usually I'm not really worried about hacking, because I feel I use trusted applications in general, and very common ones."*

3.4.3.3 Security Tools are Used to Mitigate Risk

Participants discussed a variety of security mechanisms they use to protect themselves on their device platforms. What was adopted or practiced depended on users' perception of where the most risky security vulnerabilities came from, and what was available on a device platform. For example, P18 explains their practice on their smartphone as: *"I was looking into, again, security applications, and I find that having an ad blocker in Chrome is good enough. And as long as you don't install explicitly third-party applications, which of late, I'm not, you don't necessarily need an antivirus anymore."* In other words, participants found that using the appropriate tool for what they perceive as risky behavior is enough to mitigate the majority of risk with little to no additional measures.

Participants named a number of tools they used or were familiar with, including ad blockers, password managers, VPNs, private browsers, phishing detection alerts, scam email filters, and anti-virus software. Participants expressed that such tools can be used to supplement their personal security, and thus reduce other individual security behaviors that they have to practice (l=25, s=19, t=12). P21 explains, *"I just use Windows Defender, which is the built in antivirus and security software that Windows uses. I think that's plenty to keep you from downloading viruses and things like that. Or if you download a virus, it'll get rid of it pretty quickly."*

However, some of the participants who understood that security tools were helpful in mitigating risk indicated that they did not use any security tools other than the device access password (l=5, s=13, t=8). Thus, while many participants felt that the adoption of at least one type of security tool played a key role in the protection of their device, some participants expressed that adopting additional security tools was just not a priority. Participants explained that they simply did not have the time and/or level of concern to warrant using security tools for protection (l=10, s=2, t=1). Some participants further elaborated that security was not a priority because of the costs of using certain security software (l=7, s=1, t=2). P25 explains, *"That's why I keep it on the back burner just because I'm... I would say almost in denial. I don't know. I don't want to open that door because I can't afford to pay for software if I needed it."* While these concerns were much more prevalent on laptops, they did still exist across all device platforms, indicating that the lack of awareness of risks or security mechanisms is not the only limiting factor that could be influencing users' decision to use security tools.

3.4.3.4 Web Browsing and Downloading is Risky

The next mental model we identified was that Web browsing and downloading were particularly risky behaviors. One of the main supporting perceptions was that browsing on the internet or downloading files can be risky and result in compromising

the security of your device (l=20, s=15, t=3). P11 states *"Obviously, I worry about website security. So, I usually try and stay away from if a website's questionable in terms of shopping on there."* Thus, many participants found that having good web browsing practices, such as carefully choosing which websites to visit and not downloading files or software, was necessary to mitigate these risks (l=19, s=13, t=3). As P16 explains, *"I believe most of the viruses are easy to avoid, as long as you do not go to suspicious sites or click on anything that's too suspicious".* Participants discussed how they relied on their own perceptions and cues from the browser to determine what sites and situations were risky. As P2 explains, *"When I'm in a public place, and I'm entering in my credit card details or something like that, I would be a little skeptic. Or even on Web pages, when they don't really encrypt the password with the little asterisk keys, I get a little concerned".* Additionally, participants with this mental model also did rely on web-based tools such as secure connection feedback and ad blockers to protect their devices from Internet-based vulnerabilities (l=12, s=4, t=2).

3.4.3.5 Limited Risk Due to Usage

Some participants had the perception that they were not at risk due to the limited usage of their device (l=5, s=3, t=21). Participants with this perception generally either do not use their device for many tasks or do not use their device for tasks they view as potentially security risky. As Participant 5 states, *"Not saying that it could never happen, but I don't really use, other than websites to buy certain things. Again, I primarily use it for school, so I'm not really worried about someone hacking my school account."* This was a particularly prevalent perception on tablets as our sample of participants generally did not use their tablets for much, with 7 participants reporting they use their tablets primarily for entertainment, 4 participants reporting they use their tablets primarily for schoolwork, and 2 participants reporting they use their tablet for a mix of the two activities. This meant a total of 13 out of 27

participants indicated they used for tablets for very limited activities and many had limited security concerns, if any, regarding their tablets. Similarly, some participants thought that stopping the task, closing their browser, or restarting their computer would address a potential risk (l=7, s=3, t=1). As P11 explains, *"So if you download something or you click on something, you're like, I shouldn't have clicked on that and you shut the computer off, that way it just stops everything from running."*

Section 3.4.3 Key Takeaways: Five mental models identified with device-specific variances in prevalence and application of the supporting perceptions.

3.4.4 Confidence and Trust

In addition to expressing perceptions of security, participants also expressed varying levels of confidence in three separate entities to protect themselves. The first of these could be described as confidence in companies (l=18, s=22, t=7). As previously explained, some participants believed their devices to be secure because they were manufactured by a specific company, and they trusted that company. This perception was most commonly observed by users of Apple devices. P21 sums up these perceptions when explaining, *"P21: Because I know Apple goes through a good amount of verification before putting random apps on the app store."* However, users' trust in device companies also impacted the applications they felt comfortable using on their devices. P26 explains, *"I just download the verified applications from the Play Store as I use a normal Android phone. So I don't have any specific privacy and security applications on my phone."*

Another impact of their confidence in companies was apparent in user's usage of various security tools, such ad blockers or website phishing alerts. Users' confidence, or lack of confidence, in the companies that manufactured these tools and alerts influenced whether or not they utilized the tools, or the information provided by them, when making decisions that would impact their digital security. P13 explains, *"I'm*

scared the password manager itself can get hacked. So I just have it in the little notes on my phone in code."

The next entity that users expressed trust in was other individuals (l=8, s=9, t=2). This was often trusted friends and family members, but could also include advice columns on the Internet and other similar resources. P8 explained *"I usually just panic, ask my husband what to do, and turn off my computer."* In this example, their first response to a perceived security risk is to shut everything down. They then further try to solve the issue by asking someone they trust, in this case their husband, for assistance. Users with this perception felt that there were trusted individuals that they could rely on to resolve security vulnerabilities. Aside from impacting their response to threats, this perception of confidence in others also frequently influenced what risks users were concerned about. For example, P26 states, *"Because I have never faced that issue, and I haven't seen any people who were complaining having a virus on the phone."*, to explain why they are not concerned about viruses on their smartphone.

Similar to the previous category, there was also the reverse where the lack of confidence in others influences users' security behaviors and perceptions. However, this was less common as the lack of trust was more commonly applied to individuals or sources who were not close to the user. P22 elaborates, *"You cannot trust everything that is posted on social media, because sometimes people just are very biased and fake news is very popular."* While this perception was less common, it did have an impact on whether the user viewed the security advice provided as reputable or worth disregarding.

The last entity that participants trusted was themselves (l=21, s=20, t=9). While sometimes participants expressed a lack of confidence in their ability to avoid making mistakes that would result in a security risk, most participants felt that the measures they took to mitigate security vulnerabilities were enough. P16 sums up this perception

by explaining: *"I stick to sites I know it's safe, and since I rarely really go any further than that, I never really have to worry much about viruses"* Users who trusted in their own security decisions felt that they were relatively aware of risky behavior and thus were able to avoid making mistakes. A lack of confidence in themselves was less common, and only a couple of participants indicated a lack of trust in themselves. When they did so, this lack of trust was also associated with a lack of awareness of risk or of a certain practice.

Section 3.4.4 Key Takeaways: Perceptions of trust in companies, other individuals, and themselves influence adopted security behaviors on devices.

3.4.5 Impact of Mental Models on Security Behavior

As we discussed in the previous sections, participants often implemented security behaviors based upon their mental models of risk. And they chose a combination of behaviors they thought would be most important based on what they trusted to mitigate those risks. For example, P21 stated, *"...as far as viruses go, I'm pretty good about watching out for what I download. And when I download it, if I think it's something that might be kind of suspicious, I'll run it through a virus checker to see if it contains any viruses or anything like that. And then that'd let me know if I should install it or not."* In this example, the participant first relied upon their own Internet practices and knowledge, and then supplemented their security practices with a particular security tool as an added measure.

Participants sometimes expressed a lack of confidence in their ability to avoid making mistakes that would result in a security risk. When they did so, this lack of confidence was also associated with a lack of awareness of risk or of a certain practice. P25 explains, *"...if I don't know how to do it or don't feel confident on how to do it, I usually won't."* Another common security behavior exhibited by participants was a reliance on other individuals to resolve security issues (l=8, s=9, t=2). Participants

often referred to trusted friends and family members, but did also reference advice columns on the Internet and other similar resources.

However, most participants felt that the measures they took to mitigate security vulnerabilities were enough. In general, participants felt that they were relatively aware of risky behavior and thus were able to avoid making mistakes, particularly with the assistance of a few security tools. Thus, while we saw a range of appropriate behaviors and adoption of tools across our set of participants, individual participants generally only relied on a few of these.

Section 3.4.5 Key Takeaways: Based on device-specific adoption of mental models, users also adopted device-specific security behaviors.

3.5 Discussion

When comparing the mental models and perceptions of security across platforms, we found that laptops and desktops not only had the highest presence of the original folks models, but also the most variety of device-specific models. While some of the same models could be found in discussions of smartphones, there was higher emphasis on smartphone-specific concerns, such as an emphasis on app security and that hackers may try to attack social media platforms. The mental models expressed when discussing tablets were quite different. In their case, participants' perceptions lacked the breadth of mental models expressed for laptops and smartphones. Many of the prevalent tablet perceptions were influenced by a lack of usage of that platform, which greatly reduced users' security concerns. Additionally, some common perceptions found in the study related to users perception that software, either security tools or factory-installed device security mechanisms, were a key component in device and data security as well as sometimes sufficient for mitigating risk to vulnerabilities.

Most concerns held by device users could be categorized as concerns about information security and physical device security. The portable devices, such as smartphones

and tablets, related more to device security. Participants indicated that maintaining physical control over their devices played a large role in maintaining their digital security and mitigating risk. Information security risks came up more frequently with laptops and desktops, where participants focused on risks coming from failures in Internet security - such as downloading from malicious links, visiting sketchy sites, or trusting the wrong site with personal information such as credit card information, email addresses, etc. In this case, participants believed that being susceptible to one of these risks would put them at risk for a virus, getting hacked, or having their data compromised - such as through the site's security being compromised. However, participants' concerns and perceptions worked together to influence their behavior. For example, participants with a perception that security risks come from sketchy sites focused on having good Internet security, including ensuring they were visiting legitimate websites, not clicking on unverified links in emails, being careful what they download, and not using third-party applications unless verified.

Multiple mental models and concerns also worked together with participants' level of trust or confidence in an entity to drive behavior. For example, a user who believes that the way to get a virus is by downloading something malicious, who has confidence in their own skills to avoid dangerous sites and also trusts the ad blocker they have, may feel sufficiently protected and not use anti-virus software. In this example, the participant's confidence in their own ability to detect suspicious sites as well as their trust in the ability of the ad-blocker works along with their perception that viruses come from downloading to create a lack of concern regarding susceptibility to viruses due to the security measures in place. This user may adopt some good security practices that are effective, but perhaps not the complete set of security mechanisms that would more fully protect their devices and their information.

In this example, the participant had multiple perceptions of confidence and mental models working together to decide what security behavior they felt were necessary to

protect their devices. This is a common occurrence as oftentimes participants have multiple entities they trust to handle security concerns or to provide reputable sources of information to mitigate risk. Kulyk et al. found a similar perception in their study which was that trustworthy companies could be relied upon to protect the data given to them [30].

However, one concern participants face is knowing when to trust themselves and have confidence in their own abilities to detect security risks. This concern often works alongside participants' lack of awareness of risk to result in participants not having confidence in themselves to recognize security risks or to not cause an issue due to user error, such as clicking on a dangerous link. Users also face a false sense of confidence in their abilities to mitigate risk, particularly when they rely solely on mechanisms such as passwords, device pins, and their own careful browsing behavior, to protect their devices and their information rather than utilizing additional security mechanisms.

3.5.1 Comparison to Existing Mental Models of Security

Aside from the identification of the folk models initially identified by Rick Wash [50], many of the mental models of security identified in this study are unique to the ones previously identified in literature, specifically in that they focus on device-specific perceptions of security as a whole, including device usage, security tool usage, and security behavior implementation, rather than on a narrow component of device security, such as encryption, viruses, and hackers. However, there is some overlap, at least within a broad sense with some of the mental models discussed in Chapter 2.

One of the mental models discussed in that chapter was that an individual's privacy was not at risk due to their information being non-sensitive or non-threatening [22, 23, 41, 30, 53]. This is similar to the perception identified in this study, "limited usage of device limits risk". Both of these perceptions focus on users' perceiving a decreased level of risk to their device security based on the sensitivity level of the data

stored on that device. However, the "limited usage of device limits risk" perception also applies the decreased perception of risk due to the limited functionality and usage of a device, such as for entertainment purposes only.

Another mental model previously identified in research was that users sometimes perceive it as unnecessary to adopt security measures other than using built-in security tools or being careful when clicking links or skipping security warnings [23, 41]. This mental model has base commonalities with the perceptions "security tools help protect devices", "sufficient security tools are based on risk", and "good browsing practices help mitigate risk". Users with the first two perceptions can also perceive built-in security tools as being sufficient security measures, though this specific application of these perceptions was more common with smartphone and tablet users than on traditional computing devices. However, the last perception, "good browsing practices help mitigate risk", does align relatively closely with the existing mental models regarding security behaviors, though this perception does focus on more on web-based security behaviors.

Two other mental models previously identified in literature was that "If the company is trustworthy then it is safe to provide my data to them", which is similar to the "device platform is secure" perception, and "apps from app stores are secure by default", which is similar to the "app is secure" perception [30]. One of the major differences between both of these mental models and the perceptions identified in this study is that the mental models were identified as applicable to smartphones while the perceptions were identified as applicable on all three platforms.

While there are some commonalities between the mental models and supporting perceptions identified in this study and mental models identified in prior research, the majority of the mental models identified in this study have not been previously identified, or not identified as applicable to all three platforms to some degree. Additionally, the mental models of security identified in this study focus on the three

device platforms, laptops/computers, smartphones, and tablets, as a whole rather than considering only singular security tools, risks, or behaviors on a platform. As a result, the mental models and supporting perceptions identified in this study provide a unique method for understanding and utilizing a holistic set of perceptions of security and their variances on the different device platforms.

3.5.2 Folk Models

While our intention was to examine mental models across the three platforms, our study also provides additional evidence of the prior virus and hacker-based folk models, as well as offers evidence of possible evolution of these models more than a decade after they were originally identified [50]. While we did not find evidence of two of the hacker mental models ("hackers are digital graffiti artists", and "hackers are contractors"), we do not conclude these models are no longer common. Instead, our interviews had a different focus, and thus may not have uncovered all of the same details. These models may not have been as prevalent in our sample, but may be in other samples of different populations.

There was consensus across our participants that security risks are related to having something stolen, whether that be financial or other resources. Participants also expressed a modern perception that risks come from "downloading." This focus on risky Internet behaviors was also paired with a perception that good Internet security practices played a major, and sometimes sufficient, role in protecting themselves from security risks.

Overall, we believe our study demonstrates that the original folk models found in 2010 are still applicable for general users today, even across different platforms [50]. However, the evolution of two of the models and the creation of two new folk models is indicative of users' perceptions evolving to reflect the changing capabilities and uses of technology. This indicates the likelihood of new folk models continuing to emerge, and the possibility that some of the less prevalent or more technology specific folk

models may either become obsolete or evolve as technology continues to advance and users' perceptions of risks adapts to these advances.

3.5.3 Awareness

Participants' perceptions of risk and appropriate security measures did seem to vary by device platform, with a larger awareness of risks on laptops and desktops. Despite that, there was a lack of awareness of what are sufficient security behaviors, with a primary focus on good Internet security behaviors as being a major factor in ensuring digital security. These measures were also boosted by the perceptions that security tools can be used to supplement security, with a focus on ad blockers, vpns, browser warnings, and anti-virus software.

While many studies have concluded that users often lack awareness of security risks [26, 20], our study demonstrates that this lack of awareness of risk is more acute with smartphones and tablets. Participants hear more about, and may even experience, more viruses on laptops/desktops, and thus have a limited perception of risk to themselves on their smartphones and tablets. Furthermore, there is a lack of usage of services on different platforms, browsing in the case of smartphones, and information sensitive apps such as banking, in the case of tablets. As a result, this limited usage of these services works in conjunction with users' mental models of how their devices are secured and where security vulnerabilities come from.

Nevertheless, there is still some awareness of basic security behaviors across all platforms, as previously described. These behaviors, such as the use of some security tools, good browsing habits such as awareness of website legitimacy, and common phishing preventative measures such as not clicking on links in unknown emails, indicate that education efforts are at least somewhat effective and resulting in valuable user practices. However, users generally employed only a few security measures, feeling they were sufficient for their protection. This combination results in incomplete protection of devices with a perception of safety that is not completely accurate. And

while many participants indicated awareness of a variety of security tools on laptops, such as password managers or ad-blockers, they rarely utilized those same tools on the other platforms even when they are available and would be useful.

3.5.4 Implications

One of our major findings is that users perceive fewer security risks on smartphones and tablets than on laptops/desktops, and utilize fewer security mechanisms as a result. This could result in increased risk on smartphones and tablets, depending on how those devices are used. While this risk could be less on tablets due to the frequent adoption of the "Limited risk due to usage perception" on that device, this is not a guarantee as this perception is generally based on frequent usage on a device and not necessarily exclusive usage of a device. In other words, while users might perceive tablets as being less at risk because they use it for entertainment, that does not mean they use their tablet exclusively for entertainment and don't sometimes browse the web, etc.

Furthermore, this mental model is built off of factors such as current device usage but may still be prevalent even if tablet usage shifts in the future due to its early establishment unless users modify their mental models as well. As a result, while users may have the perception that there is little to no risk on tablets or smartphones due to a variety of reasons, their actual usage and implemented behaviors as well as future usage of their device means it is still important to be aware of potential risks and security mechanisms on smartphones and tablets to decrease risk to security vulnerabilities. Thus, one implication of our results is that education or awareness campaigns should be focused more specifically on the risks and security mechanisms available on smartphones and tablets, to build off of their current understandings and existing security practices.

As previously mentioned, the same security mental models were found on each of the different platforms. This is likely an indicator that the formation of the mental

models is a result of common education and experiences which are then extrapolated and adapted to fit users' perceptions and usage for each platform. This is congruent with existing research into the formation of users' mental models through factors such as media stories, security training, stories from friends and family, and individual experiences of security compromises [44, 50]. The prevalence of traditional computing-based mental models of security being discussed on the other platforms in this study, even when in lower quantities, could mean that laptop education, security-training and experiences are the primary factors influencing the formation of the mental models in our population, which has frequent exposure to laptops through their education, work, and/or entertainment-based activities.

A part of this education should focus on the range of tools available to all devices, as well as the role of secure browsing behaviors and tools in mitigating risks. As discussed in the previous sections, many participants viewed secure browsing as being a key factor in mitigating risks. However, this perception, while resulting in good security practices, does not fully address the possible risks on any device. Therefore, bringing an awareness of the range of tools, including reputable open source or free tools, available to users and their purposes, as well as the benefits and limitations of secure browsing can help users create a more holistically secure environment and establish good security habits.

One potential path for increasing user awareness of smartphone or tablet-based security tools could utilize the tools users already are using on laptops and desktops. Such tools could help to inform or nudge users towards smartphone or tablet-based versions of the security mechanisms to build awareness of their potential use on these other platforms. We explore this idea further in Chapter 5.

Another avenue of education users need is on how to determine trustworthy sources of security information. Partly due to their trust in other entities, participants often relied on others, either internet-based sources or a trusted individual, for security-based

suggestions, advice, and information. The influence of trust in a social network on user behavior has been identified as an influential factor on behavior [54, 9, 10]. However, when this is a crucial aspect of users' education, it is important for them to know how to recognize trustworthy sources of information to prevent misconceptions or poor security behaviors. Educating users in these areas can help build on the good security practices they already implement, as well as educate other users when they act as a trustworthy digital-security knowledgeable entity to others.

3.6 Summary

Mental models of security and privacy across the three main platforms have both similarities and differences. One of the big similarities is that all three device platforms exhibit some evidence supporting each of the identified mental models of security and their supporting perceptions. These five identified mental models were "limited risk due to usage", "security tools are used to mitigate risk", "platform is secure", "web browsing and downloading is risky", and "applications are secure". Compared to existing research on mental models of security on traditional computing devices and smartphones, these findings are novel as they describe mental models of security across all three device platforms and compare the stated similarities and differences in the perceptions of security regarding each device as a whole, the security risks each device faces, the applications and general usage of that device, and the security applications used on the device. The findings discussed in this chapter are summarized in Figure 3.4.

The identified mental models of security and most of their supporting perceptions were present on all three device platforms, even in our limited sample size. However, these mental models and perceptions varied in prevalence on each device, with some perceptions within the "Security tools are used to mitigate risk" and the "platform is secure" mental models not existing on a platform at all. These mental models, along with their device specific similarities and differences, are summarized in Figure 3.5.

Relevant Study Research Questions	Contributions/Findings
RQ1.1: What are users' mental models of security on laptop/desktops, smartphones, and tablets?	• Identification of 5 novel mental models of security with supporting perceptions
RQ1.2: What are the similarities and differences in perceptions of security risks across the three platforms?	• Identification of variances in prevalance of these mental models and perceptions of security on different device platforms • Identification of similarities in prevalance of these mental models and perceptions of security on different device platforms
RQ1.3: What are the similarities and differences in security behaviors on the three platforms, and what do these behaviors indicate about the mental models users have for each platform?	• Identification of device-specific similarities and differences in security tool adoption • Identification of device-specific similarities in security behavior adoption

Figure 3.4: Summary of Findings and Contributions from Study 1.

As a result, the identification of these mental models of security and their device-specific application provides an understanding of how security mechanism adoption can vary by device, at least in part, due to the differences in perceptions of security across the platforms. Similarly, commonalities in security behaviors across platforms can also be attributed, at least in part, to some of the similarities in mental models of security across platforms. One clear illustration of this is the mental model "security tools are used to mitigate risk". This mental model exists across all three platforms and commonly results in some form of security tool being utilized on all three device platforms to secure the device and its data. However, due to device-specific variances in the supporting perceptions such as "security tools supplement security behaviors" participants were more likely to rely on device-based security tools, such as biometric passwords, on their smartphone or tablet while also being more likely to rely on application-based software, such as VPNs and antivirus software, on their

Mental Model	Perceptions	Similarities and Differences
Limited Risk Due to Usage **L= 5, S=3, T=21**	• Limited usage of device limits risk • Stopping the task/device stops risk	• Much more prevalent on tablets than on smartphones and laptops • Generally view tablets as not at risk since they are used primarily for minimal or entertainment-based activities
Security Tools are Used to Mitigate Risk **L=25, S=19, T=12**	• Smartphones are less vulnerable to hackers and viruses • Security tools help protect devices • Sufficient security tools are based on risk • Security is not a priority due to cost	• More prevalent on laptops, followed by smartphones • Participants commonly discussed application-based security tools on laptops and device-based security tools on smartphones and tablets
Platform is Secure **L=19, S=21, T=9**	• Device platform is secure • Tablets are similar to smartphones • Smartphones are more secure • Company is trustworthy thus secure • Risk comes from user error • Physical security of device influences risk	• More prevalent on smartphones, followed by laptops • Generally viewed smartphones as secure due to the manufacturer
Web Browsing and Downloading is Risky **L=20, S=15, T=3**	• Good web browsing practices help mitigate risk • Web browsing and downloading is risky • Web-based security tools help protect from internet-based risks	• More prevalent on laptops, followed by smartphones • Generally viewed security risks as coming from web-based activities and that web-based security tools and behaviors were sufficient to protect devices as a result
Applications are Secure **L=1, S=7, T=1**	• App is secure • Trustworthy apps reduce risk • Third party apps are risky	• More prevalent on smartphones • Generally viewed security responsibilities as belonging to the application being used rather than the device

Figure 3.5: Summary of device-specific similarities and differences in mental models

laptop/desktop.

The identification of the similarities and differences in device-specific mental models of security and in device-specific security behaviors provides valuable insight into how to target topics such as device security training, security tool advertisements, and device-specific security notifications and warnings to address misconceptions as well as utilize prevalent mental models and perceptions of security to increase the chances of the information, instructions, warning, etc. being noticed and being effective at encouraging good security practices. In general, participants had a broader perception of risk and security mitigation methods regarding laptops/desktops than smartphones and tablets and mental models on smartphones and tablets seemed to be at least partially influenced by the formation of laptop-based mental models of

security. However, our population was well-educated, and also heavy users of laptop and desktop computers. The next chapter will explore whether the mental models and perceptions identified in this chapter are also prevalent amongst a larger population.

CHAPTER 4: STUDY 2: UNDERSTANDING USER BEHAVIOR: THE FACTORS AND PERCEPTIONS WHICH INFLUENCE DEVICE SPECIFIC BEHAVIOR

4.1 Introduction

The previous study identified a set of mental models of security and their supporting perceptions that were present across device platforms. However, as a qualitative study, we can not make strong conclusions about the prevalence of these mental models on different platforms and amongst a larger population. In this chapter, we seek to further these findings and address this limitation. In this study we surveyed 192 participants to determine users' mental models, the most influential factors affecting their security behaviors, and the security behaviors and tools users use on their devices and how these aspects might differ based on the device platform being used. This study addresses RQ1: What are mental models of security on various device platforms and how are they similar or different, RQ2: How do the perceptions of risk and security mitigation strategies relate to each other, and RQ3:How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform of this dissertation.

Past researchers have examined various predictors for user behavior. Two such predictors are mental models and factors which influence behavior [16, 17, 43]. Prior research has established various behavior prediction theories to predict users' intended actions such as the Fogg Behavior Model [21], Protection Motivation Theory (PMT) [38], Self-Determination Theory [38], Theory of Reasoned Action [12, 48, 37], Unified Theory of Acceptance and Use of Technology (UTAUT) [48] and the Technology Acceptance Model (TAM) [12, 43, 48, 37]. While these models have similarities and differences in the factors they utilize, they are all used to predict actual user behavior.

The core concepts for each of these models are summarized in Figure 4.1 below.

