Modifying Smartphone User Locking Behavior

Dirk Van Bruggen*, Shu Liu*,
Mitch Kajzer†, Aaron Striegel*,
Charles R. Crowell†
* Department of Computer Science and Engineering
† Department of Psychology
University of Notre Dame
{dvanbrug,sliu6,mkajzer1,
striegel,ccrowell}@nd.edu

John D'Arcy
University of Delaware
Department of Accounting & MIS
jdarcy@udel.edu

ABSTRACT

With an increasing number of organizations allowing personal smart phones onto their networks, considerable security risk is introduced. The security risk is exacerbated by the tremendous heterogeneity of the personal mobile devices and their respective installed pool of applications. Furthermore, by virtue of the devices not being owned by the organization, the ability to authoritatively enforce organizational security polices is challenging. As a result, a critical part of organizational security is the ability to drive user security behavior through either on-device mechanisms or security awareness programs. In this paper, we establish a baseline for user security behavior from a population of over one hundred fifty smart phone users. We then systematically evaluate the ability to drive behavioral change via messaging centered on morality, deterrence, and incentives. Our findings suggest that appeals to morality are most effective over time, whereas deterrence produces the most immediate reaction. Additionally, our findings show that while a significant portion of users are securing their devices without prior intervention, it is difficult to influence change in those who do not.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and protection—*Authentication*

General Terms

Management, Security, Human Factors, Experimentation, Measurement

Keywords

Passwords, Mobile Devices, Awareness

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

1. INTRODUCTION

Cellular mobile devices have become an increasingly large part of society, permeating almost every aspect of life. Over the last decade, the number of mobile subscribers in the United States alone has more than doubled with 2011 seeing the number of mobile subscriptions surpass the number of people in the United States [1]. In addition to the growth in subscribers, the data usage of mobile devices is predicted to grow by over 16-fold in the next five years [2]. Moreover, not all of the cellular devices are simply phones anymore, with smart phones making up a significant portion of the market. Unfortunately, the expanding availability and usage of mobile devices brings an increased security risk.

From an organizational perspective, the increased risk is two-fold. First, with many users personally owning a variety of capable mobile devices, considerable pressure emerges from employees to have their organizations embrace BYOD (Bring Your Own Device) policies. Second, the perceived potential for productivity gains offered by capable mobile devices is appealing to the organization but tempered by the risks of exposing sensitive data. According to [3], 73% of companies now have a mix of company and employee owned mobile devices. However, only 48% had implemented security measures to protect mobile devices and 21% had no plans to implement such measures in the future.

Although specific case studies involving BYOD have demonstrated cost savings approaching nearly half of monthly service costs [4], an article in Technology Review cast significant doubts on the overall savings of BYOD [5]. According to the article, companies such as IBM are seeing potential savings in service costs by BYOD entirely eroded if not surpassed by related support costs. Central to those support costs is the issue of *risk mitigation*, namely, how can an organization ensure that various mobile apps or actions by the mobile employee are not exposing sensitive information? With a company-owned device, such policies can be strictly enforced [6]. Unfortunately, the diverse array of smart mobile devices and the resulting interplay arising from employee roles and privileges makes enforcement on BYOD decidedly non-trivial [7, 8].

Because of the complexity associated with employee-owned devices, a critical component for the acceptable execution of BYOD is user awareness of risk and security. To that end, we pose the question of whether the unobstructed security-related behavior of a smart phone user can be enhanced

through targeted interventions? Furthermore, if such behavior can be modified, what methods of interventions are most effective at achieving the desired change?

Over a period of five months, we conducted a two-part study of over one hundred fifty smart phone users to study their security habits. We start by measuring the baseline usage of secure practices on smart phones and continue by exploring the ability to drive change in the user security-related behavior through the use of a targeted intervention. After the initial five month study, passive monitoring of behavior continued for an additional seven months in order to observe any changes that occurred after the interventions. The key contributions of this paper are as follows:

- *We conducted one of the first studies to evaluate influencing change with regards to smart phone security behavior.* In particular, we focused on the usage of a screen lock which is an easily observable behavior with multiple degrees of security (no lock, pattern based, text based). Change was then prompted using a variety of messaging types (morality, deterrence, incentive) and compared to the performance of an untreated control group over a period of five months to capture both adoption of the recommended security practice and regression from it once adopted.

- *Initial baseline data showed that two-thirds of users secured their devices with a screen lock without prior interventions.* Contrary to expectations that users would be less likely to exhibit responsible behavior with regards to security, these numbers show promise for the baseline of security awareness in the studied sample of users. As the sample of users was taken from college freshmen, the findings may characterize a trend emerging as the next generation enters the workforce.

- *Interventions to promote awareness have only limited impact on user behavior causing less than one-third of unprotected users to change their security behavior.* Appeals to morality were most effective, but not significantly more effective than deterrence or incentive-based messaging. Additionally, users employing even a minimal baseline of security were slightly less likely to be persuaded to improve their security behavior than users with no security at all.

- *Peer effects may have a significant effect on the decision of a user to modify security behavior in response to a targeted intervention.* Peer effects have been demonstrated in prior work regarding health in social networks [9]. In our study, a user who responded positively to the intervention message was significantly more likely to have face to face contact with other users who also responded positively to the intervention message.

In short, our findings showed that while a significant portion of users were already securing their devices without prior intervention, influencing change in those who did not was difficult. Thus, at least in the case of smartphone security, we would argue that an organization is likely better off focusing on enforcement and detection rather than investing significant resources in ongoing awareness presuming an initial baseline of training[1].

The remainder of the paper is organized as follows. Next, we provide background information on smart phone security and the BYOD movement in Section 2. In Section 3, we introduce the data collection methods and summarize the demographics of the users in the study. We then evaluate the initial baseline security behavior of the users in the study in Section 4. The targeted interventions that were designed to influence change of security behavior are described in Section 5 along with the results of the targeted interventions. Finally, we conclude with a summary of the results and a discussion of possible future work.

2. MOBILE PHONE SECURITY

Significant research has been conducted into securing mobile devices [7, 8, 11–16]. One of the most common basic security approaches is screen locks, which enable a user to protect access to their device by automatically locking the device whenever the screen is turned off. Screen locks are similar to passwords used to log onto a computer and are based on methods that fit within the different usage patterns of mobile devices. Furthermore, given that password protecting computers to prevent unauthorized access to data and programs is important, keeping a mobile device secure is considerably more important. This is true especially because mobile devices frequently are a gateway to a wealth of sensitive data with numerous passwords and access methods pre-authorized by data already stored on the phone. With the number of lost phones eclipsing thirty million in the United States alone [17], the question becomes when, not if a mobile device will be lost, thereby putting the employing organization at risk.

Hence, an imperative emerges for organizations embracing the BYOD movement to secure or encourage security of employee devices. Naturally, a host of solutions have emerged related to the BYOD movement and organizational smart phone security includes approaches such as BizzTrust [8], Enterproid [18], Apperian [7], as well as entire suites of software offered from companies such as Samsung [19]. Such software is typically referred to as Mobile Device Management (MDM) software, a method employed by IT departments to monitor and manage mobile devices throughout an organization. These approaches can be divided into two categories: *full control* and *shared control*.

Full control approaches prescribe configurations for BYOD devices and then monitor usage to ensure that policies are in place and followed. Similar approaches have been used in traditional IT environments with software such as Cisco Clean Access [6] providing client software which is installed on end-user devices. The Clean Access software allows for complete policy enforcement across all devices at all times. With the advent of Android 2.2 (Froyo), the Android Device Administration API [20] was introduced which allows enterprise IT departments to develop branded "security-aware applications" which employees will install on their devices. These applications allow organizations to enforce policies on devices in much the same way as Clean Access.

Shared control approaches provided by companies such as BizzTrust and Enterproid take a dual personality approach

[1]By baseline of training, we refer to initial campus or employee orientation training upon starting at the organization [10].

which creates two separate virtualized environments on top of the standard operating system on a mobile device. This approach provides a secure workplace environment that can be administered by an IT department as well as a personal environment which allows a user full freedom to install and use any application or service they desire while preventing access or monitoring of personal activity by the workplace administrators. MDM software can still be utilized to control the workplace environments on all devices across the organization, while leaving personal environment management to the user.