Behavior Prediction Model	Factors
Fogg Behavior Model	Core Motivators: pleasure/pain, hope/fear, acceptance/rejection Simplicity Factors: time, money, physical effort, brain cycles, social deviance, non-routine Behavior Triggers: spark, facilitator, signal
Protection Motivation Theory	Maladaptive Response: intrinsic rewards, extrinsic rewards, severity susceptibility, threat appraisal Adaptive Response: response efficacy, self-efficacy, response costs, coping appraisal
Self-Determination Theory	percieved relatedness, percieved competence, perceived autonomy, response performance motivation
Technology Acceptance Model	External variables, perceived usefulness, perceived ease of use, attitude towards using, behavioral intention to use
Theory of Reasoned Action	attitude towards behavior, subjective norms
Unified Theory of Acceptance and Use of Technology	performance expectancy, effort expectancy, social influence, facilitating conditions, gender, age, experience, voluntariness of use

Figure 4.1: Summary of behavior prediction theories and their core factors [21, 12, 38, 43, 48, 37]

There a few factors in common between the various behavior prediction models. For this study, we selected the six factors which appear the most frequently and consistently across the various models- cues to action, perceived severity, benefit of action, cost of action, self-efficacy, and ease of use [21, 12, 38, 43, 48, 37]. While these factors do not appear verbatim in each model, they can be summarized or categorized from the core concepts of the models. For example, cues to action can be derived from behavior triggers in the Fogg Behavior Model, threat appraisal in protection motivation theory, perceived relatedness in self-determination theory, external variables in the technology

acceptance model, and voluntariness of use in the UTAUT. Because all of these concepts are related to what might prompt the implementation of a behavior, they can be summarized as "cues to action". In this study, we sought to determine if users utilize both these factors and device-specific mental models to influence the adoption of security behaviors on three different device platforms- traditional computing devices (laptops and desktops), smartphones, and tablets.

Additionally, we utilized the five specific mental models- "the device platform is secure", "apps are secure", "security tools are used to mitigate risk", "web browsing and downloading is risky", and "limited activity limits risk" from the previous study. As found in Study 1, while the overarching mental models were identical across the device platforms, the individual perceptions which formed the models differed or were implemented in different ways based on the device platform. As a result, the perceptions which were applicable to all three devices in Study 1 were selected for each mental model for usage in this study. In other words, perceptions such as "Tablets are similar to smartphones" and "Smartphones are more secure" were not selected for the "Platform is secure" mental model due to their limited applicability to all three device platforms. This was done to limit the evaluated perceptions not only for comparison amongst the device platforms but also to limit participant fatigue when taking the survey.

Our research questions were as follows:

- RQ2.1: What are the similarities and differences in mental models of security by device platform?
- RQ2.2: What are the similarities and differences in the factors influencing to security behavior on different device platforms?
- RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms?

Additionally, we created four hypotheses about what the data would show.

- H_0 2.1: There are no variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.
- H_A 2.1: There are statistically significant variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.
- H_0 2.2: There is no correlation between device-specific mental models and the adoption of security behaviors on each device platform.
- H_A 2.2: There is a statistically significant correlation between device-specific mental models and the adoption of security behaviors on each device platform.

We conducted a survey of 192 participants asking them about their mental models, most influential factors, and their actual security behaviors and security tool usage per device platform. Our results contribute the following:

1. Comparison of existing mental models and supporting perceptions across laptops/desktops, smartphones, and tablets.
2. Identification of statistically significant variance between the perceptions across the device platforms (reject H_0 2.1).
3. Identification of the perceptions which are the most prevalent on each device platform.
4. Identification of the factors which are most frequently considered when determining actual security tool and behavior usage.

While this study does not find statistically significant correlations and predictions between mental models, factors of behavior, and actual security tool and behavior implementation, it does identify patterns across device platforms between these three

categories. These patterns are important in understanding the most influential security perceptions by device platform which users consider when determining how to use their device and protect their information.

Furthermore, existing research has already established that factors of behavior do influence actual behavior [21, 16, 21, 12, 38, 17, 42]. As such, identifying the most commonly considered factors and security perceptions across each device platform can be used to inform interface design and security awareness education, particularly when attempting to prompt or nudge security actions based on actual user motivations.

While our results show similarity in the device-specific mental models of security and their underlying perceptions across all three platforms and the factors influencing behavior, there are still differences in the prevalent perceptions for each mental model across each platform. In addition, there are differences in the reported security practices on each device platform. As such, our results indicate that while there are similarities in the overall mental models of security across device platforms, the differences in the supporting perceptions may influence the implemented security practices. As such, future work would need to be done to further establish a correlation between the differences in device-specific perceptions of security and device-specific security behaviors.

4.2 Methodology

This study was a survey designed on Qualtrics and conducted through Prolific with 192 participants. It was approved by the researchers' institutional IRB and gathered information about participants' indicated mental models and the most influential factors when considering which security behaviors and tools to implement.

The survey consisted of five main sections. Participants were first asked general demographic questions and eligibility questions to ensure they met the inclusion criteria to participate in the study. To participate in the study, participants needed to be residents of the United States and 18 years or older. They also needed to own or

regularly use all three studied device platforms (laptop/desktop, smartphone, tablet). Some of these demographic questions were pulled from SA-13, a scale designed to indicate the attitude of the participants to security, including their resistance to adopt security behaviors [19]. This scale is built on the SA-6 scale which measures users attitudes towards security behaviors, but the SA-13 scale includes additional measures for resistance and attentiveness [18]. SA-13 was chosen due to the potential for its additional measures being useful in understanding the influence of mental models of security on actual security mechanism adoption. Specifically, the additional measure for resistance to the adoption of security behaviors could help explain discrepancies in existing mental models of security and adopted security behaviors on the different device platforms.

Due to a mistake when creating the survey, only three of the measures in SA-13 were measured- engagement, attentiveness, and resistance. However, this did include the most relevant measure (resistance) for helping to understand security behavior adoption by participants. When scoring, participants ranked responses as either "yes", "no or not sure", or "N/A". When scoring this for calculating the SA13 score, "yes" responses were given a value of 5, "no or not sure" responses were given a value of 1, and "N/A" responses were given a value of "3". The abbreviated form of SA-13 measured in this study will be referred to as SA-10 for distinction purposes. Figure 4.2 reports a box plot of the SA-10 scores for engagement, attentiveness, and resistance.

The next section asked participants about their general device usage, such as which device they use the most frequently and any experiences with common security risks, such as viruses. Participants were then shown three, randomly ordered sections which asked participants to identify the mental models of security and supporting perceptions they held, the security tools and behaviors they implemented, and the most common considered factors influencing adoption of these security mechanisms on one specific device (laptop/desktop, smartphone, tablet). Each of these device-specific sections

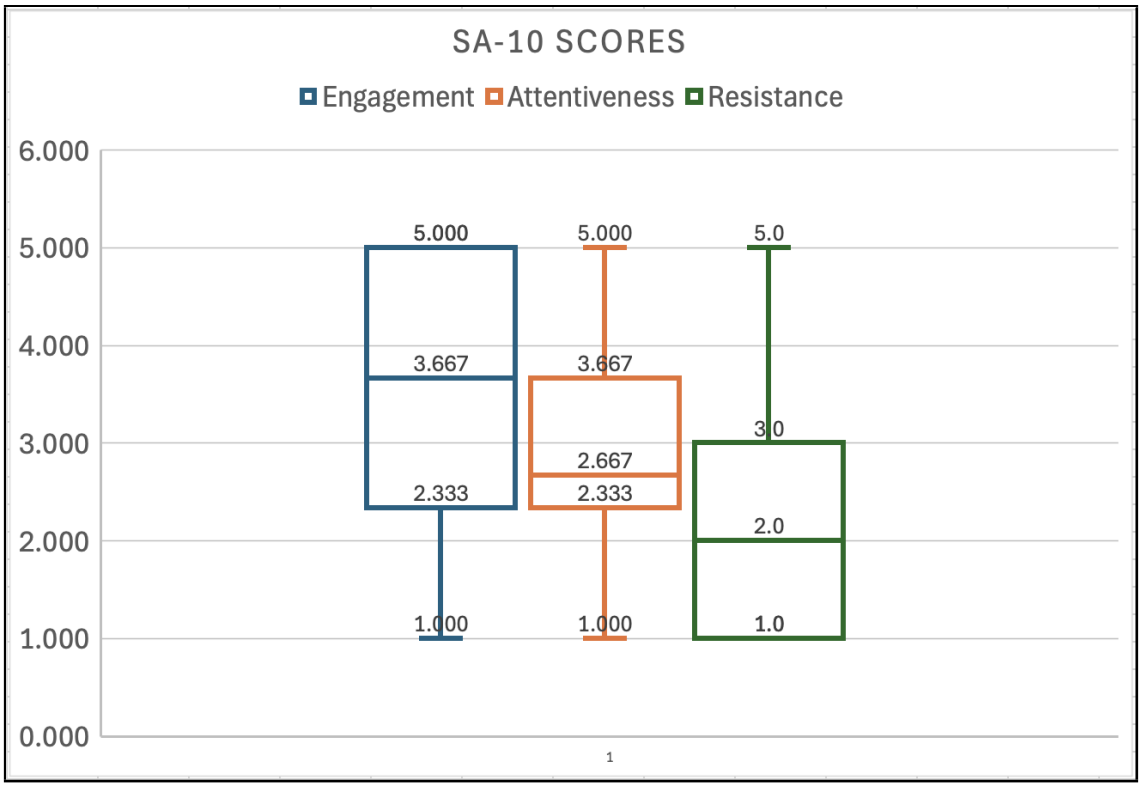

Figure 4.2: SA10 Scores for engagement, attentiveness, and resistance

differed only by the applicable device, with the rest of the wording and ordering being identical.

These sections were randomly selected from each of the device platforms to minimize bias in the responses from the same device platform being shown first each time. In other words, participants were each shown a section about traditional computing devices, smartphones, and tablets. However, the order these sections were displayed to participants was randomly chosen by Qualtrics.

4.2.1 General Device Usage

The next section was general device usage questions. In this section, participants were asked about their most frequently used device and why. This section was designed to get an overview picture of how participants use their devices while later sections went into their device-specific usage. Figure 4.3 shows the general device usage questions participants were asked.

Category	Questions
General Device Questions	Which device (of your personal devices) do you use the most frequently in a week?
	Why do you use that device the most often? [Choose all that apply]

Figure 4.3: General device usage questions asked in survey.

The second set of general device usage questions were asked for each device platform and are shown in Figure 4.4. These questions were asked to provide context or clarity to participant responses if necessary, such as if a participant mentioned their device was secure because of the manufacturer but did not mention the manufacturer.

Category	Questions
Device-Specific Background Questions	How frequently do you use your [laptop/desktop, smartphone, tablet] in a week?
	In a typical day, how often do you use your [laptop/desktop, smartphone, tablet]?
	Which brand is your [laptop/desktop, smartphone, tablet]?
	What do you think the potential security risks are on your [laptop/desktop, smartphone, tablet]? [Choose all that apply.]

Figure 4.4: Device-specific general background questions.

4.2.2 Mental Models

Participants were then asked to indicate their device-specific mental models by choosing from one of three choices (agree, disagree, can't decide) for each supporting perception. These questions, shown in Figure 4.5, were grouped by mental models and contained 3-4 perceptions per model. The mental models and supporting perceptions were derived from the previous study. Each perception, while identical, was customized to reflect the actual device being discussed. For example, the following perception "Security tools help protect my [laptop/desktop/smartphone/tablet]", would be modified to use the appropriate device platform but otherwise be identical.

Additionally, participants were offered three choices in an attempt to help them make a decision about whether they have a specific perception or not. For participants who selected "can't decide" for any of the answer choices were then asked to explain

Category	Questions
Device-Specific Mental Model Questions	Please indicate your level of agreement with the following statement about your [laptop/desktop, smartphone, tablet]. • I don't have enough sensitive or private information on my [laptop/desktop, smartphone, tablet] for there to be security concerns. • My [laptop/desktop, smartphone, tablet] is used for important activities so I am very aware of the security of my device and potential risks to it. • I limit access to apps that contain private information or access to important apps, such as banking apps, on my [laptop/desktop, smartphone, tablet]. • Turning off my [laptop/desktop, smartphone, tablet] or closing down the application/browser when encountering a potential security vulnerability prevents the vulnerability from affecting my device.
	Please indicate your level of agreement with the following statement about your [laptop/desktop, smartphone, tablet]. • Security tools help protect my [laptop/desktop, smartphone, tablet]. • Security tools are necessary to protect my [laptop/desktop, smartphone, tablet]. • The built in security features on my [laptop/desktop, smartphone, tablet] such as a password or biometric lock are sufficient to protect my [laptop/desktop, smartphone, tablet]. • Security tools are not a priority because they are too expensive. • Completing my task or goal is more important than the security of my [laptop/desktop, smartphone, tablet].
	Please indicate your level of agreement with the following statement about your [laptop/desktop, smartphone, tablet]. • My [laptop/desktop, smartphone, tablet] has built in protection which prevent it from being vulnerable to security risks. • Secuirty risks on my [laptop/desktop, smartphone, tablet] are a result of misclicks and mistakes I make rather than a vulnerability on my device. • My [laptop/desktop, smartphone, tablet] is not at risk for security vulnerabilities because of the brand/company that makes it.
	Please indicate your agreement with the statements below. • Browsing on the internet is the most likely reason for a security issue to occur on my [laptop/desktop, smartphone, tablet]. • Web browser tools, such as ad blockers, prevent my [laptop/desktop, smartphone, tablet] from being susceptible to web-based security risks. • Utilitzing good internet browsing practices prevent my [laptop/desktop, smartphone, tablet] from being susceptible to web-based security risks.
	Please indicate your level of agreement with the following statement about your [laptop/desktop, smartphone, tablet]. • The built in security features on application/websites such as a password or biometric lock are sufficient to protect my [laptop/desktop, smartphone, tablet]. • Downloading third party apps is risky and is a likely source for a security issue to occur on my [laptop/desktop, smartphone, tablet].
	For all the statements you selected "I can't decide" for the previous question, please briefly explain why you chose that answer. If you did not select "I can't decide for any of the answers above, please write "no" or "N/A" in the box below.

Figure 4.5: Device-specific mental model questions.

why they selected that answer. This was to determine what their mental model might actually be or to understand why they feel a particular perception did not apply to them, such as not being aware of a tool and thus having no perception of its

effectiveness.

4.2.3 Security Tools and Behaviors

Next, participants were asked to choose which security behaviors and tools they used on their device. These behaviors and tools were selected from lists of common security tools and advice [40, 17] as well as the security tools and behaviors mentioned by participants in the previous study. Overall, participants were asked to identify which of the following tools they used antivirus, ad-blocker, vpn, and/or password manager.

Participants were then asked to identify which security behaviors they actually did. These behaviors included not purchasing items on unsecured networks, not downloading files/apps from untrusted third-party sites, generating secure passwords for my accounts, using password, pin, biometric to unlock my device, using two-factor authentication where provided, regularly scanning my device for threats, and paying attention to phishing websites and unsecure connection warnings. This list was partially informed by the previous study, however it was also compiled from commonly suggested good practices for device security [19, 40, 15].

4.2.4 Factors Influencing Behavior

Lastly, participants were asked to select the factors that they consider when determining security tool and behavior usage. For each of these factors, participants were displayed two tabular lists each for security tools and behaviors. The first table for the security tools or behaviors contained a list of all of the tools or behaviors, respectively, that the participants indicated they implemented. The second table contained a list of all of the tools or behaviors, respectively, that the participants indicated they did not implement. As a result, participants viewed a total of four tables, two for security tools and two for security behaviors. Figure 4.6 shows the questions participants were asked on each device about their security tool adoption while Figure 4.7 shows

the questions participants were asked about their security behaviors on each device platform.

Category	Questions
Device-Specific Security Tools	Which security tools do you use on your [laptop/desktop, smartphone, tablet]?
	Why do you use those security tools on your [laptop/desktop, smartphone, tablet]? Please select the top three (3) most important factors you consider when deciding to use this tool.
	What factors did you consider when deciding not to use each of the following security tools on your [laptop/desktop, smartphone, tablet]? Please select the top three (3) most important factors you considered when deciding not to use each tool.

Figure 4.6: Device-specific security tools and influencing factors questions.

Category	Questions
Device-Specific Security Behaviors	Which security behaviors/actions do you use on your [laptop/desktop, smartphone, tablet]?
	Why do you use each of the following security behaviors/action on your [laptop/desktop, smartphone, tablet]? Please select the top three (3) most important factors you considered when deciding to use each behavior/ action.
	What factors did you consider when deciding not to use each of the following security behaviors/actions on your Why do you use each of the following security behaviors/action on your [laptop/desktop, smartphone, tablet]? Please select the top three (3) most important factors you considered when deciding to use each behavior/action.? Please select the top three (3) most important factors you considered when deciding not to use each behavior/action.

Figure 4.7: Device-specific security behaviors and influencing factors questions.

For each behavior and tool, participants indicated the three most influential factors of behavior that influenced them in deciding to implement, or not to implement, each security behavior and tool. As previously mentioned, these factors were selected from the most commonly repeated factors in theories for predicting user behavior and included cues to action, perceived severity, benefit of action, cost of action, self-efficacy, and ease of use [21, 16, 21, 12, 38, 17, 42]. For each factor, a short phrase was provided which summarized the meaning behind the factor. For example, the phrase "This behavior is easy to do" was representative of the ease of use factor. This phrase was

then negated to provide a reason why participants would not adopt a security tool or behavior. Participants were asked to select the three most common factors in order to narrow down their most influential factors when determining their behavior.

4.2.5 Attention Checks

There were 5 attention checks in the survey to ensure participants were paying attention to the questions. These attention checks were a combination of short answer written response questions and multiple choice questions. Specifically, there was one attention check after each mental model section asking participants to explain why they selected "can't decide" for any of the answer choices, if any. These questions acted not only as an attention check, but also helped encourage participants to carefully consider whether or not they do actually have a position regarding each supporting perception. There was also a simple attention check after the first device-specific section asking participants to select yes if they were paying attention. The last attention check was at the end of the survey asking participants if they had any additional comments. This not only acted as an attention check but also provided participants a place to include extra information they felt was relevant to their responses. Figure 4.8 shows the attention checks asked, except for the three at the end of the device-specific mental model sections.

Category	Questions
Attention Checks	We ask this question to check whether you are paying attention. Please select the "yes" to preserve your answers/continue with the survey.
	Do you have anything else to add to your response? Please write "None" if you do not want to add anything to your responses.

Figure 4.8: Attention check questions, excluding the three at the end of the device-specific mental model questions.

4.2.6 Participants

While 200 survey responses were originally collected, some survey responses were removed due to a lack of clarity or completeness when answering the written attention

check questions. As a result, there were 192 participants total, all 18 or older who own all three device platforms- traditional computing, smartphone, tablet. The usage of Prolific, a survey distribution platform, allowed for a more diverse sample than convenience sampling, that was relatively representative of the various attributes of multi-device users such as their technical experience, educational background, cultural influences, and prior experiences with security risks. Figure 4.9 shows the eligibility questions participants were asked at the start of the survey.

Category	Questions
Eligibility Questions	Are you a resident of the United States?
	Are you 18 years or older?
	Do you own or regularly use a laptop/desktop, a smartphone, and a tablet?

Figure 4.9: Eligibility questions asked in survey.

Participants were asked a set of demographic questions at the beginning of the survey including gender, race, education level, and average household income. Figure 4.10 shows the list of demographic questions participants were asked.

Figure 4.11 shows a summary of the participants' responses. However, for clarity and readability purposes, participants were counted for each of the race(s) they indicated. So, if a participant indicated they belonged to two races, they were counted twice, once for each race they belonged to. As shown in the Figure 4.11 below, approximately 78% of participants identified as White or Caucasian, with the second most common race being Asian with approximately 17% of participants identifying as so. Additionally, approximately 61% of participants were female, 36% of participants were male, and 3% were non-binary. However, the salary range and education level of the participants were generally more descriptive of the average US population with approximately 45% of participants having a salary between $25,000 and $75,000. Additionally, approximately 59% of participants had completed some level of higher education training.

Category	Questions
Demographics	Choose one or more races that you consider yourself to be.
	What is the highest level of education you have completed?
	How do you describe yourself?
	What was your total household income before taxes during the past 12 months?
	Please indicate your agreement with the statements below. • I seek out opportunities to learn about security measures that are relevant to me. • I am extremely motivated to take all the steps needed to keep my online data and accounts safe. • Generally I diligently follow a routine about security practices. • I often am interested in articles about security threats. • I always pay attention to experts advice about the steps I need to take to keep my online data and accounts safe. • I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe. • I am too busy to put in the effort needed to change my security behaviors. • I have much bigger problems than my risk of a security breach. • There are good reasons why I do not take the necessary steps to keep my online data and accounts safe. • I usually will not use security measures if they are inconvenient. • I want to change my security behaviors to improve my protection against threats (eg. phishing, computer virus, identity theft, password hacking) that are a danger to my online data and accounts.

Figure 4.10: Demographic questions asked in survey.

Race		Education Level		Gender		Household Income	
White or Caucasian	150	Some high school or less	2	Male	69	Less than $25,000	29
Black or African American	18	High school diploma or GED	24	Female	117	$25,000 - $49,999	47
American Indian/Native American or Alaska Native	3	Some college, but no degree	53	Non-binary/third gender	6	$50,000 - $74,999	39
Asian	32	Associates or technical degree	22	Prefer to self-describe	0	$75,000 - $99,999	25
Native Hawaiian or Other Pacific Islander	2	Bachelor's degree	69	Prefer not to say	0	$100,000 - $149,000	31
Other	9	Graduate or professional degree (MA, MS, MBA, PhD, JD, MD, DDS etc.)	22			$150,000 or more	17
Prefer not to say		Prefer not to say	0			Prefer not to say	4

Figure 4.11: Summary of demographics. Note: Some participants indicated more than one race, though they are displayed separately for readability purposes.

4.2.7 Analysis

We used two primary methods to analyze the data collected in the survey. First, we used descriptive statistics, such as creating graphs and tables to visualize patterns.

Next, we used statistical analysis, such as running single factor anovas and Student's t-tests to determine statistically significant variations in perception prevalence across the three device platforms.

The first step was to code the agreement with each supporting perception to determine the mental models held by each participant. To do so, participants were assigned a count for the total number of supporting perceptions they indicated they agreed with for each mental model. So, if a participant was coded "0" for a mental model, they either selected "disagree" or "can't decide" for each supporting perception, indicating they did not hold the mental model.

After the mental models were coded, bar charts were made to visualize how many participants "agreed" with each supporting perception across all three platforms, this allowed for a visual comparison of the prevalence of each perception, and mental model, on all three devices.

We then conducted single factor anova's on each of the perceptions for each mental model to determine if the device platform has a statistically significant effect on the adoption of a perception ($p >= 0.5$) and to test the following hypotheses.

- H_0 2.1: There are no variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.
- H_A 2.1: There are statistically significant variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.

For each of the perceptions that were found to have statistically significant variation in prevalence through the single factor anova, we conducted a two-tailed Student's t–test between each pair of perceptions to determine which platforms were causing the statistically significant variation. These platform pairs were Laptop/Smartphone, Smartphone/Tablet, and Laptop/Tablet. Because there were three hypotheses being tested for each perception, the Bonferroni method was used to adjust for the family-

wise error rate problem. As a result, the resulting significance level for the Student's t-tests became 0.017 (0.05 / 3 = 0.0167).

To compare the factors that influenced adoption of security tools and behaviors, the first step was to calculate how many participants selected each factor for each tool. As participants only chose their top three factors, not all factors were selected by each participant. After compiling these totals, a bar chart was made comparing the prevalence of each factor across the security tools and behaviors on each platform. This allowed for a visual understanding of the most common factors that influence behavior on each platform and a comparison of these factors influence on the platforms.

To compare the actual security tools and behaviors adopted on each platform, a table was created describing the total number of participants who indicated they used the respective tool or behavior on each platform.

Lastly, to determine the potential correlation between indicated mental models of security and actual security behavior adoption and test the following hypotheses, the Pearson correlation coefficient was calculated between each security tool and behavior and each mental model.

1. H_0 2.2: There is no correlation between device-specific mental models and the adoption of security behaviors on each device platform.

2. H_A 2.2: There is a statistically significant correlation between device-specific mental models and the adoption of security behaviors on each device platform

To do so, participants were coded as having a mental model (1) or not (0) depending on the total number of supporting perceptions they held. If participants agreed with approximately half of the supporting perceptions, they were determined to have the corresponding mental model. In other words, if there were 5 supporting perceptions for a mental model, participants were coded as having the mental model if they agreed with 3 or more perceptions. This was also the case if participants agreed with 3 or

more out of 4 perceptions, 2 or more out of 3 perceptions, and 1 or more out of 2 perceptions.

4.2.8 Limitations

One limitation of this study was the lack of ability for users to indicate additional factors or mental models they consider when deciding which security behaviors to take or security mechanisms to use on their devices due to the lack of an interview with the participants. However, the larger number of participants does contribute to the generalize-ability of the results.

Another limitation of the study was the limited coding range of the data, leading to similar ranges of data values between the held mental models (0 or 1) and the adopted security behaviors or tools (0 or 1). The similarity in the ranges of these variables limited the ability to calculate a correlation coefficient. Nevertheless, while we were unable to determine a statistical correlation between mental models and adopted behavior, our results do indicate patterns between prevalent mental models, most common factors influencing behavior, and the adopted security behaviors across all three device platforms.

4.3 Results

The following sections contain the qualitative and quantitative analysis of the survey results, broken down by research question. The first section provides background information about the participants' general weekly device usage. The second section looks at the differences and similarities in mental models of security across the three device platforms. The third and fourth sections look at the differences and similarities in factors that influence behavior across all three device platforms as well as actual security behaviors. The last section looks at the correlations between mental models of security and actual security behaviors across all three device platforms.

4.3.1 General Device Usage

As seen in Figure 4.12, more participants indicated they used their smartphone the most frequently in a week, followed by laptop/desktop then tablet. Additionally, as seen in Figure 4.13, the most common reason participants selected a device to use most often was that the device was the most convenient device. The second most common reason was that they always have the device on hand.

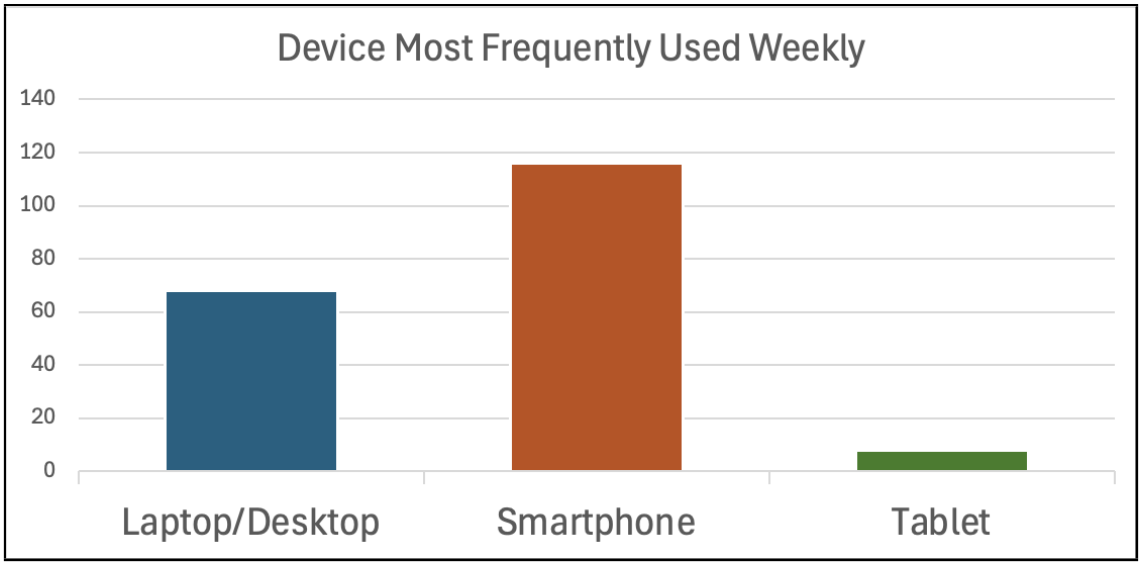

Figure 4.12: Frequency of the weekly most commonly used device by device platform.