As shown by [3,5], organizations spend a significant amount of time and effort trying to equip BYOD devices with the needed software to enforce policies. Due to this high expenditure, companies with a smaller IT budget may choose to forego such software solutions as a means of cost cutting. In the absence of these enforcement systems, the next rational course is to try using education-based approaches. Hence, it is critical to understand not only what typical security behavior can be expected from the next generation of mobile device users in the workplace, but also how effective educational approaches can be in promoting secure behavior.

Notably, mobile device security as it relates to BYOD encompasses a wide variety of aspects including screen locking, antivirus installation, permission awareness, software updates, etc [21, 22]. We focus in this paper on screen locks for two main reasons, namely ease of measurement and familiarity. By virtue of rooting the devices and our agent, we have a "perfect" ability to measure the intervention efficacy. Second, the practice of locking or protecting a device or account with a password is commonplace in modern IT environments. Although there is more to mobile device security than screen locks, we believed this practice was an interesting starting point for the present study and comment further on future work near the end of the paper.

3. DATA COLLECTION APPROACH

In order to study user behavior related to smart phone security, we worked in the context of an ongoing study at the University of Notre Dame involving two hundred incoming freshmen [23]. The study provided Android Nexus S smart phones for every participant with a free unlimited data, texting, and mobile-to-mobile minutes plan in exchange for complete monitoring privileges[2]. When students enrolled in the study, they were provided with a list of all types of data that would be monitored on their devices. The study targeted a random selection of participants with effort made to balance different demographic groups within the population.

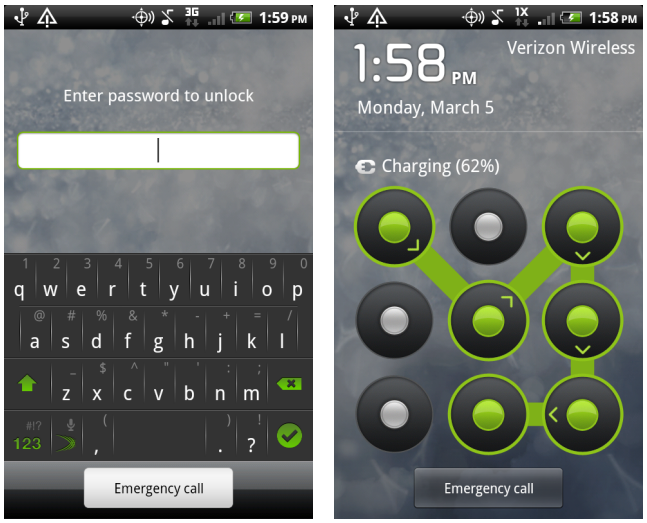
As we are studying a population of self-selected college-age participants, it is important to compare and contrast our sample with an enterprise BYOD population. First, both populations use mobile devices to keep track of personal and non-personal (e.g. school or work) data. A major difference between the two populations is the possible sensitivity of data access or data contents saved on the phone. Employees may be more concerned with protecting company data while students may not feel school-related data is sensitive and hence may view security mechanisms as irrational as posited by [24]. From a secondary comparison, both populations follow a regular schedule in which they attend either classes or work. The regular schedule results in reoccurring social peer interactions as well as the use of the mobile device in public locations. Finally, an important point to remember is that collecting detailed information from BYOD devices of all employees in an enterprise setting is much more difficult than in a university-based self-selection study. While there are some limitations that arise from the differences between our population and a typical enterprise audience, the data we collect from students about how individuals respond to security behavior interventions will likely have implications for the future work environment.

[2]Complete monitoring is defined as the state of the device (battery, network connectivity) and all instances of communication (where, when, who, length) but not actual message content. We note that all monitoring is approved by our institutional IRB.

3.1 Data Collection System

As part of the study, a data collection system was developed to run on each individual phone that consisted of two parts. First, a software application collected statistics on how the phone was being used (e.g. amount of data being used, number of text message) as well as the current phone state (e.g. using a screen lock, etc). Second, another software application presented the participants with short, multiple choice surveys on a weekly basis. For the purposes of the study, the surveys ranged in topic from week to week, including topics related to sociology, engineering, and psychology.

For our study, we focused on the Android operating system which provides two types of screen locks for users to choose from. The first method, which can be seen in Figure 1a, allowed users to employ a text-based password similar to that used on a standard computer. A related method presented the user with a numeric only keyboard, resulting in PIN-like passwords similar to ATMs. Standard, text-based passwords may have been difficult to use given the small screen and lack of physical keyboards on the mobile devices. The second method, seen in Figure 1b, allowed users to create patterns instead of text-based passwords. Android provides a pattern-based screen locking application that consists of a 3x3 grid of dots. The user then connects the dots



(a) Password (b) Pattern

Figure 1: Android Screen Locks

together in some easily remembered pattern. To unlock the phone, the user is presented with the 3x3 grid and is asked to re-enter the pattern before access was granted. The pattern-based methods may have been easier to input on the small screens of mobile devices and also easier to remember.

Both text-based and pattern-based lock codes are encrypted and saved in two separate files in a protected portion of the filesystem on the device. For the purposes of our study, the presence of the files was useful for determining what, if any, type of screen lock was being used. While there are multiple third-party screen locking applications, we decided to focus on the basic Android provided screen locks as participants in the study had access to the provided screen locks and they would not be required to install any additional software.

It is useful to consider the underlying mechanics of the security related aspects of the data collection agent. The data collection agent gathered both communication data, such as the sender and receiver of text messages and e-mails, as well as system data such as WiFi and 3G traffic usage. For the purposes of this paper, a separate thread was employed to collect screen locking data. In order to fetch the screen locking data, we accessed the files *password.key* and *gesture.key* under the `/data/system` folder. While these files contained the encrypted password and pattern, the presence of a given file and the associated file size was enough to determine what screen lock, if any, was being used.

The monitoring application started automatically when the phone was powered on and ran passively in the background on Samsung Nexus S 4G phones using Android OS version 2.3 (Gingerbread). The Android platform was selected for its customization capabilities through normal API or rooted / customized interfaces with respect to hardware-level interactions. The data records were kept in a local SQLite database on the phone and uploaded to a MySQL database on remote, secure servers by periodically utilizing public/private key encryption for secure backup and analysis. The default sensing granularity to check for updated locking data was one hour.

Both software applications were installed on the phones prior to the distribution to the participants in the study and started collecting data immediately. The users were allowed a period of four months to settle into usage patterns and habits before the screen locking study started monitoring and collecting any data. The initial settle time ensured that the participants developed a consistent security behavior as well as a habit of answering weekly surveys through the software interface. Thus, the added monitoring and surveys that were sent out as part of the study should not have seemed different and therefore should not have caused any adverse reaction by users to our methods.

Additionally, when the phones were distributed, the study participants were also asked to fill out a long-form demographic survey. The survey covered general demographic information as well as information related to prior education, personality, emotional state as well as cultural and political viewpoints.

3.2 Study Participants

The initial user population consisted of 197 participants, 195 of whom completed a demographic survey. Of the original sample, 104 (53.3%) were males and 91 (46.7%) were females, which is similar to the university admission statistics (53.8% males, 46.2% females). In addition to core demographics such as gender, historical data with regards to prior mobile device usage (prior phones) also was collected with 135 (69%) participants having previously used a feature phone and 60 (30%) users having used a smart phone[3]. Out of the 60 prior smart phone users, Android was the most popular device with 25 users (42%), followed by the iPhone with 17 users (28%). Table 1 describes the distribution of intended majors amongst the group of participants with the heaviest concentration in Engineering followed by the Sciences and Business.

Major	Number of Students		Campus Distribution	
Arts and Humanities	39	20%	3823	44%
Business	44	22%	1877	22%
Engineering	51	26%	977	11%
Sciences	49	25%	1917	22%
Undecided	14	7%	NA	NA

Table 1: Distribution of Intended College Major[4]

Usage Type		Avg	Std. Dev	Max
Received Traffic	(MB)	140	212	2261
Sent Traffic	(MB)	24	20	157
Text Messages	(Number)	402	385	2731
Screen On Time	(Minutes)	541	262	1520
Phone Calls	(Number)	26	33	254

Table 2: Table of Average Usage Per Week

The study pool was further refined down to 149 users in order to eliminate any who were not using their phone significantly or had broken their devices and had significant repair times. Filtering was based on whether or not the software agent had reported any usage data back during the first two weeks of the study. The resulting gender distribution stayed similar with 54% males and 46% females. Similarly, the ratio of previous users of smart phones stayed similar as well with 30% smart phone users and 70% feature phone users.

With regards to actual phone usage once receiving the smart phones, the study population behavior is shown in Table 2. For instance, a typical study participant across the 17 week analysis period (January through April 2012), sent and received roughly 140 MB of traffic (3G + WiFi) per week, sent and received 402 text messages per week, made 26 phone calls per week, and used the screen for 541 minutes per week.

4. INITIAL DATA

In order to establish awareness, the first critical step was to assess the security profile and perceptions of the study participants. To that end, we explored the baseline usage of the built-in Android screen locking features. Two weeks of data were collected with regards to locking in January 2012 (first two weeks of the spring semester). The gathering of the data served two critical purposes. First, it provided a contrast between what a user perceived and how a user

[3]Two students did not report previous phone usage

[4]The distribution of majors represents the intended major of the participant at the start of freshman year. Typical with most science and engineering majors, enrollment generally shifts downward after beginning the curriculum.

Type of Lock	Number of users	95 % CI
No Lock	53 35%	28% to 44%
Pattern Lock	76 51%	42% to 59%
Text Lock	21 14%	9% to 21%

Table 3: Baseline Screen Lock Usage During Week 2

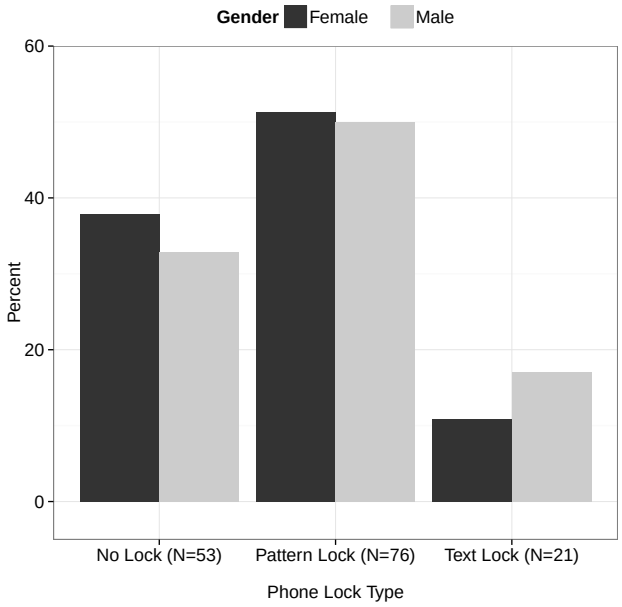


Figure 2: Percent of Gender Using Each Screen Lock

behaved. Second, the study served as a reference to any subsequent studies.

Table 3 shows the initial results from the data collection. Most notably, 65% of the students were using some type of a screen lock, which is a much higher percentage than would be expected based on previous reports of auto-lock feature use (25% of smartphone users [14]). This discrepancy may be attributed to the differences between the two populations (older vs. younger). The survey study in [14] examined a diverse workforce while our study consisted of freshman-age students who have grown up in an increasingly digital world. The younger students may be more familiar with concerns of digital privacy and therefore may have been more likely to lock the smartphones. Additionally, all of the students lived in dorms on campus which may have resulted in more concern about privacy due to unfamiliar roommates. However, data from the study shows that when the students left campus for the summer, there was no significant change in the distribution of locking behaviors. Arguably, the baseline levels of screen locking noted in our study may be more indicative of the behavior of the future workforce population.

The largest percentage of those students already utilizing security were using a pattern-based screen lock, with 51% of the total user population employing this security measure. Conversely, the remaining 14% were using a text-based password, that being either the PIN or Password screen locks. This is a significant finding, showing that a majority of users, which may be representative of a university population, will use a screen lock on their mobile device without any direct

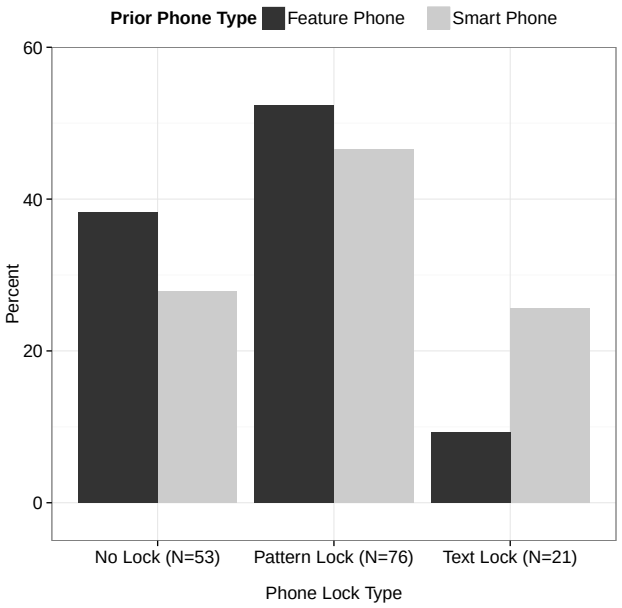


Figure 3: Screen Lock vs. Previous Type of Phone

interventions being performed.

A natural question here is how user demographics related to the likelihood of using a lock. First, the data can be analyzed with regards to different demographic characteristics that were obtained from the study participants before the start of data collection. For instance, Figure 2 presents the screen lock data with respect to gender where the percent denotes the proportion of each gender employing a particular approach. The differences in initial behavior were not statistically significant between genders (Fisher's Exact).

Beyond gender, another piece of information that was collected from participants was the type of phone used before switching to the study-provided device. The phones were classified as either a smart phone or a feature phone. Figure 3 looks at the previous phone a participant had before joining the study with respect to their locking behavior. There is no statistically significant difference (Fisher's Exact) in screen locking between the participants who had previously used smartphones and those who had not.

Alternatively, a second way to examine screen locking behavior is based on comparing individual usage patterns. As noted earlier, the data collection agent tracked the various characteristics of usage (text messages, screen time, etc.). Figure 4 shows screen lock usage categorized by text message (SMS) usage (inbound and outbound). Each grouping in Figure 4 represents one of the four quartiles of SMS usage (i.e the first grouping represents the first quartile with the least text message usage). Quartile assignment was based on the average weekly SMS usage measured over the duration of the intervention study. There was no statistically significant difference found between the behavior of participants in the different quartiles (Fisher's Exact) or when using a logistic regression on the weekly average SMS usage and initial locking behavior.

Similarly, network traffic is another measure of the usage levels of a given device which might be related to screen-

Lock Type	Screen Usage (Minutes)		Tx Traffic (MB)		Rx Traffic (MB)		SMS	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev	Mean	Std. Dev
No Lock	571	290	23.82	17.77	170.66	202.66	378	352
Pattern Lock	534	233	26.06	23.93	156.26	275.37	412	348
Text Lock	611	365	20.27	19.19	89.61	97.66	419	438