4.3.2 Mental Models and Perceptions

As part of the analysis process, the following graphs were created to illustrate the number of people who agreed, or indicated they had, each of the perceptions for each mental model. In other words, each graph below represents one mental model. The y-axis contains values for each perception within that mental model. The bars represent the number of participants for each device platform. Blue bars are responses for the laptop/desktop platform, green bars are responses for the smartphone platforms, and grey bars are responses for the tablet platform.

Additionally, single factor anovas were conducted for each supporting perception to determine which perceptions had statistically significant variability. The p-values for

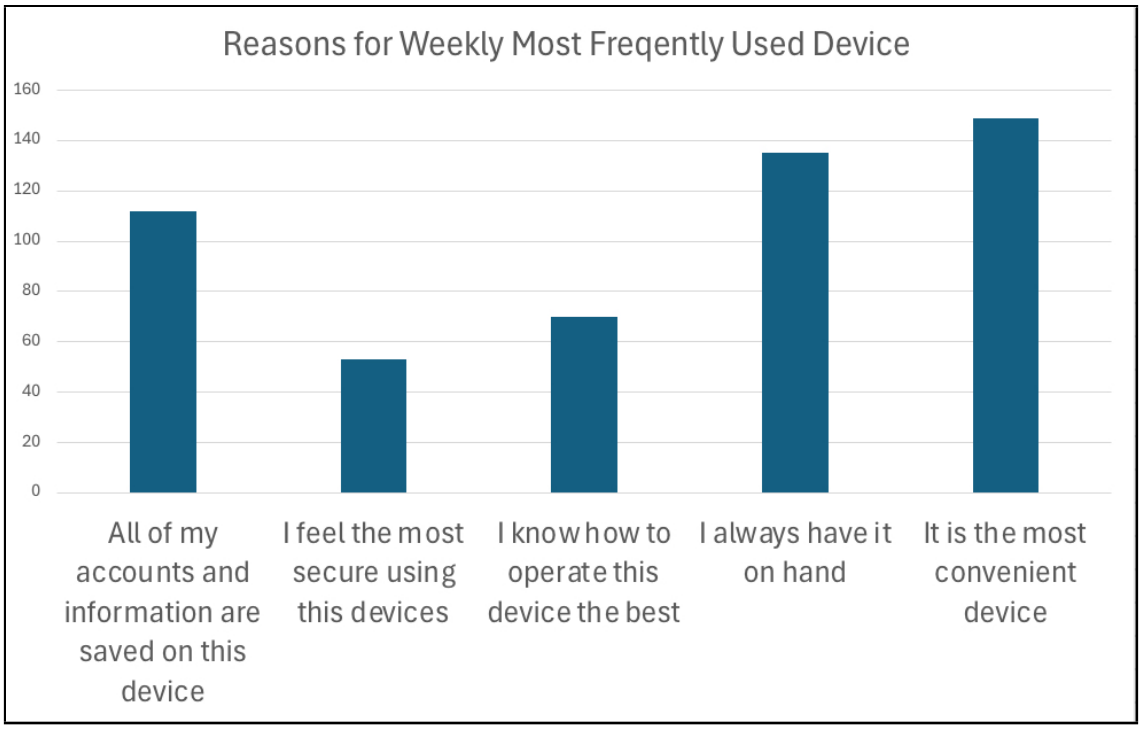

Figure 4.13: Reasons for selecting to use a device more often in a week.

these anova's are shown in Figure 4.14.

As seen in Figure 4.14, there were single factor anovas for 8 perceptions with a statistically significant p-value ($p<=0.05$). These statistically significant p-values indicate the choice of device platform does effect the belief in a perception for these platforms. However, it does not indicate which device platform is causing the variance, only that there is a variance in perception adoption means across platforms. As a result, we conducted Student's t-test on each of the device platform pairs for the perceptions with a statistically significant p-value in the single-factor anova with the results shown in Figure 4.15. As there are three pairs of device platforms that were tested for each of these perceptions, the Bonferroni method was used to adjust for the family-wise error rate problem with testing three hypothesis for each perception. As a result, the resulting significance level became $p<=0.017$ ($0.05 / 3 = 0.0167$).

The first graph (Figure 4.16) corresponds to the mental model "Limited risk due to usage". This mental model contains various perceptions regarding how the frequency

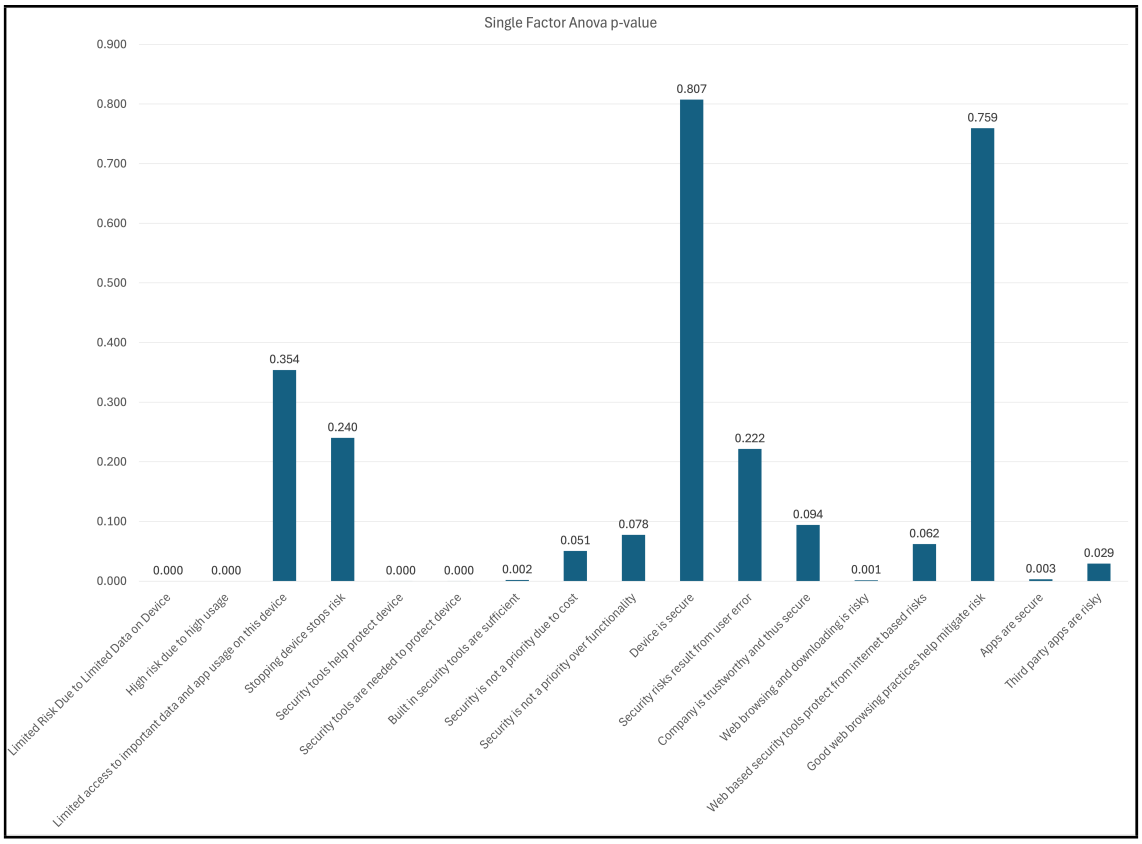

Figure 4.14: P-values for the single factor anovas conducted for each perception.

and purpose they use their device for influences the amount of security risks they face on their device. As shown in the graph below, more participants indicated they agreed with this mental model on tablets overall. However, the "Limited access to important data and app usage on this device" and "stopping device stops risk" perceptions were reported by participants to be similarly held on all three device platforms while the perception "High risk due to high usage" was held by more participants on smartphones and laptops than tablets. Additionally, the "limited risk due to limited data on device" and "high risk due to high usage" perceptions, were found to have statistically significant variability between platforms. The t-tests for these perceptions found that for both of these perceptions, there was statistically significant variability between between tablets and the other two device platforms. This indicates users generally have the mental model that tablets are not at risk to

Survey Items		Pairwise comparison statistics					
		M	SD	t	p	d	df
Limited Risk Due to Limited	Laptop (192) / Smartphone (192)	0.182/0.156	0.387/0.364	0.78	0.436	0.69	191
	Smartphone (192) / Tablet (192)	0.156/0.547	0.364/0.499	-10.023	**0.000**	-0.894	191
	Tablet (192) / Laptop (192)	0.182/0.547	0.387/0.499	-9.13	**0.000**	-0.816	191
High risk due to high usage	Laptop (192) / Smartphone (192)	0.760/0.813	0.428/0.391	-1.513	0.132	-0.127	191
	Smartphone (192) / Tablet (192)	0.813/0.385	0.391/0.488	10.65	**0.000**	0.966	191
	Tablet (192) / Laptop (192)	0.760/0.385	0.428/0.488	9.047	**0.000**	0.817	191
Security tools help protect	Laptop (192) / Smartphone (192)	0.917/0.823	0.277/0.383	3.374	**0.001**	0.281	191
	Smartphone (192) / Tablet (192)	0.823/0.724	0.383/0.448	3.198	**0.002**	0.237	191
	Tablet (192) / Laptop (192)	0.917/0.724	0.277/0.448	5.997	**0.000**	0.517	191
Security tools are needed to	Laptop (192) / Smartphone (192)	0.854/0.729	0.354/0.446	3.738	**0.000**	0.311	191
	Smartphone (192) / Tablet (192)	0.729/0.630	0.446/0.484	2.704	**0.007**	0.213	191
	Tablet (192) / Laptop (192)	0.854/0.630	0.354/0.484	6.104	**0.000**	0.528	191
Built in security tools are	Laptop (192) / Smartphone (192)	0.458/0.526	0.500/0.501	-1.731	0.085	-0.135	191
	Smartphone (192) / Tablet (192)	0.526/0.635	0.501/0.483	-3.001	**0.003**	-0.222	191
	Tablet (192) / Laptop (192)	0.458/0.635	0.500/0.483	-4.175	**0.000**	-0.361	191
Web browsing and	Laptop (192) / Smartphone (192)	0.755/0.589	0.431/0.493	4.575	**0.000**	0.36	191
	Smartphone (192) / Tablet (192)	0.589/0.625	0.493/0.485	-1.021	0.308	-0.074	191
	Tablet (192) / Laptop (192)	0.755/0.625	0.431/0.485	3.466	**0.001**	0.284	191
Apps are secure	Laptop (192) / Smartphone (192)	0.417/0.516	0.494/0.501	-2.65	**0.009**	-0.199	191
	Smartphone (192) / Tablet (192)	0.516/0.589	0.501/0.493	-2.13	0.034	-0.147	191
	Tablet (192) / Laptop (192)	0.417/0.589	0.494/0.493	-4.136	**0.000**	-0.348	191
Third party apps are risky	Laptop (192) / Smartphone (192)	0.870/0.802	0.337/0.399	1.998	0.047	0.183	191
	Smartphone (192) / Tablet (192)	0.802/0.766	0.399/0.425	1.094	0.275	0.088	191
	Tablet (192) / Laptop (192)	0.870/0.766	0.337/0.425	3.328	**0.001**	0.272	191

Figure 4.15: Pairwise comparison statistics for perceptions with a statistically significant anova. Note: Statistically significant p-values are bolded ($p<=0.017$).

security vulnerabilities because they are not used frequently and/or for important tasks or applications. However, the opposite seems to apply to smartphones and laptops with users viewing them as at risk for security vulnerabilities due to the frequency they are utilized.

The second graph (Figure 4.17), shown below, corresponds to the mental model "Security tools are used to mitigate risk". This mental model contains various perceptions regarding users' understanding of the role and importance of security tools in protecting their data and devices. As shown in the graph below, more participants indicated they agreed with this mental model on laptops and tablets overall. However, the prevalence of these perceptions was divided by the inherent type and functionality of security tools. For example, "built in security tools are sufficient" was statistically more prevalent on tablets than on laptops and smartphones. For the "security tools help protect device" and"security tools are needed to protect device" perceptions, there

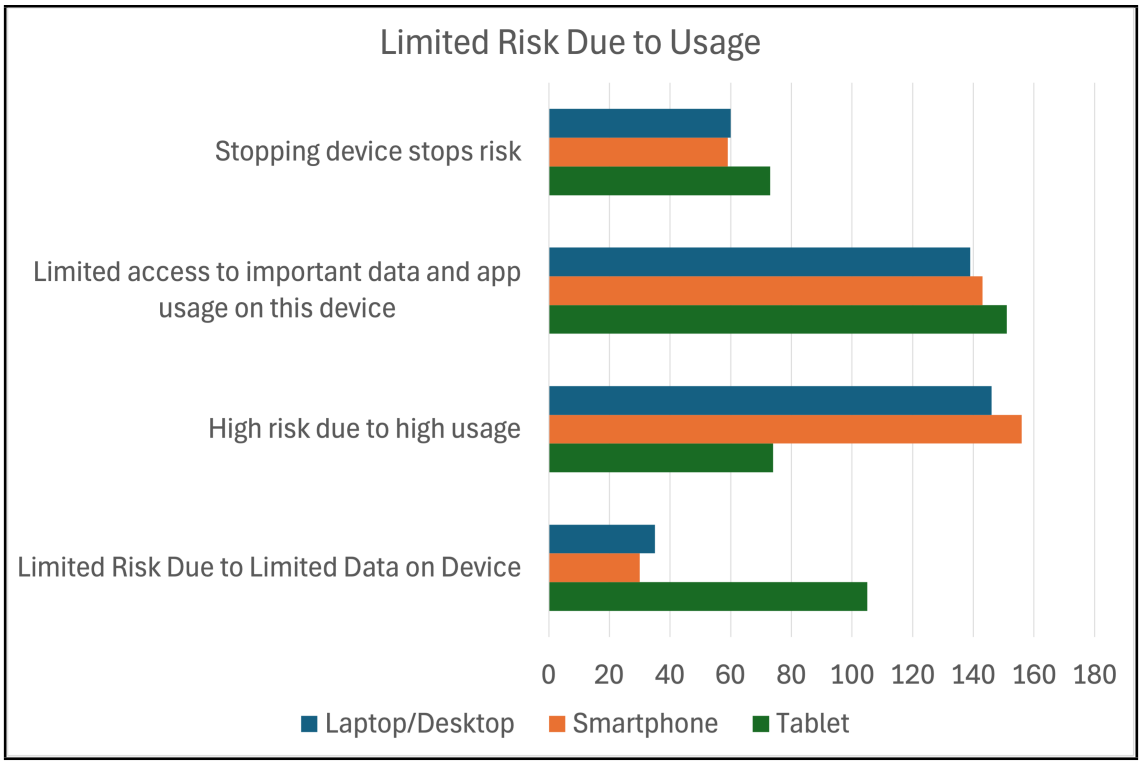

Figure 4.16: Frequency of perceptions within the "Limited risk due to usage" mental model by platform

was a statistically significant difference observed between all three device platforms. In other words, both of these perceptions were statistically more prevalent on laptops, followed by smartphones, and then followed by tablets. These results indicate users generally have more awareness of the need for security tools on laptops than on smartphones and tablets.

The third graph (Figure 4.18) corresponds to the mental model "Platform is secure". This mental model contains various perceptions regarding the security of their device due to factors such as the manufacturer and built-in security measures. In general, more participants indicated they agreed with this mental model on tablets. However, none of the relationships between the device platforms were found to be statistically significant for any of the supporting perceptions. Thus, while more participants indicated they perceived the security of the tablets was the result of the manufacturer and any built-in security measures and any risks result from their own action rather

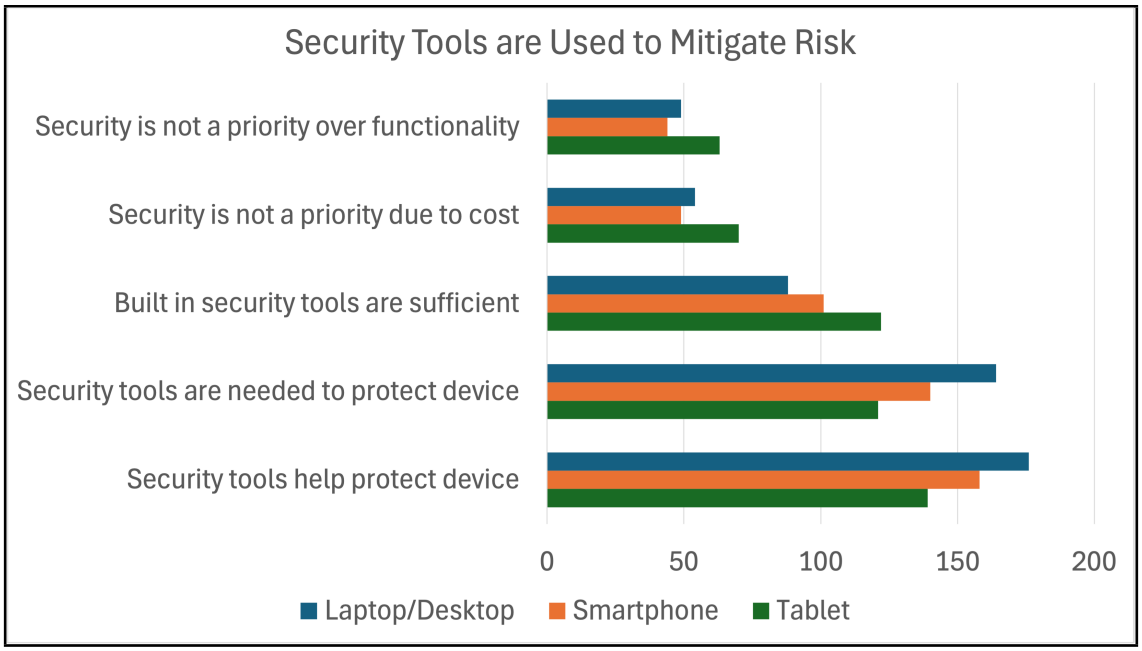

Figure 4.17: Frequency of perceptions within the "Security tools are used to mitigate risk" mental model by platform

than any vulnerabilities in their device, this cannot be concluded and would require further research to establish a statistically significant relationship.

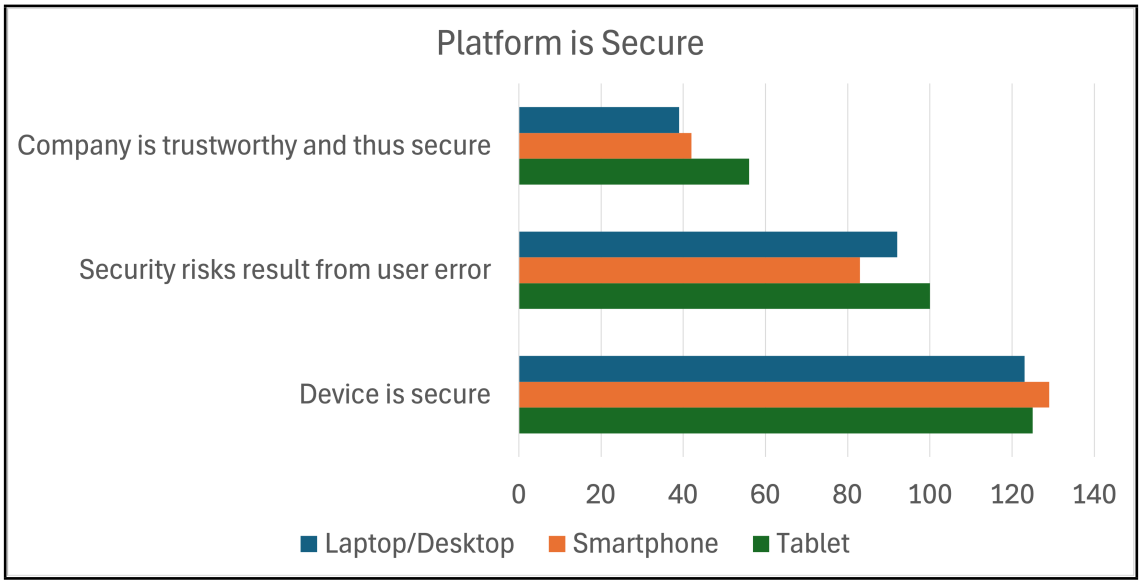

Figure 4.18: Frequency of perceptions within the "Platform is secure" mental model by platform

The fourth graph (Figure 4.19) corresponds to the mental model "Web browsing and

downloading is risky". This mental model contains various perceptions regarding the risks and security measures associated with browsing and downloading on the internet. More participants indicated they agreed with this mental model on traditional computing devices. Additionally, the "web browsing and downloading is risky" perception was statistically more prevalent on laptops/desktops than the other two device platforms. This pattern indicates participants generally perceive traditional computing devices as more at risk for security vulnerabilities from web-based behaviors.

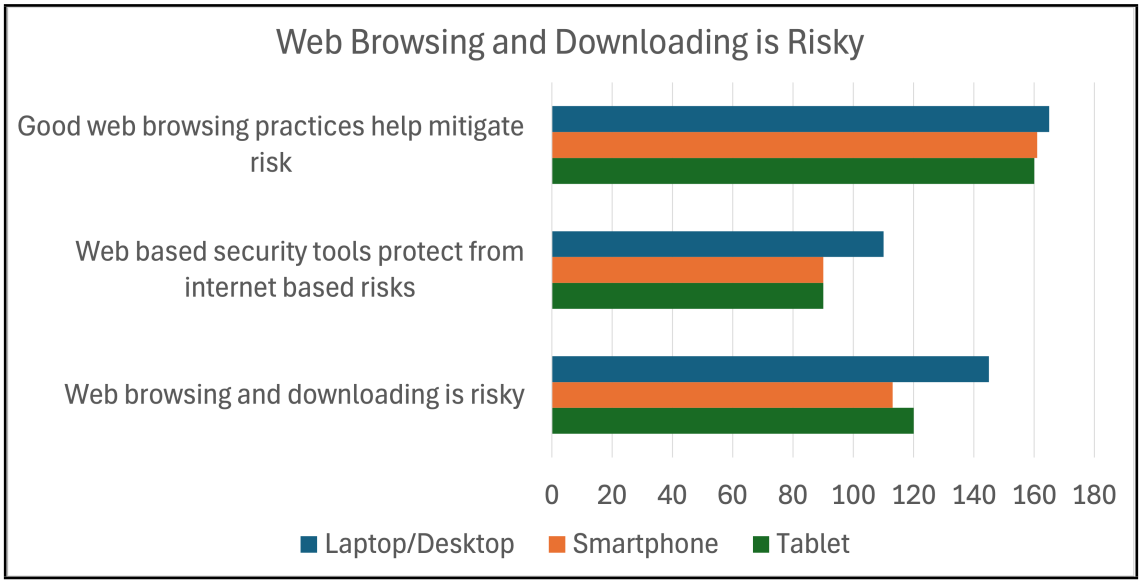

Figure 4.19: Frequency of perceptions within the "Web browsing and downloading is risky" mental model by platform

The fifth graph (Figure 4.20) corresponds to the mental model "Applications are secure". This mental model contains various perceptions regarding the inherent security and security responsibilities associated with device applications. The perception, "applications as more secure", was found to be statistically less prevalent on laptops when compared to the other two device platforms. Additionally, the perception, "third party apps are risky", was found to be statistically more prevalent on laptops than tablets, but not smartphones. These patterns indicate the general perception that applications, including third-party applications, are more secure on tablets and smartphones than traditional computing devices. This likely corresponds to the

prevalent usage of downloaded applications on smartphones and tablets compared to the usage of browser-based and native applications on traditional computing devices.

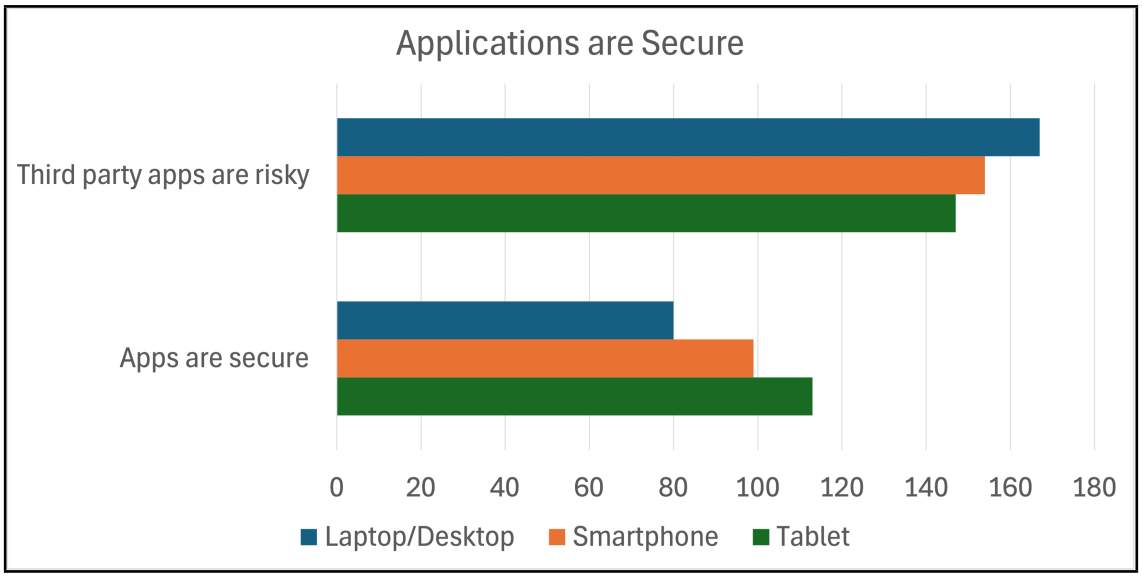

Figure 4.20: Frequency of perceptions within the "Applications are secure" mental model by platform

These graphs show a few interesting things. The first is that the responses for each of the device platforms have both similarities and differences with consistencies appearing with the perceptions that are prevalent on each device platform. One of these similarities is that there is limited difference in total frequency of the perceptions between the platforms aside from the first 2 mental models, "Limited risk due to limited usage" and "Security tools are used to mitigate risk".

However, within these two mental models, there was a perception with quite a large variability, "Limited risk due to limited data on device". This perception was much more prevalent on tablets than on the other device platforms, indicating participants generally perceive their tablets as inherently secure because they are used for fewer tasks and store less, if any, sensitive or personal data.