Table 4: Average Usage Per Week Categorized By Screen Lock Type

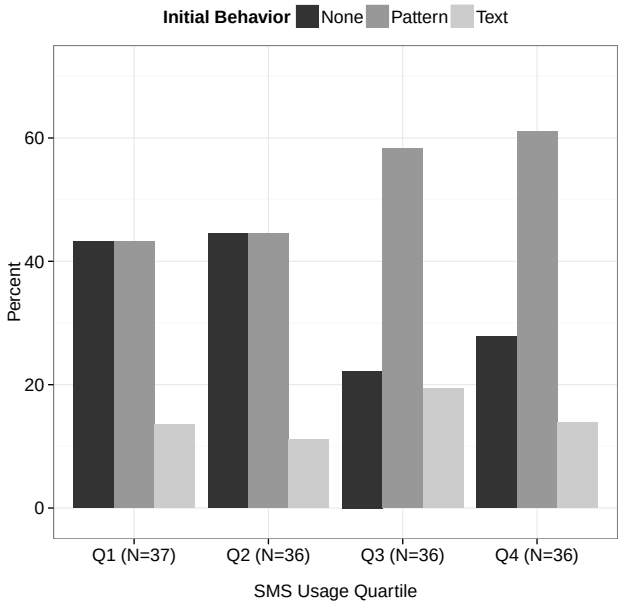


Figure 4: Screen Lock Choice Categorized By SMS Usage

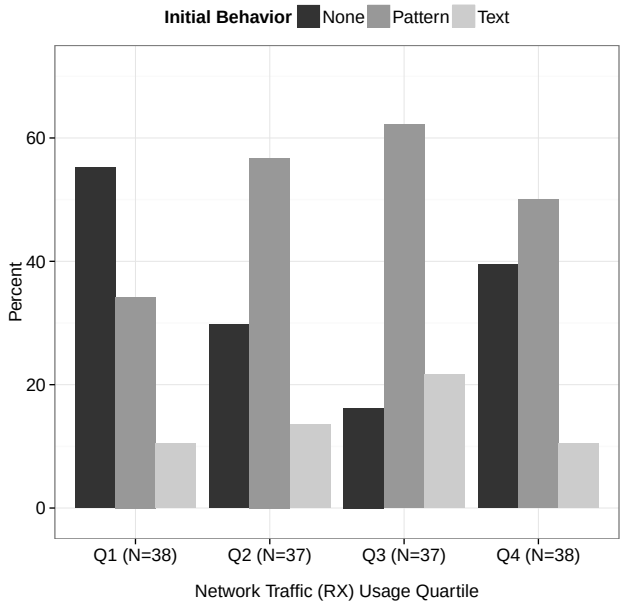


Figure 5: Screen Lock Choice Categorized By Rx (Downstream) Traffic Usage

locking behavior. Figure 5 shows the quartile grouping of the Rx, or downloaded, network traffic in much the same way as the SMS data was displayed. Similar to Figure 4, none of the groups describing screen locking follow a pattern as data usage increases. The lack of a pattern in this instance is most likely due to the high variability of network traffic usage from week to week for which the quartile slicing could not counterbalance.

Examining intended area of study, the distribution was very similar to the overall distribution of screen lock usage. The *no lock* usage ranged from 32% to 40%, *pattern-based lock* usage ranged from 48% to 56% and *text-based lock* usage ranged from 9% to 19% usage. Differences in initial behavior when compared to intended area of study were not statistically significant.

Personality data which was collected through the initial demographic survey mentioned in Section 3.1 was based on the "Big Five" personality traits: Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness [25]. Each of the sets of questions were scored for each participant and a logistic regression was used to analyze the relationship with initial screen locking behavior. None of the personality traits was a significant predictor of initial locking behavior. As will be shown later, there exists a small impact of agreeableness on the success of the intervention.

Data was also collected which describes social interaction between users within the study. Social interaction can occur in multiple ways including digital communication (e-mail, text messaging) as well as in person contact (proximity). To measure these occurrences, the study used Bluetooth signals to identify when two users in the study were within a limited distance of one another (< 5m) [26]. This information allowed for the creation of a social graph which assisted in exploring the initial locking behavior exhibited by the study participants.

Although *friendship* is an extremely difficult metric to quantify, the notion of face-to-face interactions (gathered as noted earlier via Bluetooth) can allow some inference. We informally capture friendship strength for 147 participants and characterize based on the strength and consistency of being in proximity of one another [27]. Two participants were missing proximity data, thus we do not capture all 149 individuals. Although we are limited to measuring proximity of intra-study interactions, we get a glimpse of the strongest "friends" within the study to gauge if any proximity effects might exist.

Table 5 explores the similarity of locking behavior between users and their strongest friend. For each participant, we obtain their strongest intra-study friend and compare the locking behavior between both participants. As shown in the table, of the 97 participants who lock their device, 68 of them have the same behavior as their strongest friend while 29 of them have different behavior.

My Behavior	Friend Behavior	
	Friend Locks	Friend Does Not Lock
Lock (N=97)	68	29
Do Not Lock (N=52)	44	8

Table 5: Friendship vs. Initial Locking Behavior

It is important to note that friendship strength is not a symmetric relationship. For example, consider three people: Alice, Bob and Charlie. Alice's strongest friend is Bob and Bob's strongest friend is Charlie. Both Bob and Charlie lock their phones. Thus, Bob's friendship with Charlie would be counted as part of the 68 friendships where both people lock. Alternatively, Alice's friendship with Bob would be counted as part of the 44 cases where the strongest friend locks and the participant does not lock. There was no statistically significant difference in initial behavior when considering *only* the strongest friendship. However, as discussed later, friendship may play a role in other behaviors.

4.1 Awareness Survey

The next natural question to ask is how perceptive are users of their own security profile. Similarly, does asking about their profile impact behavior and are there other interesting behaviors that may merit additional attention? Based on the initial data collected, two surveys were designed and sent to participants through the survey application that was installed on the devices. There were two main goals for the surveys: assessing the current awareness of security topics of the study participants and also to raise awareness of the presence of screen locks on the mobile devices.

Separate security lock awareness and password sharing surveys were developed and deployed to all two hundred participants in the study. Participants were given two weeks between each of the surveys, although some did not complete the first survey before the second survey was sent out. After the second survey, another three weeks were given as an observation period before any further communication occurred. The questions of each survey are detailed in Table 6. Both surveys were sent to all study participants, however the awareness and sharing surveys received 158 and 131 responses respectively.

The first awareness survey asked users about their usage of screen locks on the mobile devices and served two main purposes. First, the survey created or raised user awareness about the availability of screen locks on their mobile devices which helped to ensure that if users were not utilizing screen locks that the decision was by choice rather than by ignorance of the presence of this feature. Second, by directly asking users about their usage of screen locks, reactivity to the "observation effect" is reduced [28]. That is, by first having the participants self report their screen lock usage before they are exposed to a targeted intervention, any change during the intervention itself should less likely be due merely to a reaction to their suspicion that locking behavior is being monitored by the installed agent [29, 30].

To that end, the self-reported and the collected distributions are compared in Table 7. As expected, the self reported data was closely related to the true baseline data that was collected for the devices. In checking responses against the collected data, it was found that only 7.5% of respondents

Type	Self Reported	Collected
Use No Lock	33%	35%
Use a Pattern	54%	51%
Use a Password	13%	14%

Table 7: Self Reported vs. Collected Usage of Screen Locks

incorrectly indicated which type of screen lock they were using with the use of a pattern being the most common incorrectly answered choice. These incorrect responses most likely were due to the wording of the question, providing "Gesture Based Lock" as an option which could also fit the default "Swipe to Unlock" screen lock. For the participants who indicated they did not use a screen lock, 9% indicated the reason was due to the difficulty of input methods for screen locks. While 19% did not indicate a specific reason for not using screen locks, a likely possibility is that the participants did not see the benefit of using a screen lock on their device.

4.2 Password Sharing Survey

Although screen locks offer a baseline for security, locking will not be effective if the pattern or password is shared. A recent article discussed the rising tendencies of teenagers to share their passwords with close friends and significant others [31]. The news story was used as a motivation for the topic of the second survey which tried to assess such tendencies within the study population. The goal was to measure opinions among the population about this practice as well as to continue to raise awareness about screen locks and passwords on the mobile devices. Questions from the survey asked participants about their password sharing behavior as well as if the participants changed their password after sharing it with people. The survey attempted to assess how common password sharing was on the mobile device as well as how common password sharing was, in general.

Of the 131 responses received, only 25 (19%) shared the password for their phone while 83 (63%) shared one of their passwords for some other device or service. This finding is interesting in that users appear to value the security of their mobile devices more than that of some other devices / services. It is possible that while a person may share the password to their e-mail account with someone, granting full access to their mobile device is not often necessary. The majority of those who shared their mobile device password (10%) indicated that they did so during a time period (1-2 Months) coinciding with a semester break during which all students were off campus. Friends were the most common recipients of shared passwords, accounting for 16% of all sharing activity. Given that 63% of the population shared one of their passwords, the majority of this group limited their sharing activity to fewer than five people with only one person indicating they had shared with more than five people.

5. INTERVENTION STUDY

While it was interesting to find that 65% of the users locked their phones, there still remained 35% who did not employ a screen lock even after two subtle surveys that encouraged screen lock usage. To that end, the users without a screen lock provided a test case to see if explicit interventions, such as is typical in security awareness campaigns,

Survey	Question	n	Answers	Responses	
Self Awareness	Currently use a screen lock	158	Yes, Pattern	86	54%
			Yes, Password or PIN	20	13%
			No	52	33%
Self Awareness	Why do you not use a screen lock	158	To hard to remember	1	1%
			To hard to enter on a phone	15	9%
			Not sure how to setup	6	4%
			Other	30	19%
			NA	106	67%
Password Sharing	Have you shared your phone password	131	Yes	25	19%
			No	83	63%
			NA	23	18%
Password Sharing	How recently have you shared your phone password	131	0-2 Weeks	7	5%
			1-2 Months	13	10%
			3+ Months	5	4%
			NA	106	81%
Password Sharing	Who did you share your phone password with	131	A Friend	21	16%
			A Parent or Relative	2	2%
			Other	2	2%
			NA	106	81%
Password Sharing	How many people have you shared your phone password with	131	0	38	29%
			1	10	8%
			2-5	17	13%
			More than 5	1	1%
			NA	65	50%
Password Sharing	Do you share any other passwords	131	Yes	83	63%
			No	48	37%
Password Sharing	Do you change your password if you need to share it	131	Yes	26	20%
			No	105	80%

Table 6: Surveys sent to students

could increase screen-locking behavior among these users.

Hence, two subgroups of the population were targeted for intervention. The first group consisted of users who were not using either of the screen locks described in Section 3. Any user who did not have a screen lock present during Week 7 of the study was considered eligible for this intervention group (N = 48).

The second group consisted of users who were employing only pattern-based screen locks. The second group of users was chosen due to recent work showing that pattern-based screen locks may be more susceptible to attack than text-based alternatives [32, 33]. The users of the second group were chosen based on their usage of a pattern-based screen lock during Week 7 (N = 72).

To design the intervention, we relied on previous work that had evaluated different methods of persuading users to change their security behavior [34–39]. Based on this prior work, three message types were devised to send to each group. These types were based on the principles of *deterrence*, *morality*, and *incentives*. While we considered using feedback messages based on the work by Cialdini [40], we decided to limit our study to only three types of messages so as not to further reduce groups size and statistical power. Our future studies will make use of messages based on feedback which is discussed at the end of the paper. Both the pattern-lock and no lock groups of participants were divided into four subgroups each, one for each type of intervention approach and a control group.

Given that the study was focused on mobile phone usage, intervention messages were designed to be sent as text messages to the same devices from which the data was being collected from. Due to the 160 character limit of text messages, each intervention message was created in two parts to fit into two separate text messages that would be sent, one after another, to each of the participants in each of the groups.

Intervention messages were sent to the participants of each of the test groups and were followed up by reminder messages at one week intervals to anyone who did not modify their behavior. Hence, a user who elected not to change their behavior would have received a total of five messages. After the four reminders were complete, an additional five weeks were left for observation to see if any further changes would occur including regression. Subsequent monitoring was also done at periods of one month to observe long term behavior. Each of the intervention message types are explained in more detail below followed by the results of the intervention study.

5.1 Intervention Message Types

Intervention messages were carefully designed based on incentives [34, 41], morality [42, 43] and deterrence [44, 45]. We describe each message type and discuss the key considerations involved in the design process [5]. The incentive messages were created based on specific reward scenarios (e.g., something good will happen to you) for taking action and are based on Incentive Centered Design (ICD). ICD focuses on providing incentives in order to influence the decisions

[5]Exact wording of all messages is included in Appendix A.

people make [34]. Research related to incentive messages has had varied results. Studies such as [46–48] found incentive messages to be effective in promoting safe security behaviors. However, researchers in [49] found that incentive messages did not significantly increase security compliance amongst users.

As described in [41], a common incentive is providing financial gain like cash for correct decisions. Thus, for our study the message contained: "As a way to encourage security, we are giving away a free $10 Amazon Gift Card. You can be entered into our drawing by simply adding a password to your phone. Visit this link for more information."

The deterrence-based intervention message focused on the possible consequences to self for not following organizational practices. Siponen et. al indicate that deterrence messages are the most common type of message in both security awareness and the literature [44]. General Deterrence Theory [45] makes use of penalties to deter an individual from committing an act. As indicated in [50], there has also been contradictory results with regards to the success of deterrence-based messages to influence user behavior. Studies such as [51,52] resulted in a positive influence on safe security behavior by users. Conversely, researchers in [53–55] found no influence of deterrent messages. Our deterrent-based message read "If you misplace your phone and you don't have a password, the finder may have access to sensitive info about you or fellow students. This may put you in violation of the [institution] policy on sensitive info! Visit this link for more information."

Finally, morality-based messages focused on an organizational mandate and doing the right thing in relation to it. Moral theory extends deterrence theory and suggests that individuals will use personal moral principles and values when making decisions [56, 57]. Siponen has found that moral reasoning is effective in explaining adherence with security policies [58]. Research has also shown that moral reasoning has an effect on behavior by affecting decisions regarding policy violations [43, 59, 60]. Our morality-based message was "the [institution] believes that all information on digital devices should be secure. The right thing to do is to add a password to your phone so as to comply with this requirement. Visit this link for more information."

In designing these messages we took three precautions to conform to the ethical standards for human subject research as prescribed by our Institutional Review Board (IRB). First, to ensure the accuracy and plausibility of our messages we consulted with administrators from across campus including the Offices of Information Technology and General Counsel to insure that all were consistent with published institutional security guidelines encompassing faculty, staff, and students [61]. Second, to minimize deception for the deterrence message, we included the less certain phrase "may put you in violation," and did not specify a punitive consequence, which likely reduced the effectiveness of our deterrence-based campaign as noted above. Third, the study research protocol including the text of all messages was submitted to our IRB for independent review and approval.

5.2 More Information Website

All of the intervention messages contained a *bit.ly* link to a webpage that described how to setup both a pattern-based and a text-based screen lock. Each of the different groups received a different *bit.ly* link that allows us to track how many

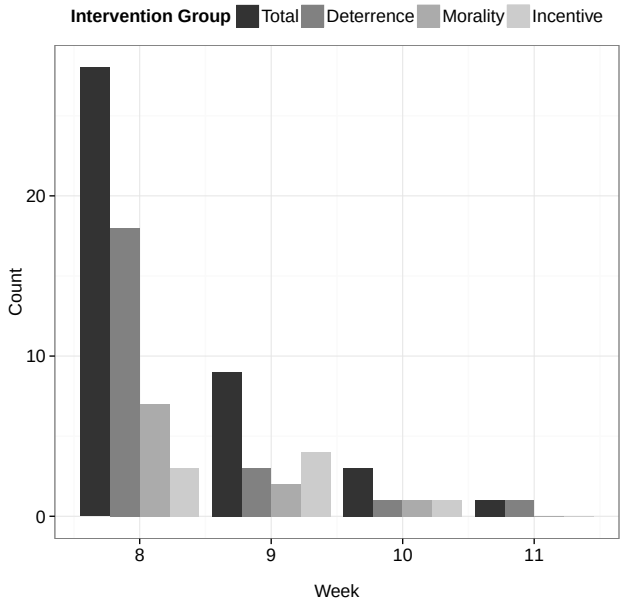


Figure 6: Click Throughs vs. Time

times the web page was visited from each of the intervention groups. This provided some indication if users wanted more information after receiving the text messages or if the users based their behavior solely on their own knowledge. Figure 6 shows how long it took users to click through to the more information website. Of the 92 users who received the intervention messages, only 41 users clicked through to the more information website. The reminders were sent on days 9, 16, 24 and 37. The level of interest in additional information diminished over time with the last two reminders only attracting a single user each to click through.

Figure 6 presents the click through data by the message type that the user received. Deterrence brought about the largest group of click throughs as well as the quickest response with the majority of click throughs occurring during the first day the intervention was sent out. A chi-squared test on Week 8 shows there is a significant difference between the click-through response of the different message types (χ^2: 12.929; $p < .05$). However, there are no significant differences for the following weeks. Such a large and quick response indicates that deterrence quickly motivates users to explore the idea further, although as described below, such exposure to security related information may not necessarily correlate with the users modifying their behavior.