Another pattern that appeared across the mental models was the awareness of the need for security tools on traditional computing devices to protect the devices and the user's personal data, but not as much awareness of the need for security tools

on other platforms. This is shown in the prevalence of the perceptions "Web based security tools protect from internet based risks", "Security tools help protect devices", and "Security tools are needed to protect device" on traditional computing devices compared to the other device platforms. The prevalence of these perceptions indicate that participants view device-based and web-based security tools are more beneficial and necessary on traditional computing devices followed by smartphones followed by tablets.

This is further supported by the lack of participants with the perceptions "Built in security tools are sufficient", "Company is trustworthy and thus secure", and "Apps are secure" on traditional computing devices compared to tablets followed by smartphones. The lack of prevalence of these perceptions combined with the prevalence of the previously mentioned perceptions indicates that participants generally do not view traditional computing devices or the applications on them as secure without additional support and protections from security tools. However these patterns also show the opposite to be true on tablets and smartphones, with participants generally viewing tablets, followed by smartphones, as secure without the additional support of security tools.

Section 4.3.2 Key Takeaways: Partially support H_A 2.1 and found there are statistically significant variances between device platforms for 8 supporting perceptions.

4.3.3 Factors Influencing Security Tool Adoption

The following graphs were created during the analysis process to indicate which factors were more influential in deciding on the usage of a security tool. These graphs only consider the top 3 factors influencing the actual usage of a security tool. Furthermore, the graphs are divided by device platform with traditional computing devices described first followed by smartphones and then tablets.

The first graph (Figure 4.21) shows which factors were the most influential by

security tool on traditional computing devices. As shown, the most influential factors on a laptop or desktop were "This tool is easy to install and setup", "This tool is affordable to use", "I know how to use this tool to protect my information", and "This tool is effective in protecting myself and my information" roughly in that order for each tool. The most common factor influencing adoption was "This tool is easy to install and setup".

Some participants also indicated they were using the tool in response to an actual/suspected risk or because they were required to. Additionally, the three most commonly used tools on a laptop/desktop were ad-blockers, antivirus software, and password managers in that order.

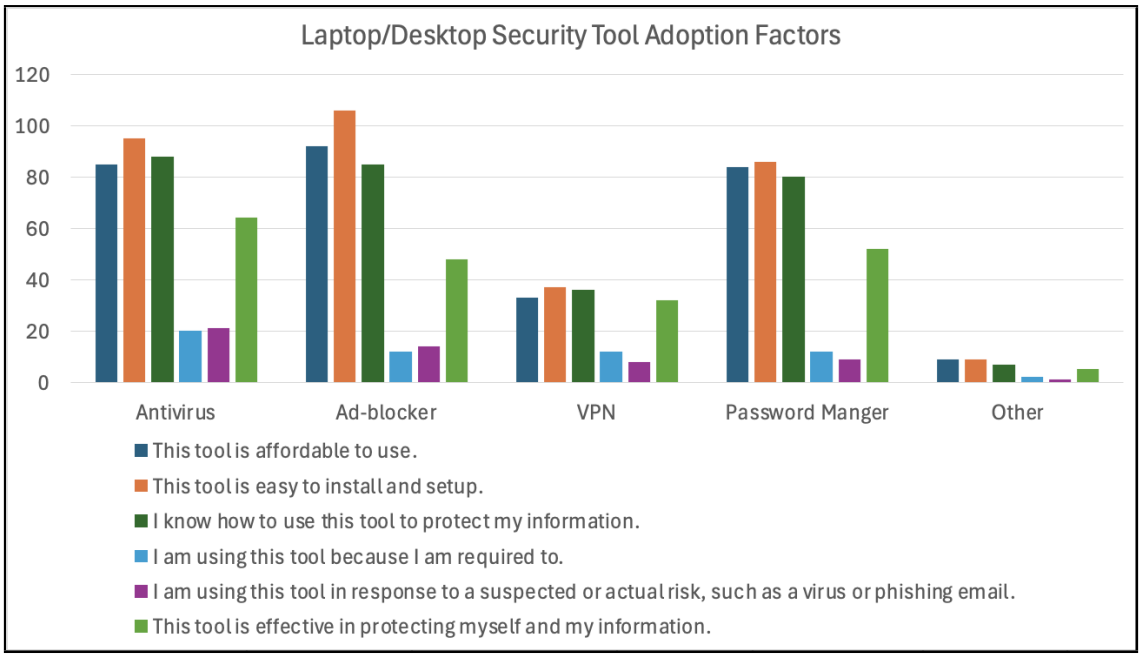

Figure 4.21: Actual security tool usage and the influencing factors on traditional computing devices

The second graph (Figure 4.22) shows which factors were the most influential by security tool on smartphones. Similar to traditional computing devices, the most influential factors on a smartphone were "This tool is easy to install and setup", "This tool is affordable to use", "I know how to use this tool to protect my information", and

"This tool is effective in protecting myself and my information", roughly in that order. However, unlike with traditional computing devices, the first two factors do switch places in prevalence amongst the security tools. Additionally, the most commonly used security tool on a smartphone was a password manager, though ad-blockers and antivirus software were the next most commonly used tools, respectively.

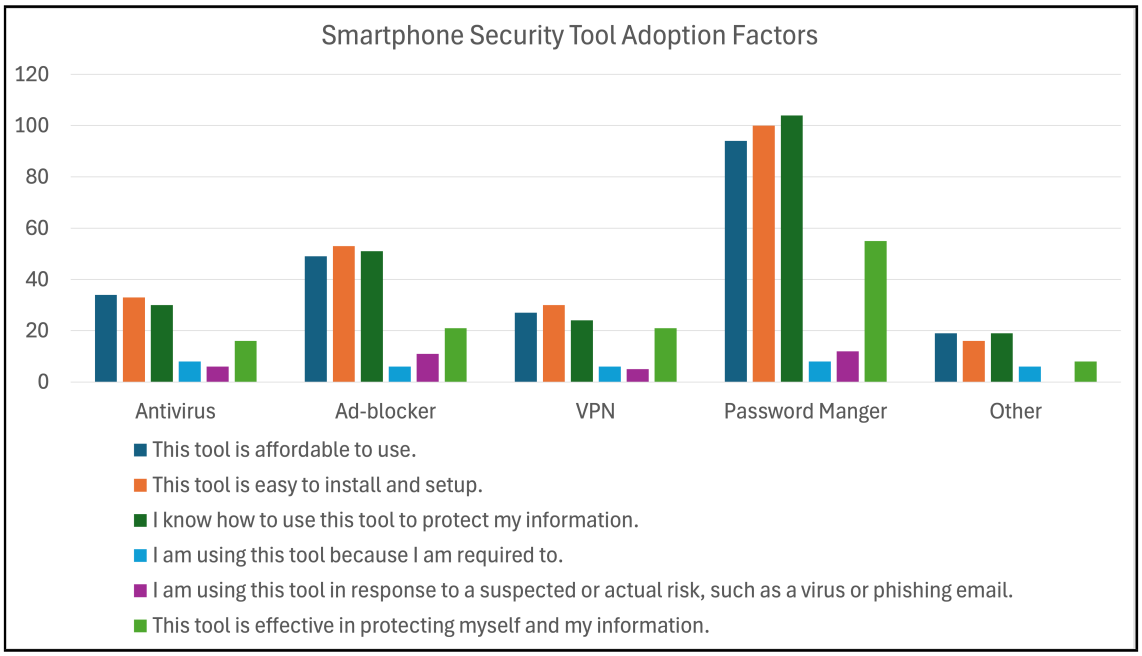

Figure 4.22: Actual security tool usage and the influencing factors on smartphones

The third graph (Figure 4.23) shows which factors were the most influential by security tool on tablets. Like the previous two device platforms, the most influential factors on a smartphone were "This tool is easy to install and setup", "I know how to use this tool to protect my information", "This tool is affordable to use", and "This tool is effective in protecting myself and my information", roughly in that order. While the order of prevalence of these factors does fluctuate across the tools, the most common factor influencing adoption of a tool on a tablet was "This tool is easy to install and setup". Additionally, the most commonly used security tool on a tablet was a password manager, followed closely by an ad-blocker then an antivirus software.

There are a few interesting patterns in the factors influencing tools adoption as

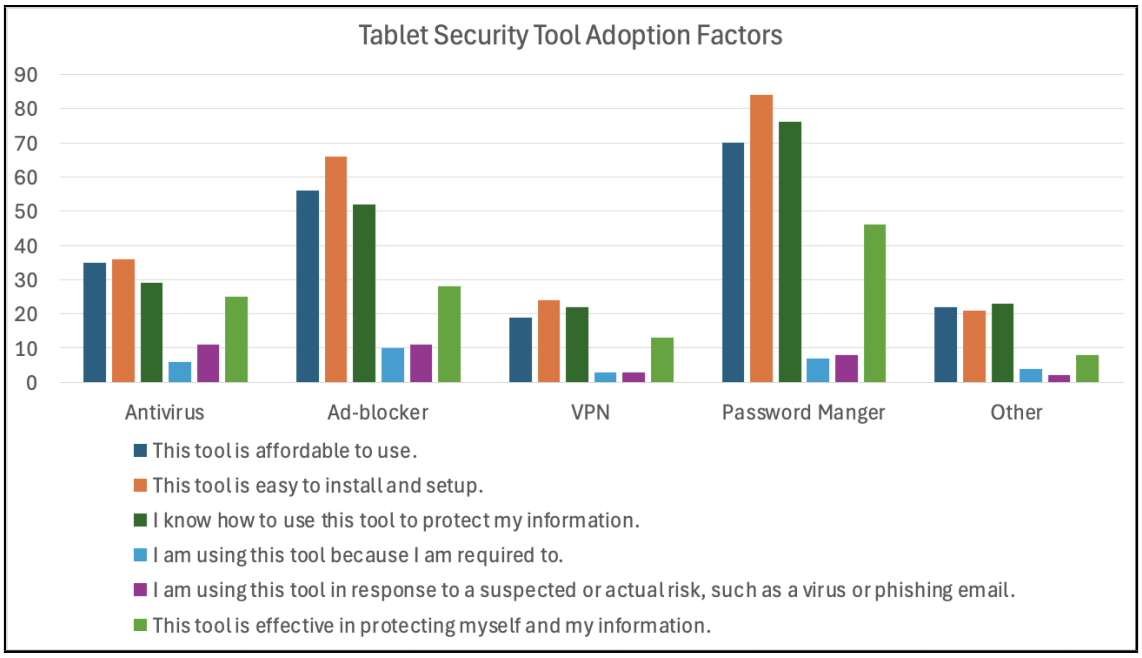

Figure 4.23: Actual security tool usage and the influencing factors on tablets

well as the tools actually used on each platform. The first was the commonalities in the three most influential factors when deciding security tool adoption on each device platform. On all three platforms, the most influential factors were "This tool is easy to install and setup", "I know how to use this tool to protect my information", "This tool is affordable to use". The prevalence of these factors illustrates the importance participant place on self-efficacy, ease of use, and the cost of the action when determining which security tools to adopt.

While the influential order of the factors did vary from tool to tool and platform to platform, in general the most influential factor was "This tool is easy to install and setup". The prevalence of this factor illustrates the high importance users place on ease of use of a tool over factors such as potential risk or benefits. However, the fourth most common factor on all three device platforms was "This tool is effective in protecting myself and my information". While this factor is less prevalent, it does show that users are considering the benefit of adopting the tool, at least to some extent, when determining their behavior.

Another interesting pattern was the similarities and differences in tool adoption across the three platforms. Specifically, the most common security tool used on smartphones and tablets was a password manager while the most commonly used security tool on traditional computing devices was an ad-blocker. However, more participants were using an ad-blocker on tablets than on smartphones. This indicates that security perceptions and security tool implementation on tablets may be primarily influenced by smartphone mental models of security but also influenced by traditional computing device mental models due to the similarities in tool adoption and the influential factors of adoption.

Section 4.3.3 Key Takeaways: There are device-specific variances in security tool implementation with more security tools being adopted on laptops.

4.3.4 Factors Influencing Security Behavior Implementation

The following graphs were created during the analysis process to indicate which factors were more influential in deciding on the implementation of a security behavior. These graphs only consider the top 3 factors influencing the actual implementation of a security behavior. Furthermore, the graphs are divided by device platform, just like the previous section.

The first graph (Figure 4.24) shows the adopted security behaviors on traditional computing devices and the most influential factors in determining adoption. The second graph (Figure 4.25) shows the adopted security behaviors on smartphones and the most influential factors in determining adoption. The third graph (Figure 4.26) shows the adopted security behaviors on tablets and the most influential factors in determining adoption.

As shown, the most influential factor across all the security behaviors on each device platform was "This behavior protects myself and my information". This shows that unlike with the security tools, one of the primary factors users consider when

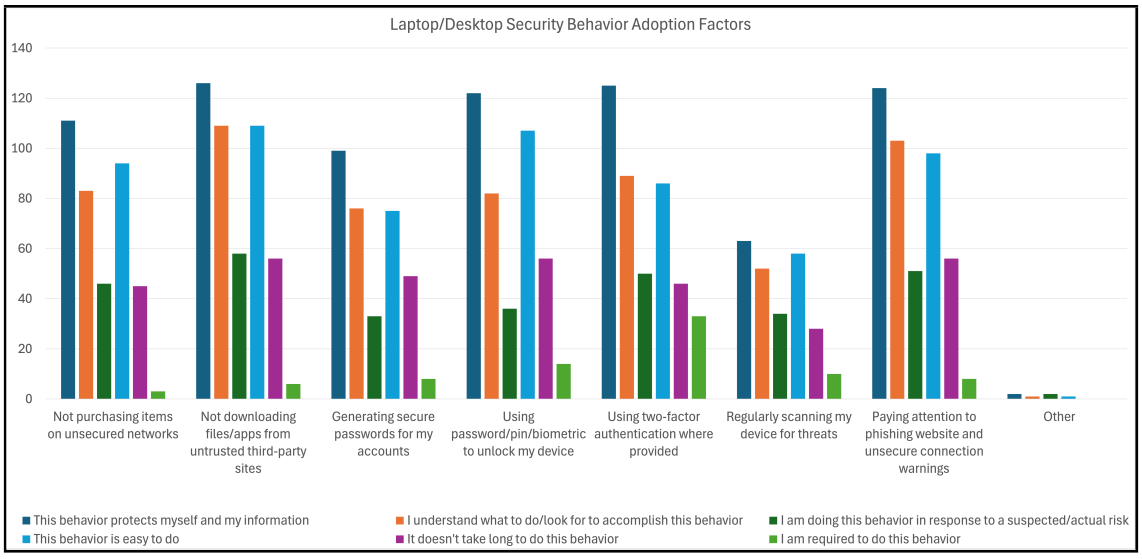

Figure 4.24: Actual security behavior implementation and the influencing factors on traditional computing devices

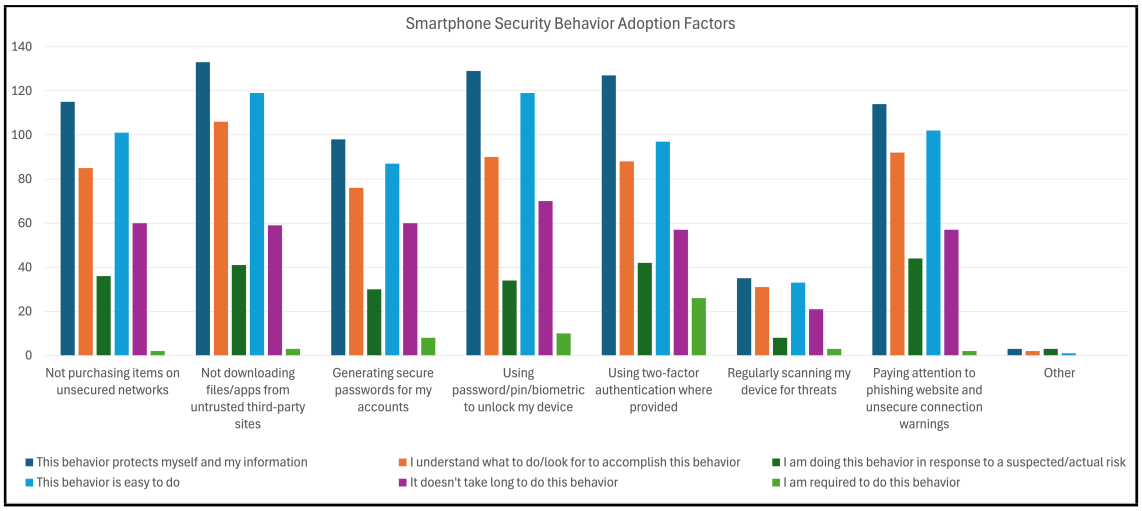

Figure 4.25: Actual security behavior implementation and the influencing factors on smartphones

determining adoption of a security behavior is the benefit of that action.

Other factors which varied in prevalence by security behavior but were still relatively prevalent across all three platforms and all security behaviors were "I understand what to do/look for to accomplish this behavior", "This behavior is easy to do", "It doesn't take long to do this behavior", and "I am required to do this behavior". The prevalence of these factors indicates that users also place importance on self-efficacy,

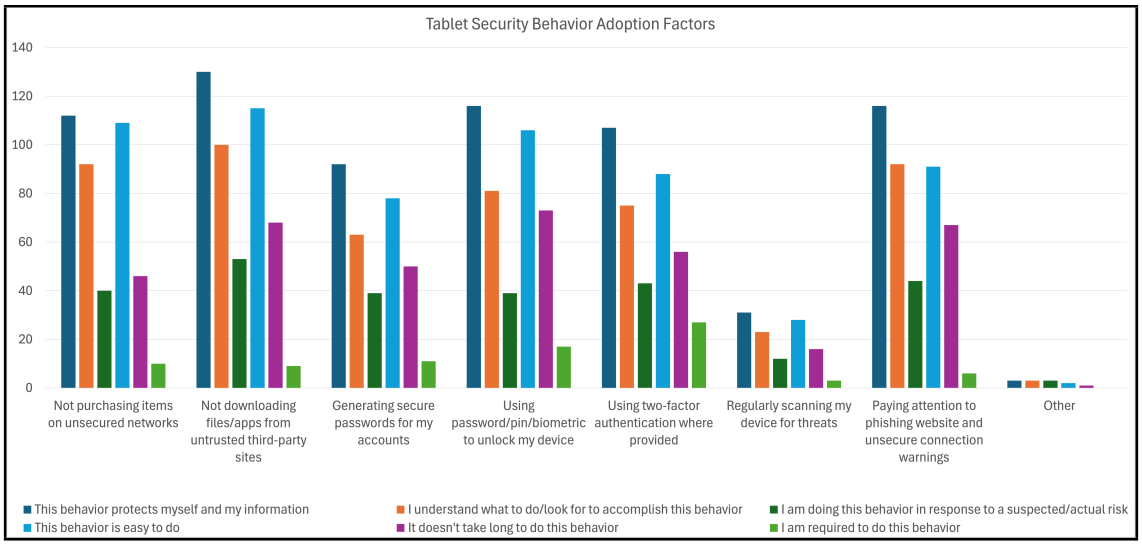

Figure 4.26: Actual security behavior implementation and the influencing factors on tablets

ease of use, cost of the action, and cues to action when determining security behavior adoption.

While there were many similarities in the security behaviors adopted on each device platform and the factors influencing those decisions on each platform, users' security behaviors and considerations on tablets is more similar to those on smartphones than traditional computing devices. This indicates that security behaviors on tablets is more likely to be influenced by smartphone security behaviors and perceptions than traditional computing devices.

Section 4.3.4 Key Takeaways: Adopted security behaviors were generally similar across the device platforms.

4.3.5 Correlating Security Behavior

The tables below show the correlation coefficient calculated between each mental model and security tool or behavior on each platform. Figure 4.27 shows the correlation coefficient between each mental model and security tool on laptops. Figure 4.28 shows the correlation coefficient between each mental model and security tool on smartphones.

Figure 4.29 shows the correlation coefficient between each mental model and security tool on tablets. Figure 4.30 shows the correlation coefficient between each mental model and security behavior on laptops. Figure 4.31 shows the correlation coefficient between each mental model and security behavior on smartphones. Figure 4.32 shows the correlation coefficient between each mental model and security behavior on tablets.

In addition to the correlation coefficient, the p-value of each correlation was calculated with a paired two-tailed t-test. The correlation coefficients which were found to be statistically significant ($p<=0.05$) are bolded in each of the tables below. As seen in the tables below, the correlation coefficients vary between negative and positive values but do not exceed -0.2 or 0.2. However, most of the correlations coefficients are statistically significant. As a result, while it cannot be concluded that there is a correlation between a mental model and a participant's adoption of a security tool or behavior on any of the device platforms, it can be concluded that the observed relationship between the majority of the mental models and adopted security tools/behaviors is not by chance due to the p-value being statistically significant ($p<=0.05$). A power analysis conducted after the study indicates that the sample size of the survey could be a contributing factor in the lack of a correlation between these variables. As a result, some of the larger correlation coefficients (positive or negative), could be indicative of a stronger correlation between mental models and security tool/behavior adoption if the survey was conducted again with a larger sample size.

Positive correlations generally mean that the two variables (mental model and security tool or behavior) are increasing together. This indicates that for the relationships with a positive correlation, there is a possibility of the user adoption of a mental model correlating to the adoption of a security tool or behavior or user adoption of a security tool or behavior correlating to the belief in a specific mental model of security in a larger sample. Conversely, the negative correlations generally mean that while the value of one variable is increasing, the other is decreasing. As such, negative

correlation coefficients indicate the possibility of user adoption of a specific mental model of security decreasing the likelihood of the adoption of a specific security tool or behavior or the adoption of a specific security tool or behavior decreasing the likelihood of user belief in a specific mental model of security.

However, the closeness of each of the calculated correlation coefficients to 0 indicates there is a very weak to negligible correlation between the two variables. As such, relational statements between adoption of mental models of security and security tools and behaviors would require future research with a larger sample size to confirm the existence of a positive or negative correlation.

Security Tool	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Antivirus	**0.036**	-0.086	**-0.222**	**0.144**	**-0.111**
Ad-blocker	**-0.082**	-0.061	**0.054**	**0.121**	**-0.033**
VPN	0.032	**-0.015**	**-0.083**	**0.069**	**0.009**
Password Manager	**-0.034**	-0.060	**-0.152**	**0.035**	**0.068**
Other	**-0.143**	**-0.067**	**0.000**	**-0.173**	**0.061**

Figure 4.27: Correlation coefficients between adoption of mental models and security tools on traditional computing devices. Note: Statistically significant correlation coefficients are in bold ($p<=0.05$).

Security Tool	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Antivirus	0.042	**-0.081**	**-0.197**	**0.015**	**0.015**
Ad-blocker	0.095	**0.026**	**0.051**	**0.160**	**0.050**
VPN	**-0.020**	**0.102**	**-0.005**	**0.046**	**0.164**
Password Manager	**-0.069**	**-0.068**	**-0.023**	-0.114	**-0.014**
Other	**0.017**	**-0.004**	**0.057**	**0.039**	**-0.038**

Figure 4.28: Correlation coefficients between adoption of mental models and security tools on smartphones. Note: Statistically significant correlation coefficients are in bold ($p<=0.05$).

Security Tool	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Antivirus	0.034	**-0.084**	**-0.115**	**-0.015**	**0.017**
Ad-blocker	0.160	**0.043**	**0.013**	**0.026**	**-0.009**
VPN	**-0.042**	**0.114**	**0.055**	**0.115**	**-0.120**
Password Manager	**0.022**	-0.071	-0.083	**0.081**	**0.169**
Other	**-0.054**	**-0.094**	**0.057**	**-0.099**	**-0.082**

Figure 4.29: Correlation coefficients between adoption of mental models and security tools on tablets. Note: Statistically significant correlation coefficients are in bold ($p<=0.05$).

Security Behavior	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Not purchasing items on unsecured networks	**-0.025**	-0.197	**-0.087**	**0.144**	**0.028**
Not downloading files/apps from untrusted third-party sites	**-0.022**	**-0.163**	**0.026**	-0.004	**0.111**
Generating secure passwords for my accounts	**-0.053**	-0.137	**-0.071**	**-0.054**	**-0.011**
Using password/pin/biometric to unlock my device	**-0.161**	**-0.036**	**-0.110**	**0.119**	**-0.029**
Using two-factor authentication where provided	**-0.055**	**-0.028**	**-0.046**	0.052	**-0.021**
Regularly scanning my device for threats	**-0.003**	**-0.048**	-0.222	**0.049**	**-0.093**
Paying attention to phishing website and unsecure connection warnings	**-0.174**	**-0.124**	**-0.089**	0.036	**-0.015**
Other	**-0.063**	**0.094**	**-0.084**	**-0.076**	**-0.185**

Figure 4.30: Correlation coefficients between adoption of mental models and security behaviors on traditional computing devices. Note: Statistically significant correlation coefficients are in bold (p<=0.05).

Security Behavior	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Not purchasing items on unsecured networks	**-0.058**	**0.008**	**0.019**	**0.015**	**0.112**
Not downloading files/apps from untrusted third-party sites	**-0.169**	**0.030**	**-0.039**	0.082	**0.088**
Generating secure passwords for my accounts	**-0.112**	-0.140	**-0.131**	-0.118	**0.030**
Using password/pin/biometric to unlock my device	**-0.151**	**-0.018**	**0.104**	0.039	**0.039**
Using two-factor authentication where provided	**-0.050**	**0.007**	**0.112**	0.039	**0.014**
Regularly scanning my device for threats	0.061	**-0.018**	**-0.105**	**0.077**	**-0.062**
Paying attention to phishing website and unsecure connection warnings	**-0.104**	**-0.026**	**-0.122**	0.016	**0.052**
Other	**0.010**	**0.041**	**-0.023**	**-0.003**	**0.043**

Figure 4.31: Correlation coefficients between adoption of mental models and security behaviors on smartphones. Note: Statistically significant correlation coefficients are in bold (p<=0.05).

Overall, the results indicated a very weak to no correlation between each mental model of security and each security tool or behavior when conducting the Linear Correlation Coefficient between the adoption of each mental model and the implementation of each security tool and behavior on each device platform. However, this was possibly a result of the sample size or the similarity in ranges for each of the variables rather than a complete lack of correlation as the majority of the correlation

Security Behavior	Limited risk due to usage	Security tools are used to mitigate risk	Platform is secure	Web browsing and downloading is risky	Applications are secure
Not purchasing items on unsecured networks	**0.079**	**0.046**	**-0.071**	**-0.015**	**0.049**
Not downloading files/apps from untrusted third-party sites	**-0.090**	**-0.046**	**-0.160**	**-0.044**	**0.094**
Generating secure passwords for my accounts	**0.037**	-0.114	-0.137	**0.013**	**-0.002**
Using password/pin/biometric to unlock my device	**-0.081**	**0.077**	**0.098**	0.069	**0.147**
Using two-factor authentication where provided	**0.000**	**0.127**	**-0.014**	0.041	**-0.045**
Regularly scanning my device for threats	**0.075**	**-0.054**	**-0.098**	**-0.018**	**-0.069**
Paying attention to phishing website and unsecure connection warnings	**-0.119**	**-0.147**	**-0.195**	0.062	**-0.101**
Other	**-0.026**	**-0.085**	**-0.002**	**-0.140**	**-0.203**

Figure 4.32: Correlation coefficients between adoption of mental models and security behaviors on tablets. Note: Statistically significant correlation coefficients are in bold ($p<=0.05$).

coefficients were statistically significant. As such, future work could further explore this research question to determine if there is a correlation between mental models and factors of behavior in influencing security behaviors.