5.3 Results

Changing behavior was not instantaneous but instead occurred across a large period of time during the study. Table 8 summarizes the usage of each of the types of screen locks throughout the study. Rows in the table were picked to represent milestones during the study with Week 1 being the start of the study, Weeks 3 and 5 were when the surveys were sent out, Week 7 was the week after the second survey was sent out, Week 8 was the week the intervention started, 13 marked the last reminder being sent out and Week 17

Week		No Lock	Pattern Based	Text Based
1		35.2 %	52.4 %	12.4 %
3	S	37.0 %	51.3 %	11.6 %
5	S	35.5 %	51.6 %	12.7 %
7		39.4 %	48.3 %	12.2 %
8	I	37.5 %	46.5 %	15.9 %
13		31.2 %	49.6 %	19.0 %
17		33.0 %	47.3 %	19.5 %

Table 8: Summary of Usage Over Time (S denotes the occurrence of a survey and I denotes the start of the Intervention)

Gender	Changed		Did Not Change
	Stayed	Regressed	
Female (N=60)	13	6	41
Male (N=60)	6	3	51

Table 9: Gender vs. Behavior Change As Observed During Intervention Study and 7 Month Follow Up

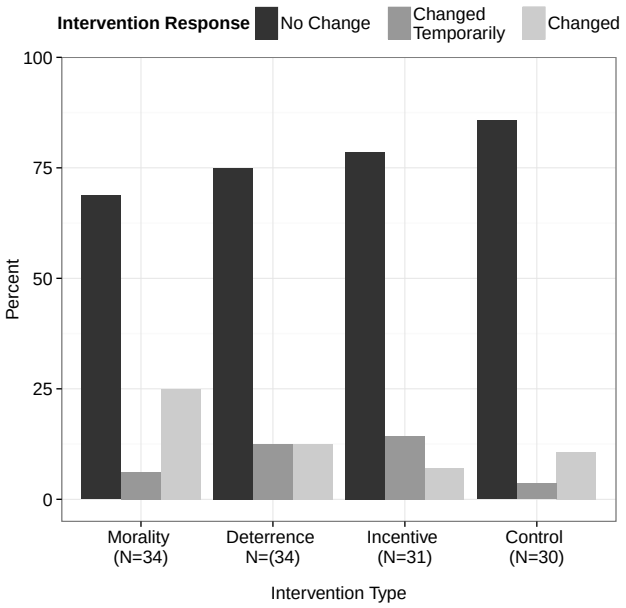


Figure 7: Overall Change Categorized by Intervention Group and Maintained vs. Regressed Behavior Over Intervention (Study and 7 Month Follow Up)

was the end of the study.

As would be expected if our interventions were effective, the usage of both gestures and text-based passwords increased after Week 8, while the size of the group using no screen lock decreased. Unfortunately, from Week 13 to Week 17, the size of the group using no screen lock increased, indicating that users started moving back to their old habits. However, usage of text-based screen locks increased as well, indicating that users were still changing their behavior.

In exploring demographics of the population in regards to changing, the only relationship that stood out was gender as shown in Table 9. Females were much more likely to modify their behavior than males. This result was confirmed statistically via a logistic regression in which gender and intervention group type were used to predict whether or not the participant changed their behavior. Gender was the only significant predictor ($p < .05$) with a beta coefficient of 0.977 which indicates that females were 165% more likely to change behavior in response to the interventions than males. Both genders showed a similar level of reversion with about half of all participants regressing back to their initial behavior before the intervention at some point during the seven month follow-up study.

An interesting comparison to consider is that between the users who changed their behavior and maintained it versus those who changed their behavior and regressed back to their previous screen locking method. Figure 7 outlines the number of participants in each intervention group who did not change, changed temporarily and changed without regressing back (i.e. those users who did not go back to poor security practices). Regression was monitored for eight months after the initial intervention message was distributed. Morality was the best intervention technique with 31% of users who received the message changing and 25% retaining better security practices. The next best method was the deterrence-based method which had 21% of users who changing and 14% of users staying with the adopted security practice. Incentive-based messaging resulted in the lowest percentage of users staying with better security behavior at 7%.

Another way to look at the data is to consider the initial behavior of users, that is, what type of screen lock they were previously using before targeted for intervention. Figure 8 outlines the change of behavior split across both intervention methods and previous behavior. The difference between users who had used a screen lock prior to the intervention study and those who had not was not statistically significant.

Usage data can also be used to explore the response to the intervention messages. A logistic regression was performed in which Rx traffic usage predicted whether or not a user who changed in response to the intervention would go back to the previous behavior. The Rx traffic beta coefficient was significant ($p < .05$) when it was analyzed by itself but when intervention group was included as a predictor variable to control for any effects from intervention groups, the Rx traffic coefficient was only marginally significant ($p = .06$). In the regression with both Rx traffic and intervention group predictors included the Rx traffic coefficient of $-1.483 * e^{-2}$ indicated that as Rx traffic usage increased by 1 MB, users were 2% less likely to change their behavior.

Alternatively, personality metrics can be used to analyze the data and search for any relationships. Figure 9 shows the average personality scores compared for two groups: participants who changed their behavior in response to intervention messages (includes all message types) and those who did not change their behavior. A logistic regression in which all five personality scores were used as predictors of whether or not users changed their behavior was performed both with and without controlling for the effects of intervention groups. The regression that did not control for effects of intervention group resulted in an agreeableness beta coefficient which was significant ($p < .05$). However, when controlling for intervention group, the agreeableness coefficient with a value of 1.122 was only marginally significant ($p = .06$). A 1 point in-

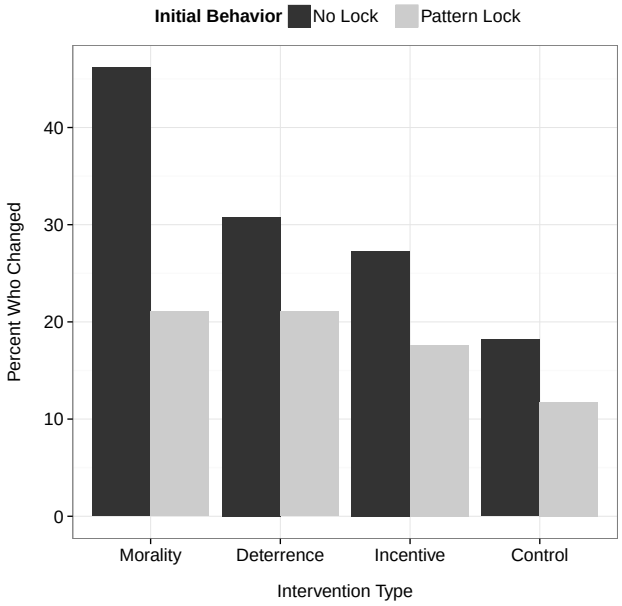


Figure 8: Overall Change as Categorized by Prior Security Behavior

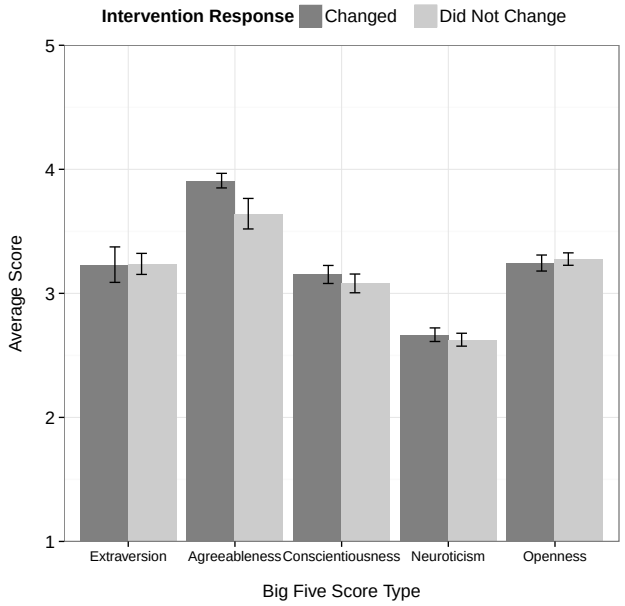


Figure 9: Average Personality Scores as Categorized by Response to Intervention (All message groups included)

My Behavior	**Friend Behavior**	
	Friend Changed	Friend Did Not Change
Changed (N=28)	15	13
Did Not Change (N = 92)	9	83

Table 10: Friendship vs. Intervention Response

crease in agreeableness scores resulted in users being 206% more likely to change locking behavior in response to an intervention message. This finding indicates a correlation between agreeableness scores and the likelihood of an individual of responding positively to an intervention message.