Section 4.3.5 Key Takeaways: Partially support H_A 2.2 and found there was a statistically significant, weak correlation between many device-specific mental models and device-specific adoption of security behaviors.

4.4 Discussion

One of the most surprising results was the similarities in the mental models of security, influential factors of adoption, and adopted security tools and behaviors on each of the device platforms. However, it was noted that there was more variability in the implemented security tools on each platform than with the adopted security behaviors. Additionally, while the prevalence of each mental model and supporting perception was similar across all three device platforms, there were a few perceptions with noticeable differences.

4.4.1 Mental Models of Security

The first of these mental models was the "limited risk due to usage". While there were some similarities in the supporting perceptions for this mental model, there were also two supporting perceptions with distinct differences- specifically "Limited risk due to limited data on device" was more prevalent on tablets and "high risk due to high usage" was less prevalent on tablets.

For both of these perceptions, users' belief in these perceptions was relatively similar for traditional computing devices and smartphones while being quite different for tablets. This shows that while participants generally have the "limited risk due to usage" mental model on all three platforms, there is a greater perception of high risk on smartphones and traditional computing devices due to a greater usage of these devices than on tablets.

The next mental model with significant differences in supporting perceptions was "security tools are used to mitigate risk". With this mental model, participants showed more support for the perception that security tools are necessary and help on smartphones and traditional computing devices than on tablets. Conversely, they also showed more support for the perception that built-in security tools are sufficient on tablets and smartphones than on traditional computing devices.

This shows that while participants generally hold the mental model that security tools are needed to protect their device, they view security tools such as application-based security tools as more relevant to the security of traditional computing devices, and to a lesser extent smartphones, than on tablets. Instead, participants generally viewed built-in security tools on tablets as being enough to ensure device security, and to a lesser extent on smartphones. This likely indicates smartphone users view a combination of application-based security tools and device-based security tools as being necessary to secure their device.

The last mental model model with noticeable differences in the supporting per-

ceptions on each platform was "web browsing and downloading is risky". With this mental model, participants generally indicated that they perceived web browsing to be more risk on traditional computing devices as well as web-based security tools as being more useful to protect devices from those risks on traditional computing devices. While there were differences in the prevalence of the supporting perceptions for this mental model, the adoption of the supporting perceptions were very similar on both smartphones and tablets. This likely indicates that users generally view web-browsing as more of a relevant risk on traditional computing devices than smartphones and tablets. Additionally, this difference in perception may correlate to the stronger support for the "apps are secure" perception for smartphones and tablets under the "applications are secure" mental model.

This shows not only a difference in perceptions of security and risk across the different device platforms but also how the mental models of security and the differing prevalence of the underlying perceptions may be influencing implementation of security mechanisms on different device platforms. These similarities and differences show that while the overall mental model may exist on all three platforms, the prevalence of the supporting perceptions does differ. As a result, these differences likely influence user adoption of security behaviors and tools alongside factors of adoption.

4.4.2 Factor of Adoption and Security Mechanisms

As previously mentioned, the most influential factors of adoption on all three device platforms were self-efficacy, ease of use, cost of action, and benefit of action. However, while ease of use was a greater consideration in determining security tool usage, benefit of action was the most influential factor in determining security behavior adoption.

This indicates that while users place a greater importance on actually being able to figure out how to use a security tool with minimal effort, they place more importance on a security behavior actually being beneficial before adopting it. This may be related or adapted from the privacy paradox, with users being more concerned about the

functionality of a security behavior than the actual security risks.

While the most influential factor differed between security tool and behavior adoption rather than device platform, less so did the actual adoption of security tools and behaviors on each platform. In general, security behavior adoption did not greatly differ between the device platforms with the majority of the security behaviors being largely adopted on each platform, as shown in Figure 4.34. However, security tool usage did differ by platform, with security tool adoption on smartphones and tablets being more similar and less than security tool adoption on traditional computing devices, as shown in Figure 4.33.

Device	Antivirus	Ad-blocker	VPN	Password Manager	Other
Laptop/Desktop	120	116	51	105	10
Smartphone	42	61	36	121	22
Tablet	47	72	28	93	26

Figure 4.33: Number of participants using each security tool divided by device platform

The similarities in security behavior combined with the differences in security tool adoption indicate that mental models of security are likely influencing the adoption of security tools more than the adoption of security behaviors. Instead, the similarity in security behaviors across all device platforms as well as the importance of the factor "benefit of action" in determining device-specific security behaviors, indicates that security behaviors are likely carried over from device to device, perhaps due to the formation of security habits on traditional computing devices or security training.

Device	Not purchasing items on unsecured networks	Not downloading files/apps from untrusted third-party sites	Generating secure passwords for my accounts	Using password/pin /biometric to unlock my device	Using two-factor authentication where provided	Regularly scanning my device for threats	Paying attention to phishing website and unsecure connection warnings	Other
Laptop/Desktop	122	147	108	134	137	78	139	2
Smartphone	126	146	114	144	138	43	129	3
Tablet	131	151	106	136	126	37	132	4

Figure 4.34: Number of participants using each security tool divided by device platform

4.5 Summary

This study was conducted using a survey research design to allow for the collection of responses from a larger population of people regarding the mental models of security, how they protect their devices, and why they use different security mechanisms. The collection of a larger number of responses allowed for the identification of patterns in the prevalence of each mental model and many of their supporting perceptions identified in Study 1. Overall, all of the mental models of security and their supporting perceptions identified in Study 1 were also found to exist in our survey population. This confirms the existence of these mental models, even in a larger population.

We were also able to identify patterns in the prevalence of these perceptions between device platforms. As an example, the perceptions "high risk due to high usage" was more prevalent on smartphones, followed by laptops, and then tablets. These observed patterns identified some of the device-specific adaptations of the mental models and supporting perceptions identified in Study 1. These observations also identified which perceptions, and in a broader sense, mental models were more influential than others on each device. As an example, the perceptions within the "Web browsing and downloading is risky" mental model were generally more prevalent on laptops than the other devices. As a result, it is possible to conclude that this mental model is generally influential to the decision making of laptop users. These prevalence patterns are summarized in Figure 4.35.

In addition to observed patterns made with descriptive statistics, we also observed statistically significant differences between the prevalence of perceptions across the device platforms. All of the mental models except for the "Platform is Secure" mental model had at least one perception with statistically significant variability. Additionally, for most of these perceptions, we were able to identify at least one device which would result in statistically significant differences in prevalence, regardless of the platform it is compared with. These results are summarized in Figure 4.36 below.

Mental Model	Perceptions	Platform Prevalence	Overall
Limited Risk Due to Usage	Limited risk due to limited data on device	Tablet	Tablet
	High risk due to high usage	Smartphone	
	Limited access to important data and app usage on this device	Tablet	
	Stopping device stops risk	Tablet	
Security Tools are Used to Mitigate Risk	Security tools help protect device	Laptop	Tablet and Laptop
	Security tools are neeed to protect device	Laptop	
	Built in security tools are sufficient	Tablet	
	Security is not a priority due to cost	Tablet	
	Security is not a priority over functionality	Tablet	
Platform is Secure	Device is secure	Smartphone	Tablet
	Security risks result from user error	Tablet	
	Company is trustworthy and thus secure	Tablet	
Web Browsing and Downloading is Risky	Web browsing and downloading is risky	Laptop	Laptop
	Web based security tools protect from internet based risks	Laptop	
	Good web browsing practices help mitigate risk	Laptop	
Applications are Secure	Apps are secure	Tablet	Tablet and Laptop
	Third party apps are risky	Laptop	

Figure 4.35: Summary of mental model and supporting perception prevalence.

Furthermore, we found that while there was some variability in the security tools adopted based on platform, with more tools being adopted on laptops than smartphones or tablets. The reported breakdown of security tool adoption is summarized in Figure 4.37. As seen in Figure 4.37, the number of participants adopting each security tool was relatively similar on smartphones and tablets. The main security tool exception to these patterns were password managers, with this tool being similarly adopted on all three platforms.

Unlike with security tools, there was less observed variability in security behavior

Mental Model	Percpetions with significant variability	Statistically significant device relationships	Platform causing variability in prevalence
Limited Risk Due to Usage	Limited risk due to limited data on device	Smartphone/Tablet	Tablet
		Tablet/Laptop	
	High risk due to high usage	Smartphone/Tablet	Tablet
		Tablet/Laptop	
Security Tools are Used to Mitigate Risk	Security tools help protect device	Laptop/Smartphone	All device platforms
		Smartphone/Tablet	
		Tablet/Laptop	
	Security tools are needed to protect device	Laptop/Smartphone	All device platforms
		Smartphone/Tablet	
		Tablet/Laptop	
	Built in security tools are sufficient	Smartphone/Tablet	Tablet
		Tablet/Laptop	
Platform is Secure	No perceptions had statistically significant variability between platforms		
Web Browsing and Downloading is Risky	Web browsing and downloading is risky	Laptop/Smartphone	Laptop
		Tablet/Laptop	
Applications are Secure	Apps are secure	Laptop/Smartphone	Laptop
		Tablet/Laptop	
	Third party apps are risky	Tablet/Laptop	—

Figure 4.36: Summary of perceptions with statistically significant variability between device platforms.

Device	Antivirus	Ad-blocker	VPN	Password Manager	Other
Laptop/Desktop	120	116	51	105	10
Smartphone	42	61	36	121	22
Tablet	47	72	28	93	26

Figure 4.37: Security tool adoption by device platform.

adoption between the device platforms. The main behavior with an observable degree of variability is "regularly scanning my device for threats". This behavior was adopted

by approximately double the number of participants on laptops than on smartphones and tablets. However, the rest of the security behaviors were relatively widely adopted across all three platforms. This is summarized in Figure 4.38 below.

Device	Not purchasing items on unsecured networks	Not downloading files/apps from untrusted third-party sites	Generating secure passwords for my accounts	Using password/pin /biometric to unlock my device	Using two-factor authentication where provided	Regularly scanning my device for threats	Paying attention to phishing website and unsecure connection warnings	Other
Laptop/Desktop	122	147	108	134	137	78	139	2
Smartphone	126	146	114	144	138	43	129	3
Tablet	131	151	106	136	126	37	132	4

Figure 4.38: Security behavior adoption by platform.

While we observed device-specific differences in both mental models and security tool/behavior adoption, we were only able to generally establish a statistically significant, weak correlation between these two variables, likely in part due to the sample size and the binary range of the two variables. As a result, additional research would need to be conducted to establish a correlation between device-specific mental models and device-specific security mechanisms outside of descriptive statistical connections. One example of this is between the "Web browsing and downloading is risky" mental model and the adoption of ad-blockers. We found that this mental model was more prevalent on laptops and, potentially as a result, more participants utilized ad-blockers on laptops than on smartphones and tablets. This is further supported by evidence that laptops were a significantly significant factor in differences between prevalence of the "web browsing and downloading is risky" perception. The contributions discussed in this chapter are summarized in Figure 4.39.

Relevant Study Research Questions	Contributions/Findings
RQ2.1: What are the similarities and differences in mental models of security by device platform?	• Identification of 5 mental models of security with supporting perceptions • Identification of variances in prevalance of these mental models and perceptions of security on different device platforms • Identification of similarities in prevalance of these mental models and perceptions of security on different device platforms • Partially accept the alternative hypothesis HA 2.1: There are statistically significant variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.
RQ2.2: What are the similarities and differences in the factors influencing security behavior on different device platforms?	• Identification of device-specific similarities and differences in security tool adoption • Identification of device-specific similarities in security behavior adoption • Identification of the four most common factors influencing security tool adoption across all three device platforms • Identification of the five most common factors influencing security behavior adoption across all three device platforms
• RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms?	• Partially support the alternative hypothesis HA 2.2: There is a statistically significant correlation between the device-specific mental models and the adoption of security behaviors on each device platform.

Figure 4.39: Summary of findings and contributions from Study 2.

CHAPTER 5: STUDY 3: AWARENESS NUDGING IN ANTI-VIRUS SOFTWARE

5.1 Introduction

One of the prevalent perceptions noted in Study 1 was a lack of awareness of risks to devices and effective measures to mitigate these risks, particularly in the case of smartphones and tablets. However, there was also a perception of the effectiveness of security tools in mitigating risk. These perceptions were more developed regarding laptops as users had both an awareness of at least a few potential risks as well as knowledge of security mechanisms such as antivirus software, even if they did not utilize the software.

Comparatively, users of smartphones not only had less awareness of risk, but they often did not utilize software-based security tools and instead relied upon factory-installed mechanisms, such as biometrics, to protect their devices and data. Due to this discrepancy in awareness and security behavior between device platforms as well as the observation that many of the perceptions present in smartphones and tablets seemed to have been formed from users' experiences and perceptions of laptops, this study sought to examine whether the usage of nudging notifications in a laptop-based security tool would encourage awareness of risk and security mechanisms as well as encourage behavior change through the utilization of the security tool on another platform.

This study sought to answer the following research questions:

- RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform?
- RQ3.2: What are the user suggested design guidelines for such a notification to

encourage attention and adoption?

Users generally perceive that their traditional computers (e.g. desktops and laptops) are more likely to be vulnerable to security risks than their smartphones, and generally trust their smartphone applications [36, 32, 46] to be secure and safe. Additionally, users are more likely to use protection mechanisms on their computers than on their smartphones [36, 32, 7, 46]. Thus, while users do care about their smartphone security, they sometimes lack awareness of the appropriate mechanisms and behaviors to secure their devices [33, 32]. As a result, educating users about suggested security actions, such as through the use of notifications, can be effective in increasing awareness and secure behaviors [47, 14, 24].

A major question then is how and when to deliver such guidance, to raise awareness of security tools and encourage their use. In this study, we are investigating whether we can use notifications on one platform where users are already using a security tool, namely a traditional computer, to raise awareness of and motivate adoption of similar tools on another platform, namely a smartphone. This study addresses dissertation RQ3: How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform, and RQ4: How can you increase awareness of risk and effective security mechanisms on different platforms based on the perceptions on an existing platform of this dissertation.

Notices have been used in a variety of situations, most relevantly in security risk awareness as well as security tool notifications, such as reminders to run system scans in antivirus software or alerting of potential phishing websites. Key criteria in providing security advice are that the advice is effective, easy to execute, consistent across notifications, and concise [40, 3, 29]. Additionally, notifications should have easy to understand language and avoid technical jargon [46]. Nudges have also been used to influence behavior when faced with a choice, such as making default choices the more secure option [40, 3]. With these guidelines in mind, we are designing and

evaluating a notification for anti-virus software on a computer, which recommends the use of that same software on a smartphone. As such, incorporating the design guidelines and best practice considerations for both security advice and nudging in the design of this notification will hopefully result in a hybrid option that not only increases users' awareness of potential security mechanisms on other device platforms but also influences their behavior by encouraging them to utilize more formalized security tools on their non-traditional computing device platforms.

5.2 Methodology

This study operated in two phases, with the first being a notification design phase. The second phase consisted of a user study to evaluate the notification designs and their perceived effectiveness. We chose anti-virus software as the tool due to wide-spread understanding of its function and purpose as well as its universal applicability to both traditional computing devices and smartphones. As such, it is a realistic expectation that if the nudge notification encourages user to utilize the anti-virus software on another platform, they could, or would, actually do so, lending authenticity to the study environment.

For both phases of the user study, a prototype of antivirus software for laptops was created. For Phase 1 of the user study, four screens were created using Google Slides. This allowed for the quick iteration of multiple notification designs by using screenshots from an existing real-world laptop antivirus software, Bitdefender, to be edited with elements added or modified to illustrate the appearance of each potential notification design. For Phase 2 of the user study, seven prototype screens were created using Figma and then added to Google Slides for easy sharing of the wireframe with participants while still simulating the functionality of the buttons and links to advance through the screens. This prototype was informed by two-real world laptop antivirus software, Bitdefender and McAfee, as well as the previously mentioned design guidelines for notifications and security advice and the participant feedback from

Phase 1 of the user study.

5.2.1 Phase 1: Notification Design

The first phase was a design phase to determine the most effective design and placement for a notification in a laptop-based anti-virus software. During the first phase, we ran iterations of notification phrasing, design, and placement with a focus group of 12 students to determine the most effective combination for catching users' attention and prompting them to read the notification. During this step, various types of notifications, such as active alerts, and banners, were designed for an antivirus software in a laptop/desktop environment. The designs shown in the first part of the study are shown below in Figure 5.1.

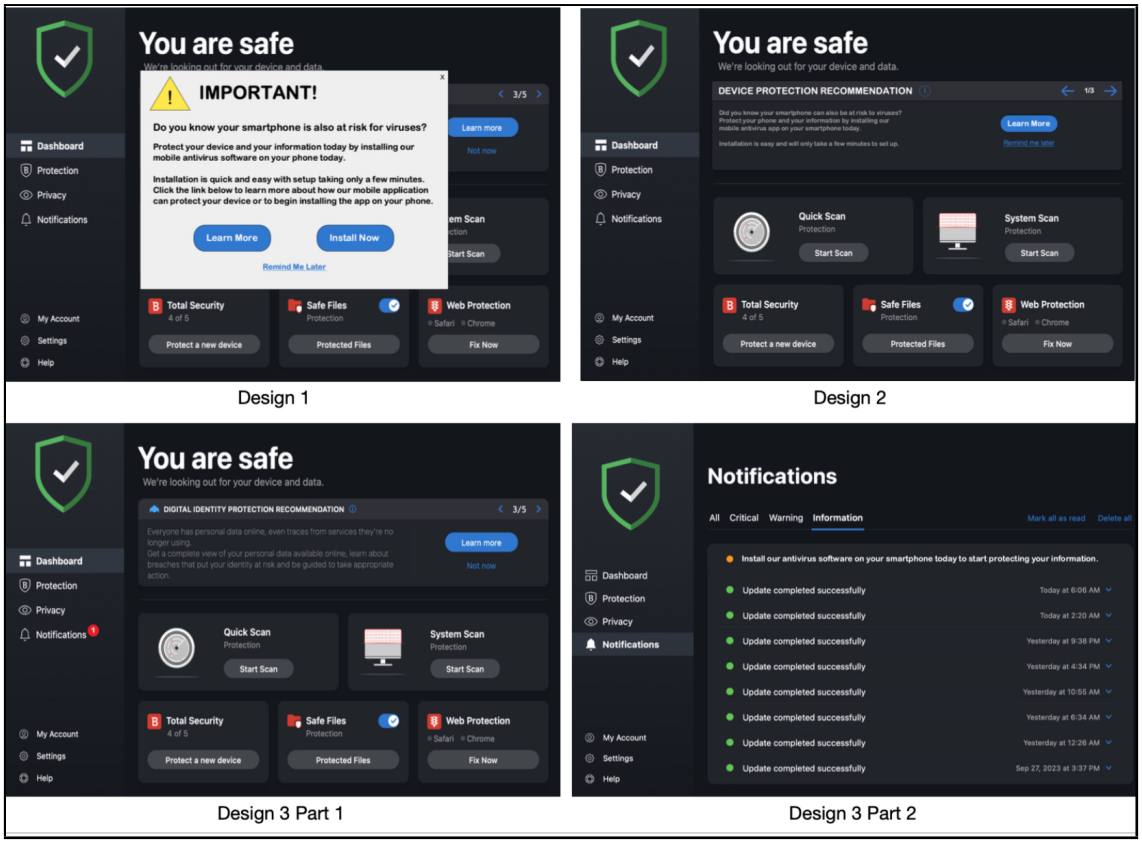

Figure 5.1: The three notification designs shown to participants in Phase 1 of the study.

These designs were informed by current research suggestions on effective elements

of notification design and security warnings [40, 3, 29, 46, 40, 3]. Additionally, two of the mental models identified in Study 1, "Security tools are used to mitigate risk" and "Platform is secure" were used to inform the message included in the notifications. These mental models were selected due to their relevance to antivirus tool adoption and platform specific vulnerabilities to risk. Specifically, participants in Study 2 indicated that the perceptions "company is trustworthy and thus secure", "device is secure", and "built in security tools are sufficient" were more prevalent on smartphones than laptops. Conversely, participants in Study 2 indicated that the perception "security tools are needed to protect device" was more prevalent on laptops than smartphones. The prevalence of these perceptions on each device platform informed the content of the notifications to addressing some of these misconceptions. Specifically, the notifications were trying to raise awareness of the potential for security vulnerabilities to viruses on smartphones to address the misconceptions with the first three perceptions and the effectiveness of mobile antivirus software at helping to protect devices to address the misconceptions with the lack of usefulness of security tools on smartphones.

Each design was shown to all 12 students to evaluate the effectiveness of the design at gaining their attention and prompting their intention to investigate the use of antivirus software on a smartphone. Participants were also asked their opinion on what they liked or disliked in each design to attempt to create an overall design that was unobtrusive, non-annoying, and effective while maintaining the usability of the laptop-based antivirus software and avoid aggravating the user and discouraging their adoption of antivirus software on their smartphone. The full list of questions for phase 1 of the user study are shown in Figure 5.2

At the conclusion of the design phase, the intention was for a single nudge notification design to be chosen to utilize during the second phase of the user study.

Question Topic	Question
Background	Do you currently use any antivirus software on your laptop/desktop? If so, which one? If not, why not?
	Do you currently use any antivirus software on your smartphone? If so, which one? If not, why not?
Notification Design	What do you like about the notification? Design, location, explanation, etc.
	What would you like to change about the notification?
	What else would you like to see in the notification or for the notification to do?
	What would you like to happen when you interact with the notification?
	Where would you like to see the notification?
	What about the notification would encourage you to install the mobile antivirus software on your smartphone?
	What about the notification might discourage you from installing the application on your smartphone?
	What would make it easier to install the antivirus on your smartphone?
Overall Feedback	Which notification design did you prefer? Why?
	Anything else you would like to add?

Figure 5.2: List of interview questions for phase 1 of the user study.

5.2.1.1 Results

Participants of the notification design focus group were relatively split between two notification designs with one participant suggesting both of these designs be used. Overall, 4 participants indicated they preferred Design 1 of Figure 5.1, 3 participants indicated they preferred design 2, 5 participants indicated they preferred design 3, and 1 participant indicated they preferred both design 1 and 3. Due to the closeness in preference for both design 1 and 3, we decided that both notifications should be used in the user study after being revised based on user feedback.

Some of the key revisions made were to alter the stylized design of the active notification and change the associated icon to decrease the similarity to scam or virus alerts. Additionally, the color scheme of the notification was changed to make it more cohesive with the antivirus software design. The passive notification underwent minor changes, with the most significant being the inclusion of a red notification icon indicating the existence of a new notification to draw awareness to the new icon.

After implementation of this feedback, two prototypes were created, shown in

Figure 5.3 and Figure 5.4. These prototypes allowed participants to click on some of the buttons and view some of the key screens in the antivirus software, such as the notification panel and dashboard. In general, a night-mode theme was chosen for the prototype and the nudges were designed following this theme as well.

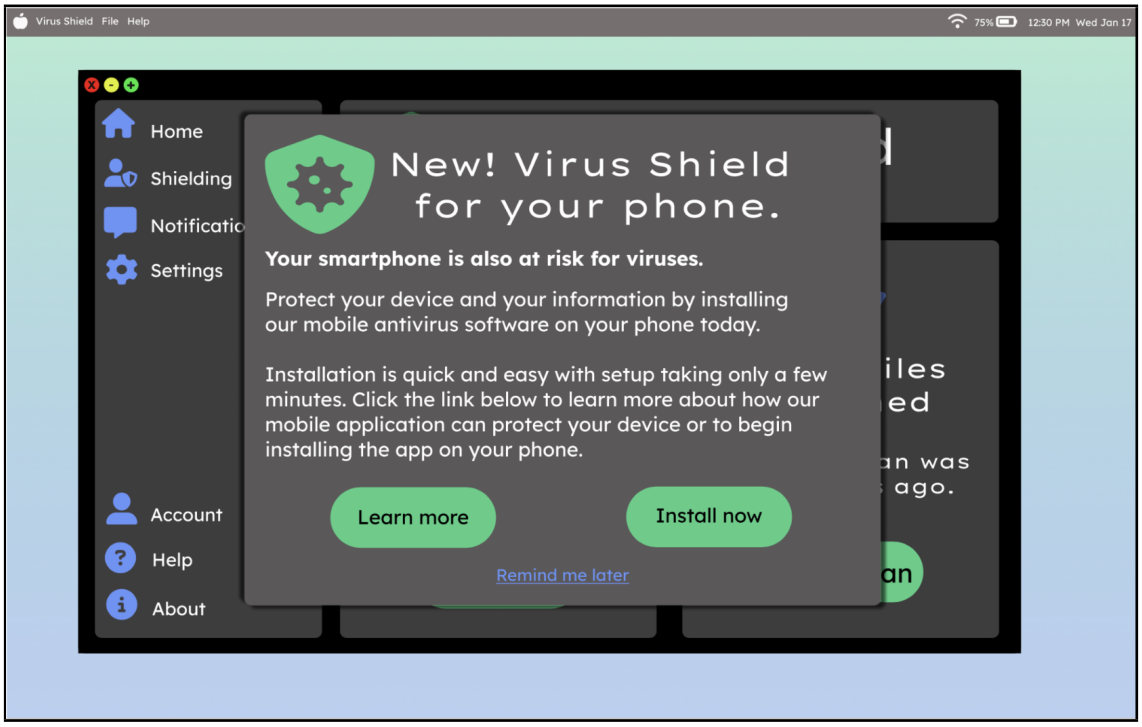

Figure 5.3: The active notification designed based on feedback from Phase 1 of the study.

5.2.2 Phase 2: User Study

The second phase of the study was a user study conducted with 36 participants to determine the effectiveness of the notification designs on encouraging the utilization of the anti-virus software on a smartphone using the notifications created based on feedback and results from the previous phase. Before beginning the user study, participants completed a demographics survey which included questions about their current usage and perceptions of antivirus software on their laptop/desktop and smartphone, including which devices they currently use antivirus software on-if any.

We utilized an A/B methodology, where half of the participants saw a control

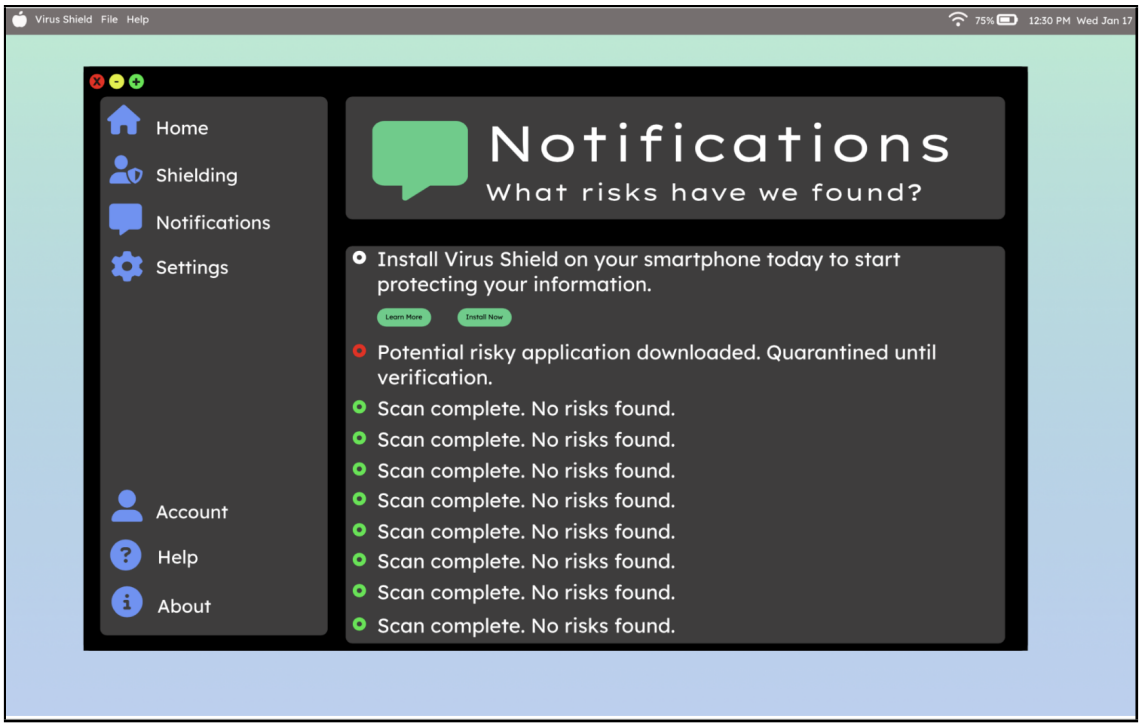

Figure 5.4: The passive notification designed based on feedback from Phase 1 of the study.

group prototype with no notifications or nudges, while half saw an active and passive notification, within the prototype. The two prototype flows are show below. Figure 5.5 shows the control group prototype shown to group A with no notifications. Figure 5.6 shows the prototype shown to group B with the active notification in the first image and the passive nudge in the image. As a note, Figure 5.6 is missing the shielding page as well as the additional dashboard page that helped simulate functionality in the prototype for ease of viewing. However, these pages are shown in the first and second images in Figure 5.5 for reference. When viewing the complete prototype, participants were able to simulate viewing the notifications, clicking the installation button on the notifications, and viewing the dashboard, shielding, and notifications page. Each participant was assigned to either group A or group B upon signing up for the study to ensure an equal distribution of participants in each group, resulting in 18 participants in each group.

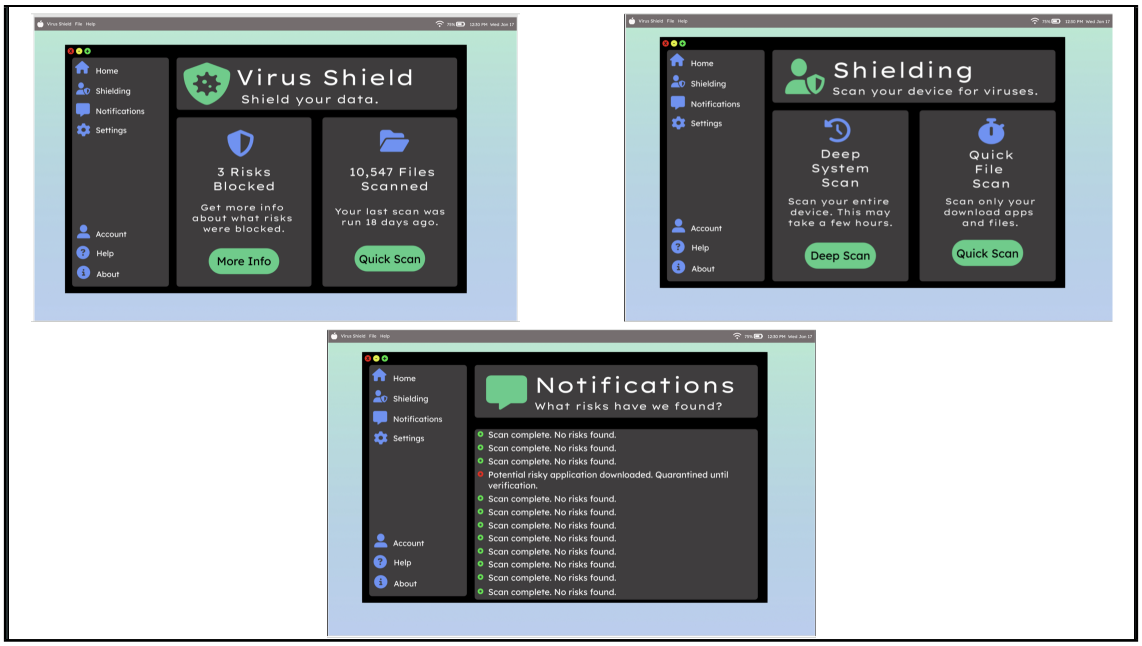

Figure 5.5: Prototype A: Control group prototype without any notifications

Figure 5.6: Prototype B: Prototype with the active and passive notifications

Participants were shown the relevant prototype of an antivirus software in a laptop/desktop environment for their group and asked to explore the prototype to familiarize themselves with the application. Once the exploration was completed, participants were interviewed to determine if they were interested in installing antivirus

software on their smartphone. After determining installation intent based on the original prototype, participants in Group A were also shown the prototype with the two notifications to provide feedback on the design and effectiveness during the interview. During this interview, all participants were asked their impressions of both notification designs, likes and dislikes, and suggestions for improving the notifications. We also asked for their perceptions as to whether and how such a notification could prompt them to install antivirus software on their smartphone. The full list of interview questions for phase 2 are shown below in Figure 5.7.

Question Topic	Question
Expressed Installation Intent	After seeing this prototyp are you interested in or considering looking into installing antivirus software on your smartphone?
Notification Design	What do you like about the notification? Design, location, explanation, etc.
	What would you like to change about the notification?
	What else would you like to see in the notification or for the notification to do?
	What would you like to happen when you interact with the notification?
	Where would you like to see the notification?
	What about the notification would encourage you to install the mobile antivirus software on your smartphone?
	What about the notification might discourage you from installing the application on your smartphone?
	What would make it easier to install the antivirus on your smartphone?
Installation Motivations	Is there anything else this antivirus software could do to encourage you to install the mobile version of the software on your smartphone? Why, why not?
	What else might encourage/prompt you to install antivirus software on your smartphone? Why, why not?
	What might discourage you from installing antivirus software on your smartphone?
	Anything else you would like to add?

Figure 5.7: List of interview questions for phase 2 of the user study.

5.2.2.1 Participants

As previously mentioned, this phase of the study was conducted with 36 participants recruited through a university listserv and snowball sampling. Figure 5.8 below shows the demographic data for each of the participants.

Participant ID	Race	Gender	Total Yearly Household Income	Use Laptop Antivirus	Use Smartphone Antivirus
1	White	Male	$100,000 - 149,999	Yes	No
2	Asian	Male	Prefer not to say	Yes	No
3	Asian	Male	$25,000 - $49,999	Yes	No
4	White	Female	Prefer not to say	Yes	No
5	Asian	Male	$25,000 - $49,999	Yes	No
6	White	Male	$25,000 - $49,999	Yes	No
7	White	Female	$25,000 - $49,999	Yes	No
8	White	Male	$50,000 - $74,999	No	No
9	White, Asian	Male	$25,000 - $49,999	Yes	No
10	White	Female	Less than $25,000	Yes	No
11	White	Female	$100,000 - 149,999	No	No
12	Black or African American	Female	Less than $25,000	No	No
13	Asian	Male	Less than $25,000	Yes	No
14	Black or African American	Prefer not to answer	Prefer not to say	Yes	Yes
15	Asian	Female	$150,000 or more	No	Yes
16	White	Female	$50,000 - $74,999	Yes	No
17	Asian	Female	Prefer not to say	Yes	Yes
18	Asian	Female	$100,000 - 149,999	Yes	No
19	White	Male	Prefer not to say	No	No
20	White	Female	$100,000 - 149,999	No	No
21	American Indian or Alaska Native	Female	Less than $25,000	No	No
22	Latino	Male	$50,000 - $74,999	No	No
23	Black or African American	Female	$50,000 - $74,999	No	No
24	Asian	Female	Prefer not to say	Yes	No
25	Black or African American	Female	$100,000 - 149,999	Yes	No
26	Middle Eastern	Female	Prefer not to say	No	No
27	Black or African American	Female	Less than $25,000	Yes	No
28	Black or African American	Male	Less than $25,000	Yes	No
29	Black or African American	Female	Less than $25,000	No	No
30	White	Female	Less than $25,000	No	No
31	White, Asian	Female	Prefer not to say	No	No
32	Asian	Male	Less than $25,000	No	No
33	White, Asian	Gender Variant/Non-conforming	$50,000 - $74,999	Yes	Yes
34	Asian	Male	Prefer not to say	Yes	Yes
35	White	Male	$100,000 - 149,999	Yes	No
36		Prefer not to answer	Prefer not to say	Yes	No

Figure 5.8: Participant demographics for study 3.

5.2.2.2 Analysis

Transcripts of the interviews from the second phase of the study were qualitatively analyzed using grounded-theory methodology to identify key themes regarding notification design preferences and motivators for installing antivirus software on a smartphone. During this analysis, codes were grouped into two groups representative of group A and B for comparison purposes. An iterative coding process was then conducted where the first five transcripts were initially coded to compile a relatively complete list of codes and three primary themes were identified. Then, all of the transcripts were coded and additional codes were added as discovered. Lastly, all transcripts were then reviewed one more time to ensure all relevant quotes were assigned appropriate codes.

The first of these themes was the effectiveness of the notifications on encouraging installation of the smartphone-based antivirus software. In other words, codes under this theme were tracking participants' stated intention to install, or not install, the antivirus software. This theme tracked both intention to install after viewing the initial prototype for each group of participants and thus user stated effectiveness of the notification and nudge compared to the control group. This was primarily compiled from responses to the initial interview question asking participants their intent to install the mobile version of the software after viewing the prototype before group A was shown the prototype with the notifications. However, this theme also tracked participants' statements of installation intent throughout the interview, both in the positive and negative, particularly if participants mentioned a motivator which would cause them to install the antivirus software on their smartphone.

The next theme was the participants' motivations to install, or not install, the antivirus software on their phone. In other words, this theme consisted of codes describing the mental models, perceptions, and factors which would encourage or discourage a user from installing antivirus software on their phone. These codes were often associated with questions asking participants what would encourage/discourage them from installing the mobile antivirus software, why/why not they would install the mobile antivirus software, and what about the nudge or notification for encourage/discourage them from installing the mobile antivirus software. As a result, this category of themes is compiled from codes describing user-indicated positive and negative considerations and motivators for installing the mobile antivirus software that can be used to inform both how and what information is communicated to users.

The last category of themes consisted of design guidelines proposed by the participants that should be considered when designing a notification to prompt implementation of a security behavior rather than merely raise awareness of the security behavior or mechanism. This theme consists of codes describing attributes, information, and

actions that the participants liked and disliked about the notification and nudge. Additionally, some of these codes describe design guidelines participants stated as important for influencing their decision to install the mobile version of the antivirus software.

5.3 Results

In this section, we describe the results of the second-phase user study. These results consist of the responses to the pre-study survey and the interview during the user study. For the most part, results are described in aggregate due to the commonalities in motivations and design guidelines identified. However, each motivation and design guideline includes the number of participants in each group (A and B) who mentioned it as important or a consideration when determining intent to install the mobile version of the antivirus software.

5.3.1 Pre-study survey

In the pre-study survey, we found that 22 participants were already using antivirus software on their laptops/desktops, while only 5 participants were using antivirus software on their phones. Nevertheless, most of the participants viewed antivirus software as beneficial to their device, with 28 participants agreeing with this statement on their smartphone and 29 participants agreeing on their laptop/desktop. However, we also found that more participants would recommend antivirus software to others on the laptop/desktop (30 participants) than the smartphone (21 participants).

As shown in Figure 5.9 and Figure 5.10, the three most common reasons for installing, or considering installing, antivirus software on the laptop/desktop and smartphone were that the software was useful, the software was pre-installed on the device, or that the participant was required to install the software.

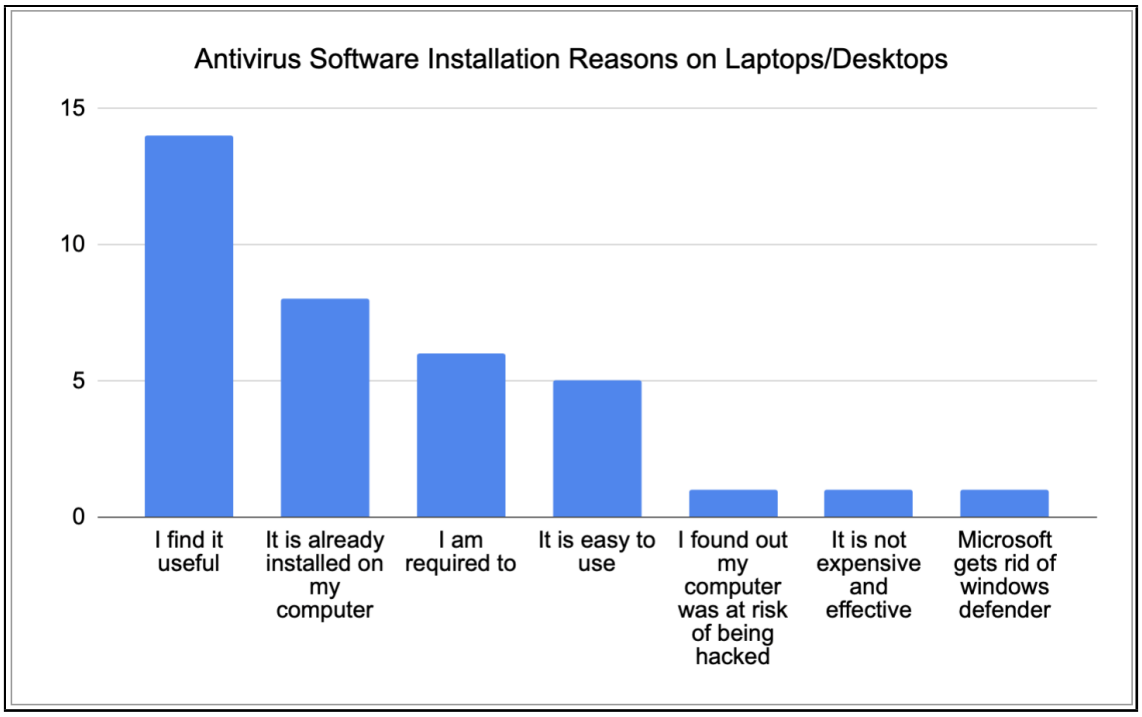

Figure 5.9: Reasons for installing antivirus software on the laptop.

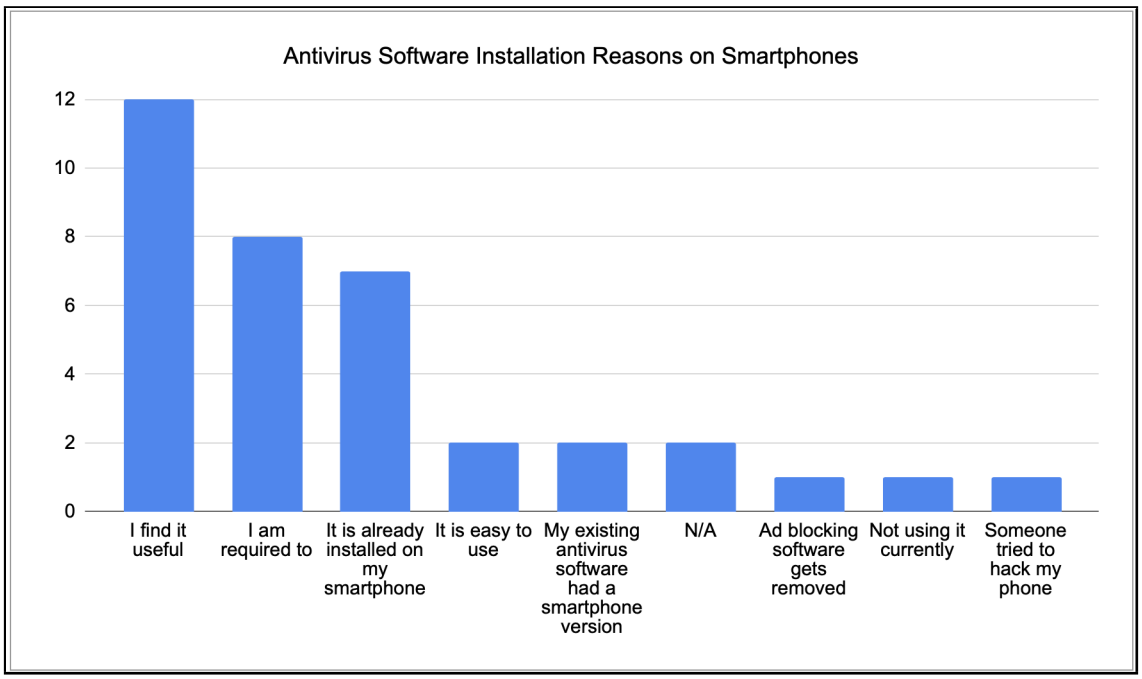

Figure 5.10: Reasons for installing antivirus software on the smartphone.

5.3.2 Installation Motivations

During the user study, we identified multiple motivations for installing antivirus software on a smartphone. One of these motivators is the **functionality** (A=15,

B=15) of the software, where participants were considering if the antivirus software would actually protect their device and their information. As participant 31 explains, "I feel like if I actually saw that it was doing something on my smartphone, I would feel like, okay, this is worthwhile having. I made a good call installing it and also keeping with it, because look at all the things that it's scanning for and protecting me from." With this motivator, participants placed importance on the mobile antivirus software working as expected and as advertised.

With this motivator, participants viewed the contributing value of the antivirus software to the device security when considering if they should installing the software. This motivator was also mentioned at times with a preference for **phone-specific operations** (A=11, B=4) to secure the device. As participant 13 explains, "Maybe have some other built-in options other than a virus scan. I know some of them have a wifi scan or they have some VPN options. I don't know, some type of other little built-in features other than just the virus scan." In other words, some participants wanted the mobile antivirus software to not only protect their device from viruses but also provide additional functionality, such as detecting phishing text messages, to justify the cost of the software.

Speaking of cost, another consideration for participants was the **cost** (A=5, B=5) of the mobile antivirus software, both monetary and physically. Aside from the potential cost of the software being too high to justify purchase, as discussed in the next motivation, many participants also expressed concern about the physical load of the software on their phone's performance, citing considerations such as decreased battery life and significant memory requirements. As participant 17 explains, "I don't need an antivirus software that is going to be my best friend and my banking assistant. A lot of apps start off that way. They start doing their job, and then they add stuff to make it better, and it just gets clunkier. If I'm downloading an antivirus, I just want it to do that job well."

Participants also stated that **promotions** (A=8, B=14) offered by the company would potentially motivate them to install the mobile version, even if just to test it. Participant 1 states, "I would say if someone already has the desktop version on there already, well, then I would say tell them, "Hey, you can also get it on your phone for free with your account as a promotion. Have you seen those ads that instead of saying that we're on sale they go, "You've earned 20% off." Some of these participant suggested promotions included the overall cost of the software and if it was included in the existing cost of their laptop/desktop coverage plan or the offering of a free trial to test the effectiveness of the software before purchasing.

Participants also considered how **easy it was to install** (A=17, B=13) and use the the antivirus software on their smartphone. Participant 2 explains, "I think that having clear instructions and as concise as they can be instructions helps the user be more motivated to download the app because they know it's not going to be a super long process." In other words, participants viewed a complicated installation process with long steps or unclear instructions as being a deterrent from installing the software on their phone. Conversely, they indicated that if there was a low effort to install the antivirus software on their smartphone and begin using it, they would be more likely to install the software when prompted by the nudge.

Another motivator was **awareness** (A=13, B=17) of the mobile version of antivirus software, with the lack of awareness of the availability of mobile antivirus software a stated reason for not installing. As Participant 1 states, "I didn't even know anti-viruses exist for smartphones before this study, so yeah. I mean the study itself. Yeah, if there is one I would get it." Many participants were generally unaware of the availability of smartphone antivirus software and the protection they provide their devices. As a result, they stated becoming aware of the availability of this software would motivate them to consider installing mobile antivirus software.

In addition to awareness of the availability of mobile antivirus software, participants

also stated awareness of the need for antivirus software on their phone as a motivator for installing the software. As participant 35 explains, "I guess if I knew that there was some sort of significant risk, and I'm sure if I were to educate myself more on it or be educated on it, I would understand that. If I were to see there was a reason to, then I would. But just with my current knowledge and a feeling like I know my way around the internet to know what would be a virus and what wouldn't, I wouldn't really feel a need for myself personally." In other words, many participants stated that understanding the risk their smartphones face and why antivirus is effective in protecting their device was an important motivator, particular in overcoming misconceptions that smartphones are inherently secure. Overall, the notifications raised awareness of the potential for both security risks from viruses on smartphones and the option for mobile antivirus software as a security mechanism to secure users' mobile devices.

Participants also considered their perceptions of **risk** (A=12, B=13) to viruses on smartphones when deciding if it was even necessary to install antivirus software on their phones to protect against viruses. As participant 19 explains, "Essentially, unless you have jailbroken the iPhone or you are in a country that will allow sideloading in the future, there's really not much vulnerability because all the software that runs on it is already been verified by Apple. There is no way to install a virus per se, unless of course there's a zero day. But a zero day is not necessarily going to be found by antivirus software any faster than Apple would find it themselves." Similar to the previous motivation, there is a lack of awareness of the need for antivirus software on smartphones and the potential security risks users face when using mobile devices. As a result, stating the risks users face on mobile devices was a motivator for installing antivirus software.

In addition to their perceptions of risk to viruses on the smartphone, participants also considered their perception of the **trustworthiness** (A=14, B=13) of the mobile

antivirus software. As Participant 32 explains, "I'm more cautious that there would be a information threat through the app itself maybe. Or the worst-case scenario, it might make my phone act weird or slow it down." In other words, participants viewed the perceived security of the mobile application and the data it accesses and stores as a consideration in installing the mobile version of the software. One common method for evaluating trustworthiness of the mobile software was the usage of reviews. As Participant 4 explains, "But if somewhere when I'm going through it you provide a sort of reference, or source where this product is not just marketed but assessed by someone reputable, maybe a cybersecurity company or whatever, would they confirm that this is a legitimate product. That will maybe entice me to look it up a bit more." In general, participants stated they would rely on reviews from 3rd party agencies and existing users to help determine if the mobile antivirus software could be trusted to effectively protect their device.

Similar to the previous motivation, participants also considered the **effectiveness of the laptop version** (A=11, B=10) of the antivirus software as an influencing factor in determining whether or not to install the mobile version of the antivirus software. As participant 18 explains, "I should be aware about this, that there exists something like this for my smartphone, and if it just randomly pops in, definitely I'll see if the brand name is familiar to me. Otherwise, I would just ignore it thinking it's some kind of a virus itself. Otherwise, yes, if I'm aware about the brand, if I'm using the same one for the laptop, this should be sufficient information for me to persuade me to download or install the software." In other words, participants felt that if they were satisfied with the performance of the antivirus software on their laptop, then they would be more likely to install it on their phone with the expectation that the mobile version would perform just as well as the laptop version of the antivirus software.

However, participants also considered if the notification was a **distraction** (A= 12, B=9) when considering if they would install the software on their smartphone. This

included if the notifications impeded their ability to complete their task or became annoying due to the frequency they were shown to users. Participant 35 explains, "I feel like if it were to just become overly intrusive, overly just annoying to me, it would make me not really have trust in that, I guess. It would just annoy me enough where I wouldn't feel like I would want to download and use their software on my phone." When the notifications become a distraction, participants indicated they would negatively impact their intention to install the software on their phone.

Section 5.3.2 Key Takeaways: Some identified motivations for installing security tools were grounded in previously identified mental models of security.

5.3.3 Design Guidelines

In addition to stating elements or considerations which would motivate them to install the mobile antivirus software, participants also explained some design guidelines they would recommend to increase the effectiveness of the notifications. For example, participant feedback indicated that such notifications should have a **minimalist** (A=8, B=8) design with only necessary buttons and text. Participant 2 illustrates this by stating, "If the steps right here were too complicated, if it was too much to read, I probably wouldn't. I think that these are concise enough, but if I had read through a page of text to figure out how to download it, that would certainly be pretty discouraging for me." In other words, participants were looking for a simple design that was not overwhelming or time consuming to read and interact with.

Additionally, to ensure the notification is **user-friendly** (A=10, B=10), participants wanted a notification that was easy to understand, navigate (including returning to the main interface), and follow any instructions if necessary. Participant 7 explains, "I think that it is pretty friendly. It doesn't use a lot of words that I will not know. I mean, I think that the main idea that the message is trying to communicate is pretty much easy to understand." When considering if the notifications were user-friendly,

participants placed a lot of emphasis on the instructions and text being **easy to understand** (A=12, B=12) and follow as well as the interface being intuitive to navigate. As such, one recommendation was to include images and graphics to help illustrate some of the steps or communicate facts. Participant 15 suggests providing "either verbal instructions or visual instructions would be good for just setting up the account, because once you set it up, it will get you straight to being able to use the antivirus software."

Participants also wanted there to be sufficient **information** (A=16, B=14) included in the notification to communicate the potential security risks users face on smartphones and how the antivirus software helps prevent these risks. As Participant 4 explains, "So here it just says there is a potential risk, but it doesn't sort of list how many risks, or what kind of risks they may be. And that may be helpful, because there's a lot of different security problems potentially. So this is just very generic and maybe a little more info, like identify risk with password, or with other things, or whatever." In general, with this design guideline participants were looking for the inclusion of statistical facts or informative graphics which helped communicate potential risk to viruses on smartphones to the users.

While participants indicate they want clear information on the nudges, many participants also state the nudge should be **skim-able** (A=6, B=6). As Participant 3 explains, "I just see your smartphone is also at risk for viruses and go, "Yeah, that sounds about accurate," and I just skip everything below protect your device and go immediately to install now...Or I would decide if I did not need it for my phone, I would see your smartphone is also at risk, go, no it isn't, and then go remind me later, or go where is a dismiss option." In other words, participants are looking for the nudge to communicate the important information quickly and clearly so that they can get back to their intended task unless they wish to learn more about the advertised mobile antivirus software.