By utilizing the friendship data discussed earlier in Section 4, behavior in response to the intervention can be compared in regards to friendship as well. Table 10 explores the similarity of intervention response between users and their strongest "friend". Unlike Table 5, an interesting pattern is present in this data. Participants in the study who changed their behavior in response to an intervention message were more likely to have similar behavior as their strongest friend than those participants who did not change their behavior ($p < .001$, CI: $(3.453, 33.181)$, Fisher's exact test). Although friendship alone may not be enough to influence locking behavior, friendship combined with an intervention may be enough to encourage change. This outcome might reflect the operation of *peer conformity* as described by [9].

Figure 10 depicts the changes that occurred in behavior over the seventeen weeks during the study. Week 8 was the start of the targeted interventions which saw a sharp increase in the number of changes. Four reminders were sent on a weekly basis, showing a larger percent of changes for the first two reminders and then the changes taper off again. The likelihood of users who employ a pattern-based screen lock to change was slightly lower than that of users with no screen lock. However, this difference was not statistically significant.

Figure 11 shows the changes over time separated by the message type that was sent to each group as well as the control group. As previously noted, the intervention was sent out on Week 8, with reminders following on Weeks 9, 10, 11 and 13. Morality had both the largest percentage of change as well as the largest response on the first day of the study. Both deterrence and incentive methods had a larger response around the second reminder that was sent out. This differs from the data presented in Figure 6 which showed initial interest in more information. The discrepancy may suggest that while deterrence works quickly to generate interest in a message, morality works quicker to change behavior.

While these results are promising, a few caveats should be addressed. First, the study population consisted of incoming freshman level students, which represents a young population compared to a standard population concerning a standard organization. Although the population is young, the data presented in the paper can be a predictive data set for the upcoming average population in any given group. Secondly, the institution at which our study was deployed has a strong religious basis and therefore the population may have a stronger response to messages based in morality. While there may be a slight bias towards morality-based messages, the finding that morality had the strongest response is still a useful finding as it aligns with previous work [34–39] indicating morality and intrinsic values as the best motivators across multiple areas of influence.

6. SUMMARY AND FUTURE WORK

In summary, the issue of BYOD for the workplace is not an issue that is likely to disappear in the near future. Although our findings point to the rising workforce as being more conscientious of security by virtue of locking their phone

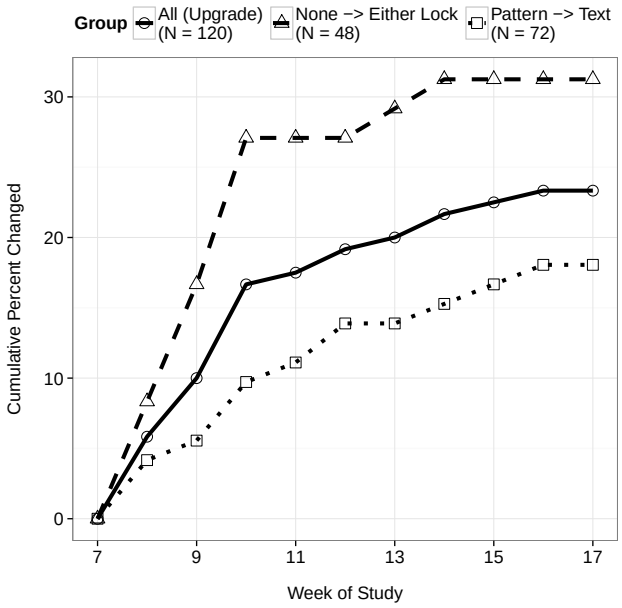


Figure 10: Cumulative Security Changes Over Time

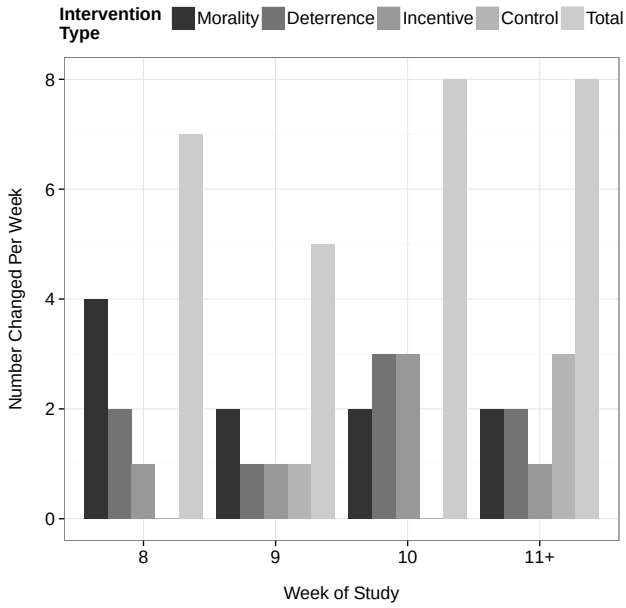


Figure 11: Frequency of Change Over Time Categorized by Intervention Group

more than the baseline population, the fact that nearly one third of our user population did not lock their phone was still worrisome from a security perspective. The most critical finding of the work was that whether encouraging even minimal security enhancement (no screen lock to pattern-based lock) or to employ a more secure form of locking (pattern-based to password-based), interventions across the three themes (morality, deterrence, and incentives) changed only one-third of the user security behavior.

While we are unable to make the claim that targeted interventions are ineffective, the presented data may indicate that targeted interventions do not provide a sufficient return on investment when dealing with *risk mitigation*. That is, the cost associated with targeting and implementing the interventions may not be worth the expenditure when such a return is observed. The net takeaway from our work is that, with regards to smartphone security, enforcement and detection are key and that resources expended towards continued security training beyond the baseline are unlikely to be effective allocations of organizational resources.

As mentioned earlier, the study on phone locking was an initial look into the behavior of our study pool. Since security encompasses multiple behaviors on mobile devices, we plan to examine additional behaviors such as the use of antivirus software. Future studies will encompass lessons we have learned from the screen locking study and will also focus on alternative message types and communication methods.

It may be useful to examine how much risk participants perceive by not using a password. When examining security behavior, it is important to take into account the tradeoffs that users make when considering different behaviors. In the case of this study, adding a screen lock may add one to two seconds of delay each time a user pulls out their device. If the perceived level of risk is low and the added time perceived to be a large inconvenience, users may be less likely to change their behavior. To further examine the tradeoffs that users make, we hope to perform a follow-up survey based on [62] which examines users perceptions of risk and privacy associated with mobile devices.

Finally, we believe that the present study opens a wide variety of questions for future work regarding the factors affecting smartphone security behavior. First, the finding that friendship strength was related to the response of a user towards a targeted intervention but not the initial security behavior warrants further exploration. Does this relationship hold for more complex security behaviors such as antivirus use, permission checking of applications or privacy concerns? Is the pressure to conform to good security hygiene weaker than the pressure to conform to recommendations passed down by authority? Are there stronger metrics of friendship that result in a stronger correlation with security behavior? Lastly, future research can explore various questions with regards to data exposure risks (use of applications like Dropbox, Siri, etc.) and user comprehension of said data exposure risks.

7. ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation by grant IIS-0915775.

8. REFERENCES

[1] CTIA. U.S. Wireless Quick Facts, 2012.
[2] Cisco. Cisco VNI Mobile Data Traffic Forecast 2012-2017. Feburary 2013.
[3] Webroot. SURVEY: Mobile Threats are Real and Costly, 2012.
[4] Enterproid. Implementing Your BYOD Mobility Strategy. 2012.
[5] B. Bergstein. IBM Faces the Perils of "Bring Your Own Device" - Technology Review, 2012.

[6] Cisco. Cisco NAC Appliance (Clean Access), 2012.

[7] Apperian. Solving Android Multiple Personality Disorder: No Drugs Required. 2011.

[8] Fraunhofer. BizzTrust, 2012.