Some participants were also interested in the notifications **repeatedly** (A=9, B=9) reminding them about the mobile antivirus, though they were split on which type of notifications and how frequently the notification should be repeated before becoming annoying. However, Participant 31 summarizes the general purpose of the notification repetition by stating, "I think honestly, the repetitiveness of a notification, which I know repetitive notifications can be annoying, but I feel like just seeing it enough times, I'll be like, oh, the first time I might write it off, but maybe after the third or fourth time I'll be like, yeah, why not? I'm already using this on my laptop, I seem to be enjoying it, it seems very straightforward. Why not just go ahead and add it on to my smart phone? " In other words, some participants were interested in the repetition of the notifications in case they were too busy to install the software at the time, unsure of the importance of the notification, etc.

While less a design guideline for the nudge, and rather a guideline for the design of the mobile antivirus software, participants indicated that one expectation was that there was **consistency** (A=3, B=6) in the designs of the laptop and mobile antivirus software. As participant 2 explains, "one of my expectations would the same layout as on my computer to be on my phone." This also relates with some of the other design guidelines, such as being user-friendly, as users would like to have a low learning curve and barrier to using the mobile antivirus software. Some participants also stated that they expected the notification design to be consistent with industry standards. Participant 16 states "I think that this is a relatively standard notification setup. None of it is too crazy or something that would... I am used to seeing this screen a lot, so I think that it gets the job done." As a result, applying consistency between device applications as well as with other common notification signifiers makes it easier for participants to interact with the notifications and antivirus software, thus decreasing user frustration.

Section 5.3.3 Key Takeaways: Users discussed guidelines for designing simple and effective notifications to raise awareness of specific security risks on smartphones and prompt installation of the software.

5.3.4 Intention to Install

Inclusion of the notifications in existing antivirus software on the laptop/desktop led to 24 out of 36 participants indicating they would be interested in installing antivirus software on their smartphone. However, only 10 participants who saw the control prototype expressed their intent to install, prior to seeing and commenting on the notification designs. Conversely, 14 participants who saw the active and passive notifications first indicated they would be interested in installing the antivirus software on their smartphone. Notably, 10 participants (A=5, B=5) expressly indicated the notifications played a role in positively influencing their stated intent to install the software on their smartphone. As Participant 18 explains, " I should be aware about this, that there exists something like this for my smartphone, and if it just randomly pops in, definitely I'll see if the brand name is familiar to me. Otherwise, I would just ignore it thinking it's some kind of a virus itself. Otherwise, yes, if I'm aware about the brand, if I'm using the same one for the laptop, this should be sufficient information for me to persuade me to download or install the software."

Approximately 67% of participants stating they would be interested in installing the antivirus software on their phone but only 27% expressly stated this was due to the notifications, which indicates increasing users' awareness of the security tool is likely a primary motivator for installation with the notifications being a potentially effective method of doing so. 5 participants had already installed antivirus software on their smartphones before participating in the user study and were among those who indicated they would install the antivirus software on their phones. However, these responses were still considered stated intent to install as all but one of those participants were still describing aspects from the prototype that would encourage

them to install the software. When asked if they would install the software on their phone based on the prototype Participant 34 states, " I don't think I would, because me, personally, I'm not a fan of pop-ups, like, "You shouldn't still have this on your phone," stuff like that. So I would not follow the pop-up, I guess, but yeah, if this was a good antivirus, a reputable one, and was on mobile, then I would consider it". However, even with their focus on the prototype, their pre-existing usage of antivirus software likely did play a factor in increasing their willingness to install the software on their phone due to prior awareness of the existence and functionality of smartphone antivirus software. This is shown in Participants 34's initial statement regarding their intent to install the mobile version of the antivirus software: "I already have it on my phone, so, I mean, I guess, yeah, because I just like to have the link scanning feature on my antivirus, so I make sure there's no malware on any website or anything."

However, effectiveness of the notifications at increasing awareness and encouraging installation of the mobile antivirus software is illustrated by the shifting intention of Participant 21 over the course of their interaction with the prototype. Participant 21 was in Group A and thus did not initially see any of the notifications when viewing the prototype. As a result, when asked if they were interested in installing antivirus software on their smartphone after viewing the prototype, they explained "Not on my phone, because it didn't really give me a prompt or something that this is being offered for a phone. I strictly gave the assumption that it's only for the computer. I wouldn't have known that it's for the phone." They then went on to suggest including a notification that states, "'Get per the phone', or, 'We also have an app.' Because from right now, I don't really see a way that I would know that this provider had something for the phone". This suggestion came before viewing the prototype with the notifications, indicating an expectation that such information is communicated through a notification.

After viewing the prototype with the notifications, Participant 21 went on to state

"Yes, yes. I would assume that I would be really liking this current software. Then yeah, it would definitely make me a lot more interested to get on my phone as well with this pop-up." This shift in opinion illustrates the effectiveness of the notifications in raising awareness of the existence of and need for mobile antivirus software as well as encouraging participants to install the mobile version of the antivirus software.

Additionally, when considering intention to install, participants often mentioned both motivations as well as design guidelines as considerations in their decisions. Participant 29 explains, "I mean, if it looks like this, I mean, sure. It seems pretty intuitive, it seems pretty easy to use." Similarly, participant 9 explains, "Yeah, it looks like it's secure and it's user-friendly". In both cases, the participants are stating both a motivation and a design guideline as deciding factors in their intention to install the antivirus software on their smartphone.

In the case of Participant 29, the motivation is that there is a low effort to install the software and use it. Meanwhile, Participant 9's stated motivation is that the mobile antivirus software is secure and will not introduce vulnerabilities to their smartphone. However, both participants state that the mobile antivirus software being user-friendly as a major consideration regarding the installation of the antivirus software on their smartphone.

This indicates that both installation motivations and design work together to nudge participants in installing antivirus software on their smartphone. As a result, consideration of both users' reasons for installing the software and their preferences for how awareness of the mobile antivirus software is raised should be considered when designing nudges, particularly active nudges. Furthermore, the installation motivations and design guidelines identified in this study, while specific to antivirus software, can be applied to nudges for to prompt adoption of other security behaviors as the underlying goal is the same, likely resulting in similar considerations and needs of the user when viewing the nudge.

Section 5.3.4 Key Takeaways: Notifications informed by device-specific mental models were stated to be effective in prompting installation of antivirus software on other platforms.

5.4 Summary

To determine the effectiveness of notification nudges on one platform in encouraging behavior changes on another platform we created two notification designs, one more active and one more passive. These notifications informed laptop users of a hypothetical antivirus software of the availability and the need for antivirus software on their smartphone to encourage them to download the software on their phone. To do this, the notifications utilized perceptions of risk from the "Security tools are used to mitigate risk" and "Platform is secure" mental models identified in Study 1 to address misconceptions of risk on smartphones. Including these mental models in the general message of the notifications addresses identified common misconceptions or lack of awareness resulting from the prevalence of these mental models on laptops and smartphones.

This study provides one method, or at least elements which were identified as effective by participants, to help future notification design utilize participants' mental models when designing notifications. To do so, both an active notification and passive notification were designed, which had indicated effectiveness in encouraging interest in, if not actual implementation of, antivirus software on a smartphone. While expressed effectiveness was not overwhelmingly different between the control group and the experimental group, more participants did indicate they would be interested in installing the mobile version of the software on their smartphone from the experimental group. While the lack of large differences in expressed notification effectiveness in prompting behavior could be due to the sample size (36 participants) or due to additional factors such as increased awareness resulting from asking about

smartphone-based antivirus software, the larger number of participants stating the laptop antivirus notifications would be effective at causing them to install the antivirus software on their smartphone suggests these notifications are effective at nudging adoption of security behaviors, specifically antivirus software usage, on other devices.

Additionally, we identified participant-stated design guidelines for designing notifications to prompt security behavior on other devices. While many of these guidelines concur with established design guidelines for notifications, some of the participant-stated design guidelines provide specific guidelines for notifications trying to prompt behavior, particularly on another device. These include repeating the notification to remind users to install the software, providing enough factual information to determine why users should download the software, and that the notification should be easily skim-mable to minimize disruption to primary tasks.

Relevant Study Research Questions	Contributions/Findings
RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform?	• Designed two nudges to encourage adoption of antivirus software on another device • Identified user stated motivations for adopting security behaviors on another platform based on two previously identified mental models of security (RQ1)
RQ3.2: What are the user suggested design guidelines for such a notification to encourage attention and adoption?	• Designed two nudges to encourage adoption of antivirus software on another device • Identified user stated guidelines for designing effective nudges to increase awareness of risk and security behaviors on other platforms from a different device

Figure 5.11: Summary of findings and contributions from Study 3.

This study also identified motivators which would encourage or discourage installation of antivirus software, and likely other security tools, on a mobile device based on usage on a laptop. These motivators showed how mental models of security can be utilized to encourage desired security behavior. For example, the motivators dubbed *promotions* and *risk* show evidence that perceptions, or misconceptions, under the *device is secure* mental model play a role in encouraging or discouraging adoption of security behaviors. As a result, these motivators indicate that addressing users' mental

models of security on their devices can encourage them to adopt desired security behaviors. The findings discussed in this chapter are summarized in Figure 5.11.

CHAPTER 6: CONTRIBUTIONS

This dissertation has uncovered five mental models of security and their supporting perceptions which users have on three primary devices- traditional computing devices, smartphones, and tablets. It also identified how these mental models differ by device platform and how these differences in device-specific mental models influence behavior, both general and security-focused behavior, on each device platform. Furthermore, this dissertation identified how these mental models can be used in conjunction with notifications to nudge security tool/behavior adoption on one platform from another, specifically antivirus software adoption on smartphones from viewing of notifications in a laptop-based antivirus software for the purposes of this dissertation. These contributions are summarized below in Figure 6.1 below.

Study 1 provides an understanding of which mental models of security existed for three different device platforms, specifically laptops/desktops, smartphones, and tablets. Additionally, it provides an understanding of how the mental models for each device influenced the security behaviors implemented on each device. In this study, five mental models were identified which were present on all three device platforms to some degree. However, while the overall models identified were the same, the supporting perceptions and prevalence varied by platform. Additionally, this studied confirmed the continued relevance of the folk models previously identified by Rick Wash with indicators of new folk models, likely as a result in shifting usage of devices. In addition to the identification of these mental models and perceptions of security, Study 1 also found a distinct lack of awareness of potential security risks and mechanisms on smartphones and tablets as compared to traditional computing devices.

Study 2 expanded upon these results and identified the generalization of the mental

Research Question	Relevant Study Research Questions	Contributions/Findings	Relevant Sections
RQ1: What are mental models of security on various device platforms and how are they similar or different?	• RQ1.1: What are users' mental models of security on laptop/desktops, smartphones, and tablets? • RQ1.2: What are the similarities and differences in perceptions of security risks across the three platforms? • RQ2.1: What are the similarities and differences in mental models of security by device platform?	Identification of 5 mental models of security with supporting perceptions	Section 3.4.3
		Identification of variances in prevalance of these mental models and perceptions of security on different device platforms	Section 3.4.3 Section 4.3.2
		Identification of similarities in prevalance of these mental models and perceptions of security on different device platforms	Section 3.4.3 Section 4.3.2
		Partially support the alternate hypothesis HA 2.1: There are statistically significant variances between the supporting perceptions for each mental model on laptop/desktops, smartphones, and tablets.	Section 4.3.2
RQ2: How do the perceptions of risk and security mitigation strategies relate to each other?	• RQ1.3: What are the similarities and differences in security behaviors on the three platforms, and what do these behaviors indicate about the mental models users have for each platform? • RQ2.2: What are the similarities and differences in the factors influencing security behavior on different device platforms? • RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms?	Identification of device-specific similarities and differences in security tool adoption	Section 3.4.5 Section 4.3.3
		Identification of device-specific similarities in security behavior adoption	Section 3.4.5 Section 4.3.4
		Identification of the four most common factors influencing security tool adoption across all three device platforms	Section 4.3.3
		Identification of the five most common factors influencing security behavior adoption across all three device platforms	Section 4.3.4
RQ3: How can mental models and adopted security behaviors on one platform be used to inform perceptions of risk on another platform?	• RQ2.3: How do these mental models of security correlate to the implementation of security behavior on the different device platforms? • RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform?	Designed two nudges to encourage adoption of antivirus software on another device	Section 5.2.2 Section 5.3.4
		Identified user stated motivations for adopting security behaviors on another platform based on two previously identified mental models of security (RQ1)	Section 5.3.2
		Partially support the alternate hypothesis HA 2.2: There is a correlation between some of the device-specific mental models and the adoption of security behaviors on each device platform.	Section 4.3.5
RQ4: How can you increase awareness of risk and effective security mechanisms on different platforms based on the perceptions on an existing platform?	• RQ3.1: Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform? • RQ3.2: What are the user suggested design guidelines for such a notification to encourage attention and adoption?	Designed two nudges to encourage adoption of antivirus software on another device	Section 5.2.2 Section 5.3.4
		Identified user stated guidelines for designing effective nudges to increase awareness of risk and security behaviors on other platforms from a different device	Section 5.3.3
		Identified user stated motivations for adopting security behaviors on another platform based on two previously identified mental models of security (RQ1)	Section 5.3.2

Figure 6.1: Summary of contributions per research question.

models identified in Study 1 to a larger population. Furthermore, this study identified descriptive and statistical differences between device platforms in the prevalence of perceptions amongst the various mental models. Additionally, it identified the factors which influence security behaviors and the potential for statistical correlations between existing mental models and adopted security tools and behavior.

Building upon the influence of mental models of security on behavior, Study 3 determined the stated effectiveness of informational notifications in security tools on one platform in encouraging the adoption of the same tool in another platform. Specifically, this dissertation proposed two notification designs which were tested in a laptop-based antivirus software and evaluated for user expressed interest in installing

anti-virus software on a smartphone. Additionally, this study identified user-stated motivations in installing software on another device and design guidelines for similar information notifications which can be used to improve the effectiveness of future notifications both in antivirus software and, likely, in other security tools.

Through these studies, this dissertation identified device-specific mental models of security and factors of behavior which influence security behaviors on each platform. Additionally, this dissertation proposed one method for building upon users' existing mental models of security by utilizing already implemented security mechanisms, specifically notifications and nudges in installing antivirus software, to raise awareness of effective security practices on other platforms and to encourage the adoption of these practices on other devices.

6.0.1 Mental Models of Security

This dissertation also identifies five mental models of security which are found on traditional computing devices, smartphones, and tablets. These mental models and their supporting perceptions were first identified in the first study and are described as "the device platform is secure", "apps are secure", "security tools are used to mitigate risk", "web browsing and downloading is risky", and "limited risk due to usage". As shown in the first and second study, these mental models and their perceptions do exist across all three platforms, even within a large population, lending support to the establishment of these as mental models of security on all three platforms.

Furthermore, this dissertation demonstrates variances in the prevalence of each mental model and their supporting perceptions on each platform. While the mental models were present on all the platforms in both Study 1 and Study 2, their supporting perceptions varied in prevalence across the platforms. Additionally, a few of the supporting perceptions were found to be unique to some of the platforms in Study 1. These perceptions were "smartphones are less vulnerable to hackers and viruses", "tablets are similar to smartphones", and "smartphones are more secure". The device-

specific differences in mental model adoption can be used to help understand and explain differences in security mechanism usage and awareness of risk on each platform. As seen in the second and third study, decreased implementation of mental models on the device platforms coincided with a decreased adoption of security tools, and, to a lesser extent, security behaviors on those platforms. Additionally, these variances can be used to help prompt security tool adoption, as shown by the third study. However, statistical correlation between mental models and adopted security mechanisms was not established and would be a component for future work to explore.

This dissertation identified the mental models "platform is secure" and "limited risk due to usage" as more prevalent on tablets than on the other devices. This generally indicates that users perceive tablets to be secure due to built-in security measures and a lack of sensitive information stored on the devices. Additionally, users perceive "applications as more secure" on tablets. This also generally corresponds to a lack of prevalence with the perceptions that security tools, including web-based security tools, are necessary for protecting the tablet from the mental models "security tools are used to mitigate risk" and "web browsing and downloading is risky". As a result of these mental models working together, users are less likely to implement additional security tools and mechanisms on tablets due to the perception that tablets are not at risk due to factors such as the manufacturer, built-in security measures, and a lack of sensitive information on the device.

The mental models "web browsing and downloading is risky" and "security tools are used to mitigate risk" are generally more prevalent on traditional computing devices with the caveat that it is the perceptions supporting the need for security tools, including application-based security tools, that are prevalent from the "security tools are used to mitigate risk" mental model. This indicates that participants generally view traditional computing devices as less secure and thus require more security mechanisms to protect information on these devices.

However, smartphones are generally perceived to be in between the two aforementioned devices regarding risk and required security behaviors. A couple of perceptions are more prevalent on smartphones, specifically "device is secure" from the "platform is secure mental model" and "high risk due to high usage" from the "limited risk due to usage" mental model. As a result, users generally view smartphones as being secure but recognize some potential for security vulnerabilities and thus the need for the implementation of security mechanisms. However, there is still a stronger reliance on built-in protections than application-based security mechanisms.

These variances in prevalence of mental models and their supporting perceptions on each device platform indicates a lack of awareness of risk and available security tools and behaviors. Additionally, these variances indicate the need to speak to existing device-specific mental models to prompt desired security behaviors on a device rather than trying to use non-prevalent mental models to encourage adoption of device-specific security mechanisms.

6.0.2 Awareness and Education

Throughout this dissertation, the importance of awareness and education in the adoption of security behaviors and mental models has been a consistent consideration. This is largely in part due to the lack of awareness of risk and available security mechanisms on smartphones and tablets. In both the first and the second study, there was a distinct difference in the types of security tools and behaviors on all three of the device platforms, with participants often relying more on less complex security tools to protect their information on smartphones and tablets, such as ad blockers and bio-metric security mechanisms, while utilizing more complex security tools on traditional computing devices, such as antivirus software.

Additionally, all three studies noted a lack of awareness of risk and available security tools on each of the platforms, though primarily on smartphones and tablets. While this appears in the first two studies in the difference of adopted security tools and

behaviors, it also appears in the differences in prevalence of perceptions within the "Security tools are used to mitigate risk" mental model. This lack of awareness is illustrated by more participants indicating they viewed security tools as useful and necessary to protect their traditional computing devices than smartphones and tablets. Additionally, users' mental model of their device being secure seems to rely, at least in part, on security tools in traditional computing devices and the device-specific protections in mobile computing devices.

This lack of awareness of risk is also seen in the third study through the motivator "awareness" and the influence it has on encouraging installation of the mobile version of the antivirus software. Additionally, some participants stated a lack of awareness of the availability of antivirus software on smartphones. This lack of awareness of the availability of smartphone-based security mechanisms and vulnerabilities results in decreased adoption of security tools compared to traditional computing devices and an increased perception that smartphones are secure, as shown in the smartphone-specific prevalent perceptions described in the previous section.

Therefore, as shown through the three studies in this dissertation, device-specific variances in mental models such as "Device platform is secure" and "Security tools are used to mitigate risk" influence device-specific security behaviors and security tool adoption. As a result, awareness and security education specific to some of the misconceptions users face on each platform are important in prompting good security practices on those devices.

6.0.3 Security Behavior Adoption

This dissertation also identifies device specific security behaviors and tool adoption that are either associated with mental models of security such as in Study 1 or have the potential of being correlated to mental models of security such as in Study 2. The identified similarities and differences in device-specific security behaviors and tool adoption along with their association with mental models of security and their

underlying perceptions indicate that not only can one potentially be indicative of the other but also that mental models of security may be used to prompt security behaviors, as shown in Study 3.

One example of this is implementation of application-based security tools versus devices-specific security tools on different device platforms. As shown in Study 1 and Study 2, users are more likely to use application-based software on traditional computing devices while relying more on device-based security mechanisms on their smartphone and tablet. This pattern of behavior has a direct association with the mental model "Security tools are used to mitigate risk" but adoption of security tools on different platforms is also likely influenced by other mental models such as limited risk due to usage decreasing the perceived need for security tools due to lower risk. As this mental model is more prevalent on tablets as shown in Study 1 and 2, this supports the lower usage of application-based security tools on tablets.

However, this found limited indications that there are device-specific differences in security tool adoption even with device-specific differences in perceptions of security. While this could indicate that there is no relationship between mental models of security and adopted security behavior, the limited awareness of risk on smartphones and tablets found in Study 1 and Study 3 indicate there is likely an alternative explanation for the similarities in adopted security behaviors across the platforms. One such reason could be the formation of security behavior habits on laptops which carry over to the other devices. However, future work would need to be done to establish the reason(s) behind this pattern.

Additionally, this dissertation shows that using users' mental models to inform design has the potential of nudging users to adopt desired security practices. For example, Study 3 shows that educating users regarding misconceptions in their mental models of security on smartphones, such as that the "platform is secure", can be effective in at least prompting users to consider adopting the described curative security

mechanism.

6.0.4 Future Work

There are three main areas of future research that would be beneficial for expanding on the findings of this dissertation. The first is to explore the mental models of security of users who do not own or use a traditional computing device. A comparison of their mental models and the ones identified in Study 1 would help determine the potential influence of security education on the formation of device-specific mental models.

Another area of future research would be to conduct another survey to attempt to establish a correlation between mental models of security and adopted security tools and behaviors. As mentioned in Study 2, this dissertation was only able to establish there were very weak to negligible statistically significant correlations between the majority of the mental models of security and adopted security tools/behaviors. This was potentially due to factors such as the similarity in the data ranges of the variables and the sample size of the dataset. However, the survey could be reformulated or completely redesigned to provide more diverse data inputs to not only explore the potential correlation between mental models and security mechanisms but also to further explore the variability of device-specific mental models. Additionally, this redesigned survey could be given to a larger population which would meet the requirements of a power analysis to determine any potential statistical correlation between mental models and security tool/behavior adoption.

The final proposed future work is to expand upon the findings of the third study which are indicative of nudges on one device platform being effective in prompting desired security mechanism adoption on another platform. To do so, a more extensive and controlled user study could be conducted to explore the actual effectiveness of the notifications in nudging security tool adoption.

6.0.5 Conclusion

This dissertation identifies mental models of security on traditional computing devices, smartphones, and tablets. Specifically, it proposes five new mental models of security as existing on all three device platforms while having variances in their supporting perception prevalence and implementation which influence device-specific security behaviors and device usage. Additionally, this dissertation observes that many of these mental models seemed to be formed on laptops and then adapted to apply to smartphones and tablets. Furthermore, participants generally had an increased awareness of risk on traditional computing devices when compared to other device platforms. This indicates that there is the potential for laptop-based security education and awareness campaigns as well as security experiences to be a primary influence in the formation of device-specific mental models.

Through this dissertation, these mental models were found to have differences in prevalence across their supporting perceptions amongst the various device platforms which resulted in device-specific applications of the mental models and device-specific adoptions of security behaviors. While there were observed differences between the stated adoption of security tools and identified mental models across device platforms, there were limited variances in the stated adoption of security behaviors across device platforms. This difference in effect of mental models on security mechanism adoption is potentially due to the formation of security behavior habits on one device influencing the adoption of the same security behaviors on other devices.

This dissertation also proposes a method of using mental models and nudges to prompt adoption of security behavior or tools on one device from another. To do so, this dissertation provides both design guidelines and motivators which should be considered when designing a nudge with the intention of prompting a desired behavior. Using these design guidelines and behavioral motivators can be used either to address misconceptions in device-specific mental models or build upon device-specific mental

models to work with users' perceptions of security and risk on each of their devices rather than against them.

REFERENCES

[1] A. H. Z. Abidin, H. Xie, and K. W. Wong. Eliciting mental model of blind people for web page. In *Proceedings of the 5th International Conference on Rehabilitation Engineering & Assistive Technology*, i-CREATe '11, Midview City, SGP, 2011. Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre.

[2] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei. Exploring user mental models of End-to-End encrypted communication tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, Baltimore, MD, Aug. 2018. USENIX Association.

[3] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), aug 2017.

[4] F. Asgharpour, D. Liu, and L. J. Camp. Mental models of security risks. In S. Dietrich and R. Dhamija, editors, *Financial Cryptography and Data Security*, pages 367–377, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[5] D. E. Bambauer. Privacy versus security symposium on cybercrime. *Journal of Criminal Law and Criminology*, 103(3):667, 2013.

[6] J. Blythe and L. J. Camp. Implementing mental models. In *2012 IEEE Symposium on Security and Privacy Workshops*, pages 86–90, 2012.

[7] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt. A survey on smartphone user's security choices, awareness and education. *Computers & Security*, 88:101647, 2020.

[8] J. M. Corbin and A. Strauss. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1):3–21, Mar 1990.

[9] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, Menlo Park, CA, July 2014. USENIX Association.

[10] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1416–1426, New York, NY, USA, 2015. Association for Computing Machinery.

[11] S. Das, B. Wang, A. Kim, and L. J. Camp. Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies. Jan 2020. Accepted: 2020-01-04T08:18:52Z.

[12] F. Davis, R. Bagozzi, and P. Warshaw. User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35:982–1003, 08 1989.

[13] J. Dinet and M. Kitajima. "draw me the web": impact of mental model of the web on information search performance of young users. In *Proceedings of the 23rd Conference on l'Interaction Homme-Machine*, IHM '11, New York, NY, USA, 2011. Association for Computing Machinery.

[14] N. Ebert, K. Alexander Ackermann, and B. Scheppler. Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[15] S. Egelman, M. Harbach, and E. 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. Association for Computing Machinery.

[16] S. Egelman and E. Peer. Predicting privacy and security attitudes. *SIGCAS Comput. Soc.*, 45(1):22–28, feb 2015.

[17] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, Denver, CO, June 2016. USENIX Association.

[18] C. Faklaris, L. Dabbish, and J. Hong. A self-report measure of end-user security attitudes (sa-6), 05 2019.

[19] C. Faklaris, L. Dabbish, and J. I. Hong. Do they accept or resist cybersecurity measures? development and validation of the 13-item security attitude inventory (sa-13), 2022.

[20] E. Fife and J. Orjuela. The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, 4:11, 2012.

[21] B. Fogg. A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology*, Persuasive '09, New York, NY, USA, 2009. Association for Computing Machinery.

[22] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 591–600, New York, NY, USA, 2006. Association for Computing Machinery.

[23] N. Gerber, V. Zimmermann, and M. Volkamer. Why johnny fails to protect his privacy. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 109–118, 2019.

[24] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 321–340, Denver, CO, June 2016. USENIX Association.

[25] J. Haney, Y. Acar, and S. Furman. "it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. page 19.

[26] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*, pages 209–223, 2012.

[27] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. pages 39–52, 2015.

[28] M. Kauer, S. GÃŒnther, D. Storck, and M. Volkamer. A comparison of american and german folk models of home computer security. In L. Marinos and I. Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, pages 100–109, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[29] A. Kitkowska, M. Warner, Y. Shulman, E. Wästlund, and L. A. Martucci. Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 437–456. USENIX Association, Aug. 2020.

[30] O. Kulyk, P. Gerber, K. Marky, C. Beckmann, and M. Volkamer. Does this app respect my privacy? design and evaluation of information materials supporting privacy-related decisions of smartphone users. In *Proceedings 2019 Workshop on Usable Security*, San Diego, CA, 2019. Internet Society.

[31] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak. 'no telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), dec 2017.

[32] A. Mylonas, A. Kastania, and D. Gritzalis. Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security*, 34:47–66, 2013.

[33] J. D. Ndibwile, E. T. Luhanga, D. Fall, D. Miyamoto, and Y. Kadobayashi. A comparative study of smartphone-user security perception and preference towards

redesigned security notifications. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, AfriCHI '18, New York, NY, USA, 2018. Association for Computing Machinery.

[34] M. Nourani, C. Roy, J. E. Block, D. R. Honeycutt, T. Rahman, E. D. Ragan, and V. Gogate. On the importance of user backgrounds and impressions: Lessons learned from interactive ai applications. *ACM Trans. Interact. Intell. Syst.*, 12(4), dec 2022.

[35] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako, and L. F. Cranor. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies*, 2018(4):5–32, Oct 2018.

[36] J. Ophoff and M. Robinson. Exploring end-user smartphone security awareness within a south african context. In *2014 Information Security for South Africa*, pages 1–7, 2014.

[37] A. R. Peslak and N. Bhatnagar. A review of internet shopping factors: Do the technology acceptance model or theory of reasoned action model apply? *Issues Inf. Syst*, 10:495–504, 2009.

[38] G. J. B. Philip Menard and R. E. Crossler. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4):1203–1230, 2017.

[39] X. Qian, Y. Yang, and Y. Gong. The art of metaphor: A method for interface design based on mental models. In *Proceedings of the 10th International Conference on Virtual Reality Continuum and Its Applications in Industry*, VRCAI '11, pages 171–178, New York, NY, USA, 2011. Association for Computing Machinery.

[40] R. W. Reeder, I. Ion, and S. Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security and Privacy*, 2017.

[41] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why doesn't jane protect her privacy? In E. De Cristofaro and S. J. Murdoch, editors, *Privacy Enhancing Technologies*, pages 244–262, Cham, 2014. Springer International Publishing.

[42] M. Sherer, J. E. Maddux, B. Mercandante, S. Prentice-Dunn, B. Jacobs, and R. W. Rogers. The self-efficacy scale: Construction and validation. *Psychological Reports*, 51(2):663–671, 1982.

[43] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, Mar. 2015.

[44] E. Spero and R. Biddle. Out of sight, out of mind: Ui design and the inhibition of mental models of security. In *New Security Paradigms Workshop 2020*, NSPW '20, pages 127–143, New York, NY, USA, 2021. Association for Computing Machinery.

[45] M. Tabassum, T. Kosinski, and H. R. Lipford. "i don't own the data": End user perceptions of smart home device data practices and risks. pages 435–450, 2019.

[46] N. Taha and L. Dahabiyeh. College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, 26(2):1721–1736, Mar. 2021.

[47] R. van Bavel, N. RodrÃguez-Priego, J. Vila, and P. Briggs. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123:29–39, Mar. 2019.

[48] V. Venkatesh, M. Morris, G. Davis, and F. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27:425–478, Sept. 2003.

[49] M. Volkamer and K. Renaud. *Mental Models - General Introduction and Review of Their Application to Human-Centred Security*, pages 255–280. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[50] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery.

[51] R. Wash and E. Rader. Influencing mental models of security: A research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*, NSPW '11, pages 57–66, New York, NY, USA, 2011. Association for Computing Machinery.

[52] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 1077–1093, 2017.

[53] J. Wu and D. Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, Baltimore, MD, Aug. 2018. USENIX Association.

[54] S. Xiao, J. Witschey, and E. Murphy-Hill. Social influences on secure development tool adoption: why security tools spread. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 1095–1106, New York, NY, USA, 2014. Association for Computing Machinery.

[55] B. Xie, J. Zhou, and H. Wang. How influential are mental models on interaction performance? exploring the gap between users' and designers' mental models through a new quantitative method. *Advances in Human-Computer Interaction*, 2017(1):3683546, 2017.

[56] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[57] V. Zimmermann, M. Bennighof, M. Edel, O. Hofmann, J. Jung, and M. von Wick. 'home, smart home' - exploring end users' mental models of smart homes. In R. Dachselt and G. Weber, editors, *Mensch und Computer 2018 - Workshopband*, Bonn, 2018. Gesellschaft fÃŒr Informatik e.V.

APPENDIX A: STUDY 1: INTERVIEW SCRIPT

1. Which study is this?
2. Do you own at least two devices, if so what?
3. What personal technology devices, such as smartphones or laptops, do you use on a regular basis?
4. Which device(s) would you use for banking transactions? Check all that apply.
   (a) Tablet
   (b) Laptop/Desktop
   (c) Smartphone
   (d) Other:
5. Why would you use this/these devices? Why would you not use [device(s)]?
6. Which device(s) would you use for bill payment? Check all that apply.
   (a) Tablet
   (b) Laptop/Desktop
   (c) Smartphone
   (d) Other:
7. Why would you use this/these devices? Why would you not use [device(s)]?
8. Which device(s) would you use for online shopping? Check all that apply.
   (a) Tablet
   (b) Laptop/Desktop
   (c) Smartphone

(d) Other:

9. Why would you use this/these devices? Why would you not use [device(s)]?

10. Which device(s) would you use for social media? Check all that apply.

    (a) Tablet

    (b) Laptop/Desktop

    (c) Smartphone

    (d) Other:

11. Why would you use this/these devices? Why would you not use [device(s)]?

12. Which device is being used for Device 1?

13. What types of applications do you or would you primarily use on [Device 1]?

14. What types of applications do you not or would you not use on [Device 1]? Why?

15. Have you ever had any security or privacy problems with [Device 1] or the applications used on [Device 1]? Such as a virus? Or getting hacked?

16. If yes, can you describe what happened? Follow up questions: How did you know it was a [virus/hacker/identity theft/other type of concern]? How was it detected? How did you fix it?Do you know where it came from/how you got it? (Virus only) Do you know who did it? (Hackers only)

17. What types of security/privacy issues are you concerned about happening on [Device 1]?

18. Are you worried about viruses on [Device 1]?

19. If yes, what are you worried viruses will do? What do you do about it?

20. If no, why not?

21. Are you worried about hackers on [device 1]?

22. If yes, what do you think they will do? What do you do to protect yourself?

23. If no, why not?

24. What security/privacy measures do you have on [Device 1]? Do you use an antivirus, call blocker, etc?

25. Which device is being used for Device 2?

26. What types of applications do you or would you primarily use on [Device 2]?

27. What types of applications do you not or would you not use on [Device 2]? Why?

28. Have you ever had any security or privacy problems with [Device 2] or the applications used on [Device 2]? Such as a virus? Or getting hacked?

29. If yes, can you describe what happened? Follow up questions: How did you know it was a [virus/hacker/identity theft/other type of concern]? How was it detected? How did you fix it? Do you know where it came from/how you got it? (Virus only) Do you know who did it? (Hackers only)

30. What types of security/privacy issues are you concerned about happening on [Device 2]?

31. Are you worried about viruses on [Device 2]?

32. If yes, what are you worried viruses will do? What do you do about it?

33. If no, why not?

34. Are you worried about hackers on [Device 2]?

35. If yes, what do you think they will do? What do you do to protect yourself?

36. If no, why not?

37. What security/privacy measures do you have on [Device 2]? Do you use an antivirus, call blocker, etc?

38. What types of applications do you or would you primarily use on [tablets, smartphones, laptops/desktops (whichever option isn't covered by Device 1 and 2)]? Why?

39. What types of applications do you not or would you not use on [tablets, smartphones, laptops/desktops (whichever option isn't covered by Device 1 and 2)]? Why?

40. If you know anyone who may be interested in participating in the study, please feel free to share the study information with them.

APPENDIX B: STUDY 2: SINGLE FACTOR ANOVA RESULTS BY PERCEPTION

Anova: Single Factor- Limited Risk Due to Limited Data on Device						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM1_1	192	35	0.18229167	0.14984184		
SM1_1	192	30	0.15625	0.13252618		
M1_1	192	105	0.546875	0.24910013		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	18.3159722	2	9.15798611	51.6944587	2.2909E-21	3.01144916
Within Groups	101.510417	573	0.17715605			
Total	119.826389	575				

Figure B.1: Single factor anova of the first perception in the "Limited risk due to usage" mental model.

Anova: Single Factor- High risk due to high usage						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM1_2	192	146	0.76041667	0.183137		
SM1_2	192	156	0.8125	0.15314136		
TM1_2	192	74	0.38541667	0.23811082		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	20.8472222	2	10.4236111	54.4418914	2.2557E-22	3.01144916
Within Groups	109.708333	573	0.19146306			
Total	130.555556	575				

Figure B.2: Single factor anova of the second perception in the "Limited risk due to usage" mental model.

Anova: Single Factor- Limited access to important data and app usage on this device						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM1_3	192	139	0.72395833	0.20088896		
SM1_3	192	143	0.74479167	0.19107221		
TM1_3	192	151	0.78645833	0.1688209		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.38888889	2	0.19444444	1.04021396	0.3540454	3.01144916
Within Groups	107.109375	573	0.18692736			
Total	107.498264	575				

Figure B.3: Single factor anova of the third perception in the "Limited risk due to usage" mental model.

Anova: Single Factor-Stopping device stops risk						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM1_4	192	60	0.3125	0.21596859		
SM1_4	192	59	0.30729167	0.21397797		
TM1_4	192	73	0.38020833	0.23688373		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.63541667	2	0.31770833	1.42933671	0.2403202	3.01144916
Within Groups	127.364583	573	0.22227676			
Total	128	575				

Figure B.4: Single factor anova of the fourth perception in the "Limited risk due to usage" mental model.

Anova: Single Factor- Security tools help protect device						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM2_1	192	176	0.91666667	0.07678883		
SM2_1	192	158	0.82291667	0.14648778		
TM2_1	192	139	0.72395833	0.20088896		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	3.56597222	2	1.78298611	12.6105432	4.3694E-06	3.01144916
Within Groups	81.015625	573	0.14138853			
Total	84.5815972	575				

Figure B.5: Single factor anova of the first perception in the "Security tools are used to mitigate risk" mental model.

Anova: Single Factor- Security tools are needed to protect device						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM2_2	192	164	0.85416667	0.12521815		
SM2_2	192	140	0.72916667	0.19851658		
TM2_2	192	121	0.63020833	0.23426592		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	4.83680556	2	2.41840278	13.0021502	3.0035E-06	3.01144916
Within Groups	106.578125	573	0.18600022			
Total	111.414931	575				

Figure B.6: Single factor anova of the second perception in the "Security tools are used to mitigate risk" mental model.

Anova: Single Factor- Built in security tools are sufficient						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM2_3	192	88	0.45833333	0.2495637		
SM2_3	192	101	0.52604167	0.25062718		
TM2_3	192	122	0.63541667	0.23287522		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	3.06597222	2	1.53298611	6.27359298	0.00201751	3.01144916
Within Groups	140.015625	573	0.24435537			
Total	143.081597	575				

Figure B.7: Single factor anova of the third perception in the "Security tools are used to mitigate risk" mental model.

Anova: Single Factor- Security is not a priority due to cost						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM2_4	192	54	0.28125	0.20320681		
SM2_4	192	49	0.25520833	0.19107221		
TM2_4	192	70	0.36458333	0.23287522		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.25347222	2	0.62673611	2.99799991	0.05066993	3.01144916
Within Groups	119.786458	573	0.20905141			
Total	121.039931	575				

Figure B.8: Single factor anova of the fourth perception in the "Security tools are used to mitigate risk" mental model.

Anova: Single Factor- Security is not a priority over functionality						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM2_5	192	49	0.25520833	0.19107221		
SM2_5	192	44	0.22916667	0.17757417		
TM2_5	192	63	0.328125	0.22161322		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.01041667	2	0.50520833	2.56772614	0.07759223	3.01144916
Within Groups	112.739583	573	0.1967532			
Total	113.75	575				

Figure B.9: Single factor anova of the fifth perception in the "Security tools are used to mitigate risk" mental model.

Anova: Single Factor- Device is secure						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM3_1	192	123	0.640625	0.23142997		
SM3_1	192	129	0.671875	0.22161322		
TM3_1	192	125	0.65104167	0.22837587		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.09722222	2	0.04861111	0.21401417	0.80740145	3.01144916
Within Groups	130.151042	573	0.22713969			
Total	130.248264	575				

Figure B.10: Single factor anova of the first perception in the "Platform is secure" mental model.

Anova: Single Factor- Security risks result from user error						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM3_2	192	92	0.47916667	0.2508726		
SM3_2	192	83	0.43229167	0.24670048		
TM3_2	192	100	0.52083333	0.2508726		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.75347222	2	0.37673611	1.51007396	0.22177138	3.01144916
Within Groups	142.953125	573	0.24948189			
Total	143.706597	575				

Figure B.11: Single factor anova of the second perception in the "Platform is secure" mental model.

Anova: Single Factor- Company is trustworthy and thus secure						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM3_3	192	39	0.203125	0.1627127		
SM3_3	192	42	0.21875	0.17179319		
TM3_3	192	56	0.29166667	0.20767888		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.85763889	2	0.42881944	2.37273047	0.09414123	3.01144916
Within Groups	103.557292	573	0.18072826			
Total	104.414931	575				

Figure B.12: Single factor anova of the third perception in the "Platform is secure" mental model.

Anova: Single Factor- Web browsing and downloading is risky						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM4_1	192	145	0.75520833	0.18583661		
SM4_1	192	113	0.58854167	0.24342823		
TM4_1	192	120	0.625	0.23560209		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	2.94791667	2	1.47395833	6.65076696	0.00139516	3.01144916
Within Groups	126.989583	573	0.22162231			
Total	129.9375	575				

Figure B.13: Single factor anova of the first perception in the "Web browsing and downloading is risky" mental model.

Anova: Single Factor- Web based security tools protect from internet based risks						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM4_2	192	110	0.57291667	0.24596422		
SM4_2	192	90	0.46875	0.25032723		
TM4_2	192	90	0.46875	0.25032723		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.38888889	2	0.69444444	2.79035793	0.06223379	3.01144916
Within Groups	142.604167	573	0.24887289			
Total	143.993056	575				

Figure B.14: Single factor anova of the second perception in the "Web browsing and downloading is risky" mental model.

Anova: Single Factor- Good web browsing practices help mitigate risk						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM4_3	192	165	0.859375	0.12148233		
SM4_3	192	161	0.83854167	0.13609839		
TM4_3	192	160	0.83333333	0.13961606		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.07291667	2	0.03645833	0.27536729	0.75939361	3.01144916
Within Groups	75.8645833	573	0.13239892			
Total	75.9375	575				

Figure B.15: Single factor anova of the third perception in the "Web browsing and downloading is risky" mental model.

Anova: Single Factor- Apps are secure						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM5_1	192	80	0.41666667	0.2443281		
SM5_1	192	99	0.515625	0.25106348		
TM5_1	192	113	0.58854167	0.24342823		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	2.85763889	2	1.42881944	5.80176423	0.00320257	3.01144916
Within Groups	141.114583	573	0.24627327			
Total	143.972222	575				

Figure B.16: Single factor anova of the first perception in the "Applications are secure" mental model.

Anova: Single Factor- Third party apps are risky						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
LM5_2	192	167	0.86979167	0.11384708		
SM5_2	192	154	0.80208333	0.15957679		
TM5_2	192	147	0.765625	0.18038285		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.07291667	2	0.53645833	3.54638866	0.02946303	3.01144916
Within Groups	86.6770833	573	0.15126891			
Total	87.75	575				

Figure B.17: Single factor anova of the second perception in the "Applications are secure" mental model.

APPENDIX C: STUDY 2: QUALTRICS SURVEY FLOW

Figure C.1: The first part of the survey flow from Study 2.

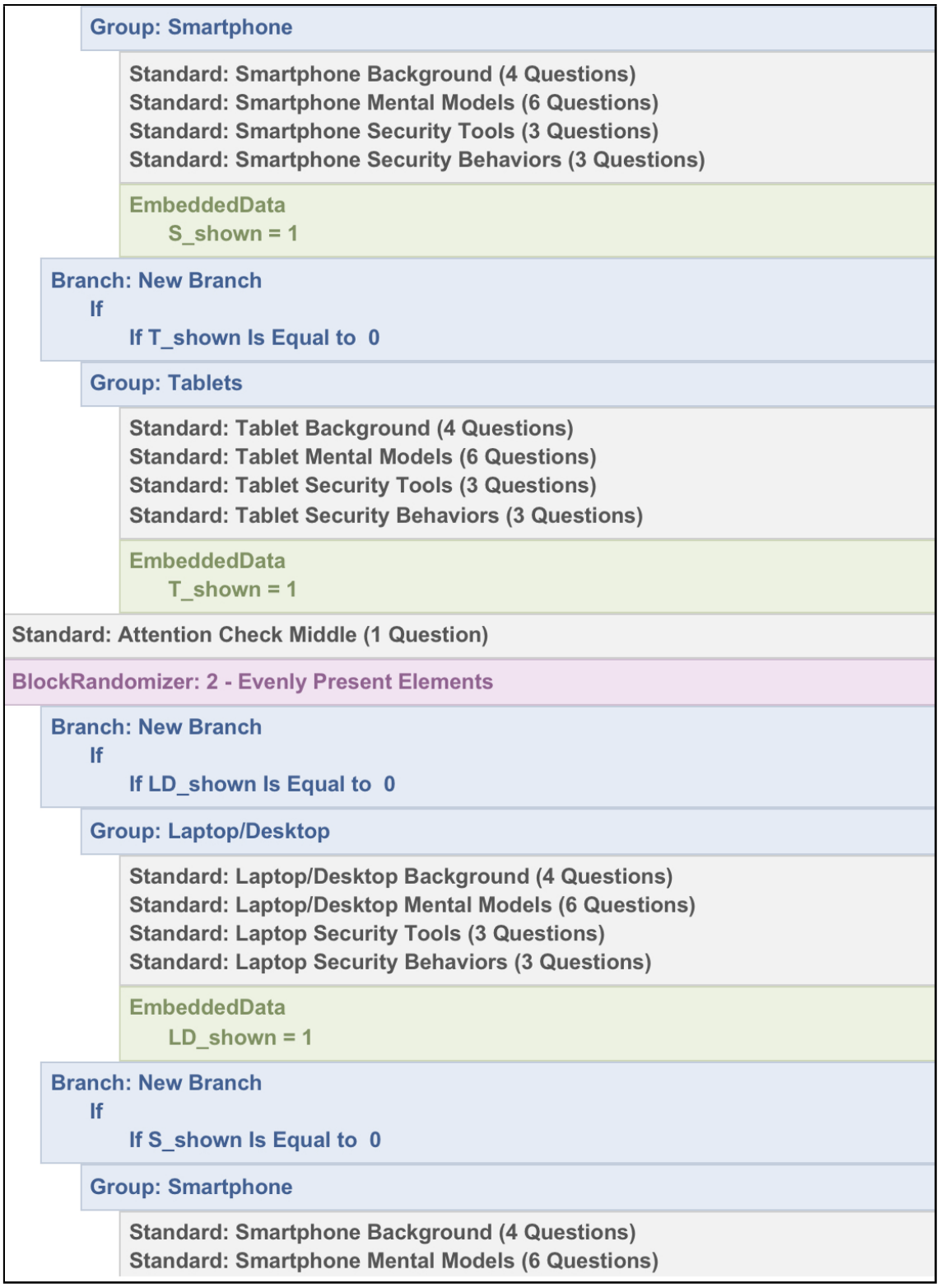

Figure C.2: The second part of the survey flow from Study 2.

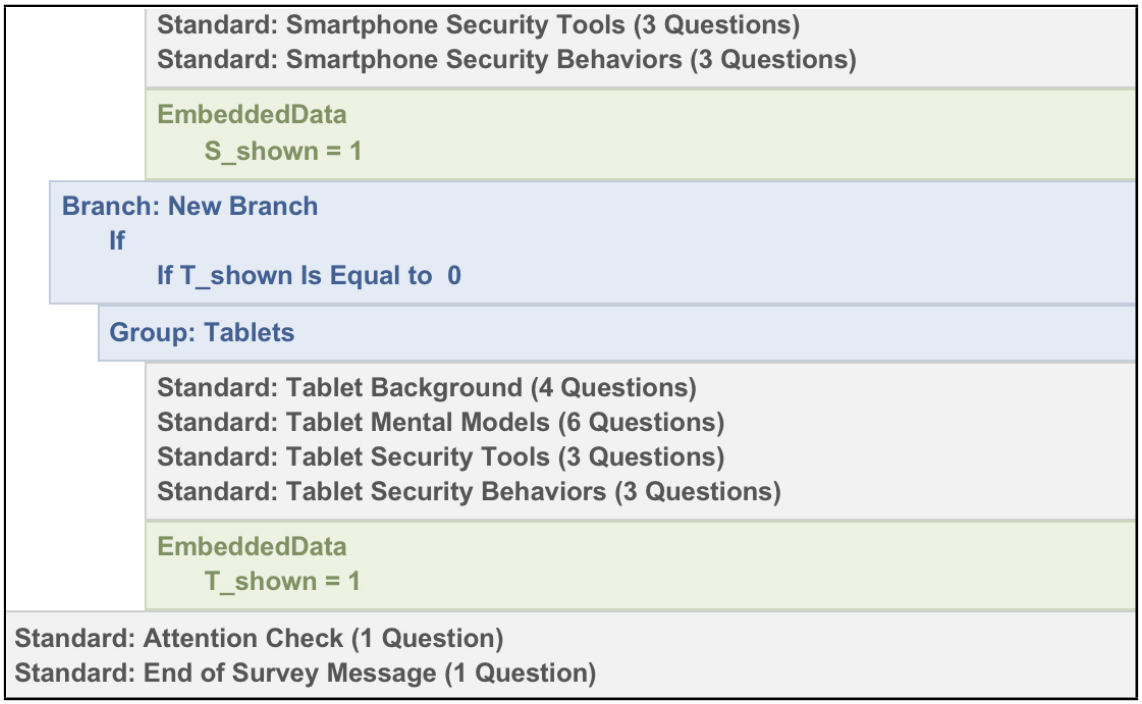

Figure C.3: The third part of the survey flow from Study 2.

APPENDIX D: STUDY 3: PHASE 1 SCRIPT

Introduction: "Hello, my name is [Your Name]."

If the participant hasn't filled out the consent form: "I am seeing that you haven't filled out the consent form yet. You can find a link to the consent form in the same email that contained today's zoom link. Will you please take a few minutes to complete the consent form before we begin?"

Begin zoom recording: "This study is being recorded, so I am now going to begin the recording."

Introduction: In this study we are trying to test a few designs for encouraging customers of a hypothetical antivirus software to install a new mobile version of the software on their phones to determine the most effective notification design for prompting installation of the new software. This study has two parts. During this first part, I will walk you through the three potential notification designs in the hypothetical laptop antivirus software. During this walkthrough you can ask any questions, including questions about the design or functionality of the notification. For the second part of the study, I will ask you a few questions about your experience and thoughts on the design of the notification. I will also ask you to provide feedback and suggestions on the design of the notifications and which notification design you preferred.

Notification Walkthrough:

Per storyboard: I am showing you the [first/second/third] design for a notification. Please take a moment to look through the design and let me know if you have any questions about it.

For third design: "This notification has two parts. After clicking on the Notification tab in the menu on the left (Part 1), you would be sent to this notification page (Part 2).

End of walkthrough: "Thank you; that was the last of the designs. I am now going to ask you some questions to get your feedback for each of the designs. For this portion of the study, I will show you an overview of all the designs for reference. If you would like to see any of the designs again, please let me know and I will pull up that design.

Interview Questions

1. Do you currently use any antivirus software on your laptop/desktop? If so, which one? If not, why not?
2. Do you currently use any antivirus software on your smartphone? If so, which one? If not, why not?
3. For each notification
   (a) What did you like about the notification? Design, location, explanation, etc
   (b) What would you like to change about the notification?
   (c) What else would you like to see in the notification or for the notification to do?
   (d) What would you like to happen when you interact with the notifications?
   (e) Where would you like to see the notification?
   (f) What about the notification would encourage you to install the mobile antivirus software on your smartphone?
   (g) What about the notification might discourage you from installing the application on your smartphone?

(h) What would make it easier to install the antivirus on your smartphone?

4. Which notification design did you prefer? Why?

5. Anything else you would like to add?

APPENDIX E: STUDY 3: PHASE 2 SCRIPT

Introduction:

"Hello, my name is [Your Name]."

If the participant hasn't filled out the consent form/prestudy survey: "I am seeing that you haven't filled out the consent form (and/or the pre-study survey) yet. You can find a link to the consent form in the same email that contained today's zoom link. Will you please take a few minutes to complete the consent form before we begin?"

Begin zoom recording: "This study is being recorded, so I am now going to begin the recording."

Introduction: In this study I will show you a prototype of a hypothetical antivirus software. This study has two parts. During this first part, you will be shown the prototype and asked to use it to complete a task. For the second part of the study, I will ask you a few questions about your experience and thoughts including feedback and suggestions on the design of the prototype and any security behaviors you might consider taking based on what you saw during phase 1.

Prototype A

[Shareable View Only URL]

Prototype B

[Shareable View Only URL]

Notification Walkthrough:

Group A: Shown Prototype without smartphone installation notification.

Group B: Shown Prototype with smartphone installation notification at the beginning.

"As previously mentioned, this is a prototype for hypothetical antivirus software. During this phase please click through the prototype and familiarize yourself with the application. As this is a prototype, not all of the screens and buttons are functional. If you have any questions, please let me know.

If struggling to figure out how to explore the prototype: To help guide you in exploring the prototype, why don't you try completing a task such as figuring out where to set up a virus scan.

End of walkthrough: "Thank you; that was the end of phase 1. I am now going to ask you some questions to get your feedback about your experience. For this portion of the study, you may refer to the prototype as needed when answering the questions.

Interview Questions

1. After seeing this prototype are you interested in or considering looking into installing antivirus software on your smartphone?
2. For the notification- show group A at this time- "This is a notification for encouraging potential customers to install the mobile version of the hypothetical antivirus software on their smartphone.
   (a) What do you like about the notification? Design, location, explanation, etc
   (b) What would you like to change about the notification?
   (c) What else would you like to see in the notification or for the notification to do?
   (d) What would you like to happen when you interact with the notifications?

(e) Where would you like to see the notification?

(f) What about the notification would encourage you to install the mobile antivirus software on your smartphone?

(g) What about the notification might discourage you from installing the application on your smartphone?

(h) What would make it easier to install the antivirus on your smartphone?

3. Is there anything else this antivirus software could do to encourage you to install the mobile version of the software on your smartphone? Why, why not?

4. What else might encourage/prompt you to install antivirus software on your smartphone? Why, why not?

5. What might discourage you from installing antivirus software on your smartphone?

6. Anything else you would like to add?