[9] J. H. Fowler and N. A. Christakis. Estimating peer effects on health in social networks, 2008.

[10] P. Puhakainen and M. Siponen. Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4):757–778, December 2010.

[11] iGillottResearch. Securing Mobile Devices on Converged Networks. 2006.

[12] J. D'Arcy and A Hovav. Does one size fit all? examining the differential effects of is security countermeasures. *Journal of Business Ethics*, 89:59–71, 2009.

[13] P. Dunphy, A. P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, page 1, 2010.

[14] S. Cobb. Sizing Up the BYOD Security Challenge. 2012.

[15] P. J. Connolly. iPad, iPhone Challenge Management Orthodoxy, 2012.

[16] C.L. Anderson and R. Agarwal. Practicing Safe Computing: A MultiMethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3):613–643, 2010.

[17] R. Jaroslovsky. Help for Lost Cell Phones, 2012.

[18] Enterproid. The Divide^{TM}platform enables BYOD mobility, 2012.

[19] Samsung. Mobile Device Management, 2013.

[20] Android. Device Administration API, 2012.

[21] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 96–111. IEEE, 2011.

[22] AP Felt, K. Greenwood, and D. Wagner. The effectiveness of application permissions. In *Proceedings of the 2nd USENIX conference on Web application development*, pages 7–7. USENIX Association, 2011.

[23] S. Liu and A. Striegel. Casting doubts on the viability of wifi offloading. In *Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design*, CellNet '12, pages 25–30, New York, NY, USA, 2012. ACM.

[24] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144. ACM, 2009.

[25] P. T. Costa and R. R. McCrae. Professional manual: revised neo personality inventory (neo-pi-r) and neo five-factor inventory (neo-ffi). *Odessa, FL: Psychological Assessment Resources*, 1992.

[26] S Liu and A. Striegel. Accurate extraction of face-to-face proximity using smartphones and bluetooth. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pages 1–5, 2011.

[27] N. Eagle and AS Pentland. Reality mining: sensing complex social systems. *Personal Ubiquitous Comput.*, 10(4):255–268, March 2006.

[28] F. C. Harris. Subject reactivity in direct observational assessment: A review and critical analysis. *Clinical Psychology Review*, 2:523–538, 1982.

[29] J. F. George. Computer-based monitoring: common perceptions and empirical results. *MIS Quarterly*, 20(4):459–480, 1996.

[30] J. Gittelsohn, A. V. Shankar, K. P. West, and R. M. Ram. Estimating reactivity in direct observation studies of health behaviors. *Human Organization*, 56(2):182–189, 1997.

[31] M. Richtel. "Young, in Love and Sharing Everything, Including a Password", 2012.

[32] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith. Smudge attacks on smartphone touch screens. In *USENIX 4th Workshop on Offensive Technologies*, 2010.

[33] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 6:1–6:12, New York, NY, USA, 2011. ACM.

[34] R. Wash and J. K. Mackie-mason. Security When People Matter : Structuring Incentives For User Behavior. *Screening*, 2007.

[35] J. M. Stanton, K. R. Stam, P. R. Mastrangelo, and J. Jolton. Behavioral Information Security : Two End User Survey Studies of Motivation and Security Practices. In *Information Security*, 2004.

[36] R. West. The psychology of security. *Commun. ACM*, 51(4):34–40, April 2008.

[37] A. C. Johnston. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3):549–566, 2010.

[38] H. Xu and M. B. Rosson. Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View. *Workshop on Usable IT Security*, 2007.

[39] C. Wright and P. Ayton. Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices? *International Journal of Human-Computer Studies*, 62(6):759–783, June 2005.

[40] R. B. Cialdini. Basic social influence is underestimated. *Psychological inquiry*, 16(4):158–161, 2005.

[41] E. A. Locke. Toward a theory of task motivation and incentives. *Organizational Behavior and Human Performance*, 3(2):157 – 189, 1968.

[42] M. T. Siponen. Advanced topics in information resources management. chapter On the role of human mortality in information system security: from the problems of descriptivism to non-descriptive foundations, pages 301–319. IGI Publishing, Hershey, PA, USA, 2003.

[43] P. M. King and M. J. Mayhew. Moral judgement development in higher education: Insights from the defining issues test. *Journal of moral education*, 31(3):247–270, 2002.

[44] M. Siponen, R. Willison, and R. Baskerville. Power

and practice in information systems security research. 2008.

[45] J. P. Gibbs. *Crime, punishment, and deterrence*. Elsevier New York, 1975.

[46] S. Pahnila, M. Siponen, and A. Mahmood. Employees' behavior towards is security policy compliance. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 156b–156b. IEEE, 2007.

[47] T. August and T. I. Tunca. Network software security and user incentives. *Management Science*, 52(11):1703–1720, 2006.

[48] B. Bulgurcu. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Women*, 221(243):243, 2010.

[49] SR Boss and LJ Kirsch. The last line of defense: motivating employees to follow corporate security guidelines. In *Proceedings of the 28th International Conference on Information Systems*, pages 9–12, 2007.

[50] J. D'arcy and T. Herath. A review and analysis of deterrence theory in the is security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6):643–658, 2011.

[51] R. D. Gopal and G L Sanders. Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, pages 29–47, 1997.

[52] A. Kankanhalli, HH Teo, B. CY Tan, and KK Wei. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2):139–154, 2003.

[53] C. B. Foltz and P. Adviser-Cronan. *The impact of deterrent countermeasures upon individual intent to commit misuse: a behavioral approach*. University of Arkansas, 2000.

[54] S. J. Harrington. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS quarterly*, pages 257–278, 1996.

[55] S. M. Lee, SG Lee, and S. Yoo. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6):707–718, 2004.

[56] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance. What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *European Journal of Information Systems*, 18(2):126–139, 2009.

[57] L. Kohlberg. Stages in the development of moral thought and action, 1969.

[58] M. T. Siponen. On the role of human mortality in information system security: from the problems of descriptivism to non-descriptive foundations. *Information Resources Management Journal (IRMJ)*, 14(4):15–23, 2001.

[59] A. Blasi. Bridging moral cognition and moral action: A critical review of the literature. *Psychological Bulletin*, 88(1):1, 1980.

[60] J. Greenberg. Who stole the money, and when? individual and situational determinants of employee theft. *Organizational Behavior and Human Decision Processes*, 89(1):985–1003, 2002.

[61] Notre Dame. Information Security Policy, 2012.

[62] DL Huang, PL P Rau, and G Salvendy. Perception of information security. *Behaviour & Information Technology*, 29(3):221–232, 2010.

APPENDIX

A. INTERVENTION MESSAGES

Deterrence - No Previous Screen Lock

(1) IMPORTANT: If you misplace your phone and you don't have a password, the finder may have access to sensitive info about you or fellow students.

(2) IMPORTANT: This may put you in violation of [Institution's] policy on sensitive info! Visit this link for more information. [bit.ly]

Deterrence - Pattern Screen Lock

(1) IMPORTANT: Gesture based passwords have are easy to guess and thus anyone with your phone could have access to all your personal messages and info.

(2) IMPORTANT: This may put you in violation of [Institution's] policy on sensitive info! Visit this link for more information. [bit.ly]

Morality - No Previous Screen Lock

(1) IMPORTANT: [Institution] believes that all student, faculty and staff info on digital devices should be secure.

(2) IMPORTANT: The right thing to do is to add a password to your phone so as to comply with this requirement. Visit this link for more information. [bit.ly]

Morality - Pattern Screen Lock

(1) [Institution] believes that all student, faculty and staff info on digital devices should be secure, but yours is not because gesture passwords are easy to guess.

(2) The right thing to do is upgrade your phone to a text based password so as to comply with this requirement. Visit this link for more information. [bit.ly]

Incentive - No Previous Screen Lock

(1) IMPORTANT: As a way to encourage security, we are giving away a free $10 Amazon Gift Card.

(2) IMPORTANT: You can be entered into our drawing by simply adding a password to your phone. Visit this link for more information. [bit.ly]

Incentive - Pattern Screen Lock

(1) IMPORTANT: As a way to encourage better security practices, we are giving away a free $10 Amazon Gift Card.

(2) IMPORTANT: You can be entered into our drawing by simply upgrading your phone to a text based password. Visit this link for more information. [bit.ly]